Tetiana Venkel

ENGLISH FOR SPECIFIC PURPOSES

CYBERSECURITY: THREATS, ISSUES, AND DEFENCES

Chernivtsi
2021

Тетяна Венкель

Англійська мова за професійним спрямуванням

Кібербезпека:
загрози, проблеми, захист

ББК 81.432.1-923.7
УДК 811.111(075.8)

Англійська мова професійного спрямування. Кібербезпека: загрози, проблеми, захист. Част. 1 / Укл.: Венкель Т. В. – Чернівці, 2021. – 102 С.

Посібник укладений на основі текстових матеріалів *Discovering Computers Enhanced*: *Tools, Apps, Devices, and the Impact of Technology: – Shelly Cashman Series, 2017. – 640 p.* (навчальні тексти) та наявних в широкому доступі Інтернет-джерел і розрахований на студентів 2 курсу вищих навчальних закладів України, які навчаються за освітньо-кваліфікаційним рівнем «Бакалавр» за спеціальністю 125 «Кібербезпека» і мають базовий рівень підготовки з англійської мови не нижче B1 (згідно CEFR). Посібник містить опорні тексти, цикли лексичних вправ, спрямовані на: (1) вивчення та засвоєння студентами фахової англомовної термінології із зазначеної спеціальності; (2) активізацію навичок читання, перекладу, реферування та анотування англомовної фахової літератури; (3) активізацію навичок усного мовлення в межах тематики, що вивчається. Мета посібника: • забезпечити студентів базовою інформацією про найновіші технології в галузі кібербезпеки з автентичних англомовних джерел; • забезпечити поглиблене розуміння важливості вмілого й безпечного застосування комп'ютерів та Інтернет-ресурсів у сфері бізнесу та суспільного життя; • сприяти розумінню та вільному оперуванню основними поняттями та англомовною термінологією в галузях, пов'язаних з користуванням Інтернет-мережею, з захистом інформації та кібербезпекою. Зазначена мета досягається шляхом виконання вправ, завдань та інтерактивних навчальних видів діяльності, що підвищує мотивацію студентів навчатися із залученням безпосереднього використання комп'ютерів, мобільних пристроїв та Інтернет-ресурсів. Лексичні вправи і навчальні й тестові завдання до автентичного текстового матеріалу розроблені укладачем посібника. Уроки 1-4 розроблялися за участю Л.І. Ніжнік.

Посібник містить автентичні фахові тексти, пов'язані з тематикою, що вивчається, для самостійного опрацювання з подальшим анотуванням та обговоренням прочитаного.

BEFORE YOU START…

(1) Read the Information file below and answer the following questions.
Information file

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cybersecurity and physical security.

Ensuring cybersecurity requires coordinated efforts throughout an information system. Elements of cybersecurity include:

- Application security
- Information security
- Network security
- Disaster recovery / business continuity planning
- Operational security
- End-user education

One of the most problematic elements of cybersecurity is the quickly and constantly evolving nature of security risks. The digital world moves very fast, but a new survey claims that cybersecurity strategy does not move fast enough to keep up with threats – and experts tend to agree.

The traditional approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment.

"The threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk. It's no longer possible to write a large white paper about the risk to a particular system. You would be rewriting the white paper constantly..."

(Adam Vincent, CTO-public sector at Layer 7 Technologies (a security services provider to federal agencies including Defense Department organizations)

To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach, for example, recently issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments.

1. What do you need to know about digital safety and security?
2. While you may be familiar with some of the content in this manual, **do you know how to:**
   a) avoid risks when playing online games?
   b) determine if an email message has been spoofed?
   c) tell if your computer or device is functioning as a zombie?
   d) set up a personal firewall?
   e) protect computers and devices from viruses and other malware?
   f) protect your passwords?
   g) use two-step verification?
   h) prevent your data from being lost on the cloud?
   i) follow a disaster recovery plan?
   j) secure your wireless network?

k) safeguard your hardware and data from a disaster?
l) protect against a phishing scam?
m) protect yourself from social engineering scams?
n) evaluate your electronic profile?

(2) Read and discuss the statement in the box basing on the questions below.

"Users should take precautions to protect their digital content. I am careful when browsing the web, use antivirus software, and never open email messages from unknown senders. I use a cloud storage provider to back up my computer and mobile devices."

1. Do you agree with the author of the statement above? 2. Do you take precautions when you browse the Internet? 3. Which of the steps mentioned in the statement do/don't you do?

After completing this course, you will be able to:

- define the term 'digital security risks' and briefly describe the types of cybercriminals.
- describe various types of Internet and network attacks (malware, botnets, denial of service attacks, back doors, and spoofing) and explain general ways to safeguard against these attacks, including firewalls.
- discuss techniques to prevent unauthorized computer access and use, including access controls, user names, passwords, possessed objects, and biometric devices.
- explain ways that software manufacturers protect against software piracy.
- discuss how encryption, digital signatures, and digital certificates work.
- identify safeguards against hardware theft, vandalism, and failure.
- explain options available for backing up.
- identify risks and safeguards associated with wireless communications.
- recognize issues related to information accuracy, intellectual property rights, codes of conduct, and green computing.
- discuss issues surrounding information privacy, including electronic profiles, cookies, phishing, spyware and adware, social engineering, privacy laws, employee monitoring, and content filtering.

Unit 1. Digital Security Risks

Pre-Reading Activity

Answer the questions.

1. What digital security risks can you name? 2. Can you give an example of an accidental security breach? 3. What categories of cyber criminals can you name? What do these people do? Why is their activity considered criminal? Give your reasons and examples.

1. a) Read the texts using the dictionary; b) translate the underlined words and word combinations into Ukrainian (in writing); c) pay attention to the terminological units in bold type. Be sure you can give their definition in English and their Ukrainian equivalents.

Digital Security Risks

Today, people rely on technology to create, store, and manage their critical information. Thus, it is important that computers and mobile devices, along with the data and programs they store, are accessible and available when needed. It is also crucial that users take measures to protect or safeguard their computers, mobile devices, data, and programs from loss, damage, and misuse.

For example, organizations must ensure that sensitive data and information, such as credit records, employee and customer data, and purchase information, is secure. Home users must ensure that their credit card numbers are secure when they make online purchases.

A **digital security risk** is any event or action that could cause a loss of or damage to computer or mobile device hardware, software, data, information, or processing capability. The more common digital security risks include Internet and network attacks (for example, virus attacks), **unauthorized access** and use (e.g.[1], intercepting wireless communications), **hardware theft** (e.g., stolen computers), **software theft** (illegal copying), **information theft** (stolen identity), and **system failure** (e.g., caused by a lightning strike).

While some **breaches** to digital security are accidental, many are intentional. Some **intruders** do not disrupt a computer or device's functionality; they merely access data, information, or programs on the computer or mobile device before signing out. Other intruders indicate some evidence of their presence either by leaving a message or by deliberately altering or damaging data.

Cybercrime

An intentional breach to digital security often involves a deliberate act that is against the law. Any illegal act involving the use of a computer or related devices generally is referred to as a **computer crime**. The term **cybercrime** refers to online or Internet-based illegal acts such as distributing **malicious software** or committing **identity theft**. Software used by cybercriminals sometimes is called **crimeware**. Today, combating cybercrime is one of the top priorities.

Perpetrators of cybercrime typically fall into one of these basic categories: *hacker, cracker, script kiddie, corporate spy, unethical employee, cyberextortionist*, and *cyberterrorist*. The term **hacker**, although originally a complimentary word for a computer enthusiast, now has a derogatory meaning and refers to someone who accesses a computer or network illegally. Some hackers claim that the intent of their security breaches is to improve security.

A **cracker** also is someone who accesses a computer or network illegally but has the intent of destroying data, stealing information, or other malicious action. Both hackers and crackers have advanced computer and network skills. A **script kiddie** has the same intent as a

cracker but does not have the technical skills and knowledge. Script kiddies often use prewritten hacking and cracking programs to break into computers and networks.

Some **corporate spies** have excellent computer and networking skills and are hired to break into a specific computer and steal its proprietary data and information, or to help identify security risks in their own organization. Unscrupulous companies hire corporate spies, a practice known as corporate espionage, to gain a competitive advantage. Unethical employees may break into their employers' computers for a variety of reasons. Some simply want to exploit a security weakness. Others seek financial gains from selling confidential information. Disgruntled employees may want revenge.

A **cyberextortionist** is someone who demands payment to stop an attack on an organization's technology infrastructure. These perpetrators threaten to expose confidential information, exploit a security flaw, or launch an attack that will compromise the organization's network – if they are not paid a sum of money.

A **cyberterrorist** is someone who uses the Internet or network to destroy or damage computers for political reasons. The cyberterrorist might target the nation's air traffic control system, electricity-generating companies, or a telecommunications infrastructure. The term, **cyberwarfare**, describes an attack whose goal ranges from disabling a government's computer network to crippling a country. Cyberterrorism and cyberwarfare usually require a team of highly skilled individuals, millions of dollars, and several years of planning. Some organizations hire individuals previously convicted of computer crimes to help identify security risks and implement safeguards because these individuals know how criminals attempt to breach security.

[1] abbreviation for *exempli gratia*: a Latin phrase that *means* "for example"

2. Translate the following word combinations.

a) into Ukrainian:

1) to know how criminals attempt to breach security; 2) the goal ranges from disabling a government's computer network to crippling a country; 3) credit records, employee and customer data, and purchase information; 4) financial gains from selling confidential information; 5) to indicate some evidence of their presence; 6) the intent of destroying data, stealing information, or other malicious action; 7) to launch an attack that will compromise the organization's network; 8) to disrupt a computer or device's functionality; 9) to safeguard the computers from loss, damage, and misuse; 10) to target the nation's air traffic control system, electricity-generating companies, or a telecommunications infrastructure.

b) into English:

1) невдоволені компанії можуть помститися; 2) навмисне порушення цифрової безпеки; 3) дехто просто хоче скористатися зі слабини у захисті; 4) подолання кіберзлочинності – найвищий пріоритет; 5) нелегальний доступ до комп'ютера чи мережі; 6) зловмисники погрожують виказати таємну інформацію; 7) навмисна дія, що є протизаконною; 8) розповсюджувати шкідливе програмне забезпечення; 9) визначити слабкі місця у безпеці системи; 10) одержувати конкурентні переваги.

3. Fill in the table choosing from the box the appropriate Ukrainian equivalents of the following words and word combinations.

найважливіша/критична інформація; незахищені дані; покладатися; пошкодити комп'ютер; дефект (вразливість) системи безпеки; здійснити вторгнення до

комп'ютерних систем та мереж; здатність обробляти інформацію; приватна інформація; запобігати, захищати; навмисний(-о); невдоволений; бути звинуваченим у злочинному використанні можливостей комп'ютера; робити непридатним; недобросовісний/нерозбірливий в засобах; корпоративне шпигунство; боротися з кіберзлочинністю; зловмисник/злочинець; зневажливий; розкривати конфіденційну інформацію; називатися

1.	to rely on	
2.	to be referred to	
3.	crucial/critical information	
4.	derogatory	
5.	to cripple	
6.	to safeguard	
7.	sensitive data	
8.	security flaw	
9.	processing capability	
10.	to break into computers and networks	
11.	to expose confidential information	
12.	to disrupt a computer	
13.	intentional/deliberate(ly)	
14.	proprietary data	
15.	disgruntled	
16.	to be convicted of computer crimes	
17.	unscrupulous	
18.	corporate espionage	
19.	to combat cybercrime	
20.	perpetrator	

4. What do we call?

1) an attack whose goal ranges from disabling a government's computer network to crippling a country; 2) someone who accesses a computer or network illegally but has the intent of destroying data, stealing information, or other malicious action; 3) any illegal act involving the use of a computer or related devices; 4) someone who uses the Internet or network to destroy or damage computers for political reasons; 5) someone who has the same intent as a cracker but does not have the technical skills and knowledge 6) any event or action that could cause a loss of or damage to computer or mobile device hardware, software, data, information, or processing capability; 7) software used by cybercriminals; 8) online or Internet-based illegal acts such as distributing malware or committing identity theft; 9) someone who demands payment to stop an attack on an organization's technology infrastructure; 10) someone hired to break into a specific computer and steal its proprietary data and information.

5. a) Match the definitions with the following terms and terminological units; b) translate the terms into Ukrainian.

No.	**Word**	**Definition**		**Ukrainian equivalent**
1.	cyberwarfare	a)	viewing private accounts, messages,	*кібервійна*

			files or resources when one has not been given permission from the owner to do so	
2.	script kiddie	b)	any event or action that could cause a loss of or damage to computer or mobile device hardware, software, data, information, or processing capability	
3.	computer crime	c)	any program or file that is harmful to a computer user and can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission	
4.	crimeware	d)	stealing of personal information that makes it possible to use someone's bank account, credit card etc.	
5.	breach	e)	any illegal act involving the use of a computer or related devices	
6.	hacker	f)	online or Internet-based illegal acts	
7.	malicious software (malware)	g)	an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so	
8.	software theft	h)	unauthorised duplication and/or use of computer software	
9.	cyberterrorist	i)	someone who uses the Internet or network to destroy or damage computers for political reasons	
10.	unauthorized access	j)	an attack whose goal ranges from disabling a government's computer network to crippling a country	
11.	identity theft	k)	software used by cybercriminals	
12.	cybercrime	l)	someone who accesses a computer or network illegally	
13.	cyberextortionist	m)	is someone who demands payment to stop an attack on an organization's technology infrastructure	
14.	system failure	n)	someone who accesses a computer or network illegally with the intent of destroying data, stealing information, or other malicious action	
15.	digital security risk	o)	someone who uses prewritten	

			hacking and cracking programs to break into computers and networks	
16.	information theft	p)	stealing a computer and/or the associated physical equipment directly involved in the performance of data-processing or communications functions	
17.	cracker	q)	a condition which prevents a computer system from functioning properly	
18.	intruder	r)	someone trying to gain secret information on a government or a business competitor	
19.	hardware theft	s)	stealing of financial and/or personal information through the use of computers for making its fraudulent or other illegal use	
20.	corporate spy	t)	a person who is not authorised to use a computer or connect to a network	

6. Choose the correct answer.

1. According to the passage, corporate spies …
   a) are hired to break into a specific computer and steal its proprietary data.
   b) demand payment to stop an attack on an organization's technology infrastructure.
   c) require a team of highly skilled individuals, millions of dollars, and several years of planning.
   d) claim that the intent of their security breaches is to improve security.
2. Someone who uses the Internet or network to destroy or damage computers for political reasons is …
   a) a hacker.
   b) a cracker.
   c) a script kiddie.
   d) a cyberterrorist.
3. A script kiddie is…
   a) software used by cybercriminals.
   b) someone who accesses a computer or network illegally.
   c) someone who uses prewritten programs to break into computers and networks.
   d) any program or file that is harmful to a computer user.
4. The word *breach* in this text is closest in meaning to
   a) "an act of breaking or failing to observe a law, agreement, or code of conduct";
   b) "a gap in a wall, barrier, or defence, especially one made by an attacking army";
   c) "viewing, stealing or using sensitive, protected or confidential data by an individual unauthorized to do so";
   d) "rise and break through the surface of the water".
5. Any illegal act involving the use of a computer or related devices generally is referred to as a …
   a) computer crime.

b) corporate espionage.
c) malicious software.
d) cyberwarfare.

6. The word *gains* in the text is translated into Ukrainian as
a) прибутки.
b) збільшення.
c) коефіцієнт підсилення.
d) гніздо, паз.

7. The word *intruder* in the text is closest in meaning to
a) someone not authorised to use a computer or connect to a network.
b) a person who for some reason is not wanted or welcome.
c) someone who settles on land without right or title.
d) someone who enters the privacy or property of another without permission.

8. According to the text, organizations hire individuals previously convicted of computer crimes
a) to expose confidential information, exploit a security flaw, or launch an attack.
b) to help identify security risks and implement safeguards.
c) to gain a competitive advantage.
d) to improve security.

9. Which is the best way to translate the following sentence:

A script kiddie has the same intent as a cracker but does not have the technical skills and knowledge.

a) Хакер-дилетант має ті самі наміри, що й зламувач, але не володіє технічними навичками і знаннями.
b) Скрипткіді має ті самі наміри, що й крекер, але не має технічних навичок і знань.
c) Скриптмалюк має такі самі інтенції, які й заломувач, але не володіє технічними вміннями і знанням.
d) Хакер-дилетант має той же намір, що й крекер, але не має технічних умінь і знань.

10. The word combination *to implement safeguards* in the text is translated as:
a) імплементувати сейфгардів.
b) застосовувати засоби захисту.
c) реалізовувати заходи безпеки.
d) надавати гарантії.

7. a) Translate the following sentences into Ukrainian. Use the dictionary if necessary.

1. A security breach is one of the earliest stages of a security attack by a malicious intruder, such as a hacker, cracker or malicious application. 2. To gain advantage over their competitors, many corporations hire ex-military and government agents trained as spies. 3 Hacker is a term used by some to mean "a clever programmer" and by others, especially those in popular media, to mean "someone who tries to break into computer systems." 4. My co-worker opened an unknown email containing multiple viruses, infected our data center, and caused a large security breach in our network. 5. Due to their most recent security breach, the company offered identity theft protection to all of their customers as a countermeasure. 6. If an intrusion, abnormality or violation is detected, the firewall issues a notification to the network or security administrator. 7. A cracker is someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs;

or in other ways intentionally breaches computer security. 8. When a company tracks web searches and keystrokes of employees who are using its computers, it is not breaking the law. 9. The typical script kiddy uses existing and frequently well-known and easy-to-find programs to exploit weaknesses in other computers on the Internet – often randomly and with little regard or perhaps even understanding of the potentially harmful consequences. 10. Hackers view script kiddies with alarm and contempt since they do nothing to advance the "art" of hacking but sometimes unleashing the wrath of authority on the entire hacker community.

b) Match the synonyms:

intruder	easy-to-find	contempt	violation	wrath	malicious	intentional	breach

gap	anger	trespasser	harmful	disrespect	deliberate	intrusion	accessible

8. a) Render the following text in English. b) Be ready to explain how script kiddies use malware.

Хакер-дилетант (скрипткіді) – це часто, але не завжди, неповнолітній хакер, зловмисник, який використовує скрипти або програми, розроблені більш досвідченими хакерами чи зламувачами. Часто основна мотивація хакерів-дилетантів для атаки – це просто привернути увагу однолітків. Скрипткіді, як правило, не користуються повагою боку спільноти хакерів через відсутність самостійно набутих навичок і залежність від попередньо розроблених програм і файлів. Часто вважається, що скрипткіді приречені стати хакерами-зламувачами, оскільки їхнє прагнення до набуття майстерності та влади переважно витісняє їхнє бажання навчатися складнощам хакерської справи. Хакери-дилетанти вирізають та вставляють коди, написані іншими, не розуміючи або не бажаючи зрозуміти, як цей код насправді працює, і взагалі лише дбають про те, чим цей код може прислужитися їм. Частіше вони займаються скануванням Інтернету у пошуках комп'ютера-жертви, який має певну вразливість, радше для того, щоб знайти спосіб застосувати свої обмежені навички, а не націлитись на конкретну компанію чи сайт з якихось причин. Через велику кількість доступних в Інтернеті програм, розроблених справжніми хакерами чи зламувачами, скрипткіді можуть легко завдавати шкоди, іноді просто ввівши IP-адресу та натиснувши кнопку. Вважається, що зараз в Інтернеті можуть існувати мільйони таких хакерів-дилетантів.

*c)** **Internet Research**

- Browse the free web resources to search for 'Difference between the main types of cybercrime and cybercriminals'. Be ready to present the results of your research in class in the form of PowerPoint Presentation / written (oral) report / 200-250-word essay (choose the form that suits you best).

9. Write a short summary of the text "How Should Cybercriminals Be Punished?", p. 13 (see the scheme in the box below).

The title of the article/text is: _____
*The authors of the article/text are: _____
The article/text is dedicated to _____
It also touches upon the problems of _____. _____ are discussed in the article/text.
The authors stress that _____
It should be (noted / stressed / pointed out / emphasized / mentioned) that _____
*The (experimental) data analysis led to the following conclusions: _____

Extended Reading

(1) How Should Cybercriminals Be Punished?

A hacker received a 10-year jail sentence for selling credit card information from several large corporations, costing one company approximately $200 million. In another case, a hacker accessed the personal online accounts of celebrities, as well as people he knew, and distributed revealing photos and information. He also received 10 years in jail, in part for the emotional distress his actions caused his victims. Do these sentences seem too harsh? Some legal experts point out that the punishment given to some hackers is not in line with crimes of a violent nature.

In addition to the extent of the punishment, other issues surrounding cybercrime laws include whether an action is defamation or free speech and who should be punished, the hacker or those who were hacked. If a hacker's actions damage the reputation of another via libel or slander, should the hacker be prosecuted under the defamation law or be protected under the First Amendment? A hacktivist, which is a type of hacker whose actions are politically or socially motivated, believes his or her actions should be protected under the First Amendment. Should companies whose systems have been breached be punished for their lax security? The Federal Trade Commission (FTC) has fined companies whose security flaws enabled hackers to access their systems.

Legislators have made efforts to define and prevent cybercrime, with both new laws and the expansion of existing laws. Cybercrime laws vary between states and countries, making it difficult to establish what is illegal.

Determining who has jurisdiction over a case can create more legal hassles. For example, which area is responsible for determining punishment: where the victim(s) resides or where the criminal lives?

Consider This:

1. Should hacktivism be punishable? Why or why not? 2. Should corporations be liable for damages caused by hackers? Why or why not? 3. Should hackers receive comparable punishment to violent criminals? Why or why not?

(2) Corporate Cyber Crime Definition

Cyber crime is the criminal enterprise of our age. In the same way that the Cold War feared spying by enemy agents and the turn of the last century was terrified of anarchist bombings, cyber crime has come to define what it is that we are most afraid of. Perhaps most prominent of the varieties of these crimes is corporate cyber crime, which by some reports costs billions of dollars every year. However, we are often very afraid of things we don't understand, so why don't we take a look at what corporate cyber crime actually is.

Cyber crime is leveraging the power of the internet in order to defraud, spy on, or otherwise violate the private systems of other individuals. Corporate cyber crime is focused specifically on large companies and trying to gain access to their systems for a variety of reasons. Some of those reasons include attempting to gain access to proprietary data like formulas for products, whether it be a new medication or simply how they make Coca-Cola, trying to access business plans and intended corporate strategies, attempting to gain personal information about employees of the company, or trying to maliciously alter data for one reason or another. Having access to a corporate database gives a hacker amazing amounts of power to do incredible damage with little more than erasing a file or changing a few numbers.

Methods of Cyber Criminals

While there are highly technical ways of gaining access to corporate systems, the most common ways are fairly low tech in their method, if not necessarily in their execution. Since the beginning of spying, those involved in espionage have relied primarily on their ability to convince people who have access to sensitive information to give the spies access as well. Modern cyber criminals do much the same thing, but they do it online and usually in exchange for passwords. There are three primary ways in which this is accomplished.

- Security Breaches – Hackers use their social skills and charm in order to convince an employee to simply give them the access they want. Sometimes this is just by trying to make a friend, sometimes it involves threats or blackmail, and sometimes it comes with the promise of rewards for the person inside. Regardless, this is merely them speaking to the right person in the right way.
- Spear Phishing – this method involves using other forms of access to gain greater access. A hacker who has already broken into somebody's email can then send a message to somebody else, pretending to be the owner, and convince them to give up sensitive information.
- Social Media Fraud – This comes in a variety of different forms. It can be a method of one of the above two types, or it can also mean accessing a person's social media account, doing research on them, and trying to determine what sorts of passwords or security keys they might employ.

There are also a number of security holes in any operating system or connection client. In a system that is designed to communicate to outside actors, it's sometimes very difficult to make sure that all of the extra access methods that creates are closed. Techniques like packet sniffing can also be employed, where somebody can "watch" the data being transferred over a wireless network and pick out important information.

Methods of Preventing Corporate Cyber Crime

There are a number of methods that corporations use in order to try to avoid these types of breaches. First of all, they usually will use a Unix based system for most of their networking. While employing this form of operating system with every computer in the company would be even more secure, they are often difficult to use, so companies are forced to provide Windows or Mac machines instead. They also employ cyber security teams to keep an eye out for potential security holes.

Something that many companies have started doing is putting highly sensitive information on closed networks with no access to the outside world so that enterprising cyber criminals have to be physically present to access them.

More than that, though, companies are starting to require that their employees undergo training designed to help them recognize when a hacker is trying to manipulate them into sharing company secrets and what they should do if this happens. More than anything, humans are the easiest piece of any security plan to exploit, so arming them with knowledge can help to significantly reduce a hacker's chance of getting what they want.

These types of attack don't happen often, but it only takes one breach to be devastating. That's why it's so important that companies take cyber crime seriously.

(http://www.internationalbusinessguide.org/what-is-corporate-cyber-crime/)

(3) Computer Security Ethics and Privacy

By Vincent Deguzman

Today, many people rely on computers to do homework, work, and create or store useful information. Therefore, it's important for the information to be stored and kept properly. It's also extremely important to protect computers from data loss, misuse and abuse. For example,

businesses need to keep their information secure and shielded from hackers. Home users also need to ensure their credit card numbers are secure when participating in online transactions. A computer security risk is any action that could cause loss of information to software, data, processing incompatibilities or damage to computer hardware.

An intentional breach in computer security is known as a computer crime, which is slightly different from a cybercrime. A cybercrime is known as illegal acts based on the Internet and is one of the FBI's top priorities. There are several distinct categories for people that perpetrate cybercrimes, and they are: hacker, cracker, cyberterrorist, cyberextortionist, unethical employee, script kiddie and corporate spy. A hacker is defined as someone who accesses a computer or computer network unlawfully. They often claim that they do this to find leaks in the security of a network.

The term cracker refers to someone intentionally accessing a computer or computer network with malice in mind. They access computers with the intention of destroying or stealing information. Both crackers and hackers have advanced network skills.

A cyberterrorist is someone who uses a computer network or the Internet to destroy computer systems for political reasons. It's similar to a terrorist attack because it requires highly skilled individuals, millions of dollars to implement and years of planning. The term cyberextortionist is someone who uses email as an offensive force. They usually send a company a threatening email stating that they will release some confidential information, exploit a security leak, or launch an attack that will harm a company's network. They use blackmail to demand a certain amount of money in exchange for not launching an attack.

An unethical employee is one who illegally accesses their company's network for numerous reasons. One could be the money they can get from selling top secret information, or some may be bitter and want revenge.

A script kiddie is similar to a cracker because they might want to do harm, but often lack the technical skills. Script kiddies tend to use prewritten hacking and cracking programs.

A corporate spy has extensive computer and networking skills and is hired to break into a specific computer or computer network to steal, delete data and/or information. Shady companies hire these types of people in a practice known as corporate espionage. They do this to gain an advantage over their competition. Business and home users must do their best to protect or safeguard their computers from security risks. […] However, one must remember that there is no guaranteed way of protecting your computer, so learning about your options is important.

When you transfer information over a network it has a high security risk compared to information transmitted in a business network because the administrators usually take stringent measures to protect against security risks. Over the Internet the risk is much higher. If you're not sure if your computer is secure, it's advisable to use an online security service to check your computer for email and Internet vulnerabilities. The company will then give some pointers on how to correct these vulnerabilities. The Computer Emergency Response Team Coordination Center is a good resource.

The typical network attacks that puts computers at risk are: viruses, worms, spoofing, Trojan horses and denial of service attacks. Every unprotected computer is vulnerable to a computer virus. Once the virus is in the computer it can spread throughout, infecting other files and potentially damaging the operating system itself.

A computer worm is a program that repeatedly copies itself and is similar to a computer virus. However, a virus needs to attach itself to an executable file and become part of it. A computer worm doesn't need to do that. It copies itself, travels to other networks and eats up a lot of bandwidth. A Trojan horse is a program that hides and seems to be a legitimate program

but in reality is a fake. A certain action usually triggers the Trojan horse, and unlike viruses and worms they don't replicate. Computer viruses, worms, and Trojan horses are all classified as malicious-logic programs. These three are the most common but there are many variations, which are impossible to list here. You know when a virus, worm, or Trojan horse if one infects a computer or more of the following events take place:

- Screen shots of strange messages or pictures appear.
- You experience a sudden drop in memory.
- Music or sound plays randomly.
- Files become corrupted.
- Programs or files don't work properly.
- Unknown files or programs randomly appear.
- System properties fluctuate.

Computer viruses, worms, and Trojan horses deliver their payload or instructions through four common ways:

- When an individual runs an infected program. If you regularly download data from the Internet, you should always scan it, especially if you've downloaded executable files.
- When an individual runs an infected program.
- When an individual boots a computer with an infected drive. Don't leave media files in your computer when you shut it down.
- When a user connects an unprotected computer to a network.

Today, a common method of infection is by opening an infected file, which arrives as an email attachment. Again, it's important to scan all incoming data. There are literally thousands of computer malicious logic programs and new ones appear every day, so it's important to update your virus and spyware protection programs regularly. Whenever you start a computer, you should have no removable media in the drives. This goes for CD, DVD, and floppy disks, as well.

As mentioned earlier, there's no known method for completely protecting a computer or computer network from computer viruses, worms, and Trojan horses, but people can take several precautions to significantly reduce their chances of being infected.

(http://www.webreference.com/internet/security/index.html)

Unit 2. Internet and Network Attacks

Pre-Reading activities:
Answer the questions.

1. What is *malware*? Can you give examples of any software that leads to security risks? 2. What harm can this software cause to the computer system? 3. How do you protect your computer from Internet and network attacks?

1. a) Read the texts using the dictionary. b) Translate the underlined words and word combinations into Ukrainian (in writing). c) Pay attention to the terminological units in bold type. Be sure you can give their definition in English and their Ukrainian equivalents.

Malicious Software

Information transmitted over networks has a higher degree of security risk than information kept on an organization's premises. In an organization, network administrators usually take measures to protect a network from security risks. On the Internet, where no central administrator is present, the security risk is greater. Internet and network attacks that jeopardize security include **malware**, **botnets**, **denial of service attacks**, **back doors**, and **spoofing**.

Malware, short for *malicious software*, consists of programs that act without a user's knowledge and deliberately alter the operations of computers and mobile devices. Some malware contains characteristics in two or more classes. For example, a single threat could contain elements of a *virus*, *worm*, and *trojan horse*.

The term *malware* was first used by computer scientist and security researcher Yisrael Radai in 1990. However, malware existed long before this; one of the first known examples of malware was the *Creeper virus* in 1971, which was created as an experiment by BBN Technologies engineer Robert Thomas. Creeper was designed to infect mainframes on ARPANET. While the program did not alter functions, or steal or delete data, the program moved from one mainframe to another without permission while displaying a teletype message that read, "I'm the creeper: Catch me if you can." Creeper was later altered by computer scientist Ray Tomlinson, who added the ability to self-replicate to the virus and created the first known computer worm. The concept of malware took root in the technology industry, and examples of viruses and worms began to appear on Apple and IBM personal computers in the early 1980s before becoming popularized following the introduction of the World Wide Web and the commercial internet in the 1990s.

Malware can deliver its *payload*, or destructive event or prank, on a computer or mobile device in a variety of ways, such as when a user opens an infected file, runs an infected program, connects an unprotected computer or mobile device to a network, or when a certain condition or event occurs, such as the computer's clock changing to a specific date. A common way that computers and mobile devices become infected with viruses and other malware is through users opening infected email attachments.

What if you cannot remove malware? In extreme cases, in order to remove malware from a computer or mobile device, you may need **to erase**, or **reformat**, an infected computer's hard drive, or **reset** a mobile device to its **factory settings**. For this reason, it is critical you have uninfected (clean) **backups** of all files. Consider creating **recovery media** when you purchase a new computer, and be sure to keep all **installation media** in the event you need **to reinstall** the computer's operating system and your apps. Seek advice from a technology specialist before performing a format or reformat instruction on your media.

Types of malware. There are different types of malware that contain unique traits and characteristics. A **virus** is the most common type of malware, and it's defined as a malicious program that can execute itself and spreads by infecting other programs or files. A **worm** is a type of malware that can self-replicate without a host program; worms typically spread without any human interaction or directives from the malware authors. A **Trojan horse** is a malicious program that is designed to appear as a legitimate program; once activated following installation, Trojans can execute their malicious functions. **Spyware** is a kind of malware that is designed to collect information and data on users and observe their activity without users' knowledge.

Other types of malware include functions or features designed for a specific purpose. **Ransomware**, for example, is designed to infect a user's system and encrypt the data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data. A **rootkit** is a type of malware designed to obtain administrator-level access to the victim's system. Once installed, the program gives threat actors root or privileged access to the system. A **backdoor virus** or *remote access Trojan* (RAT) is a malicious program that secretly creates a backdoor into an infected system that allows threat actors to remote access it without alerting the user or the system's security programs.

2. Translate the following word combinations.

a) into Ukrainian:

1) to infect a user's system and encrypt the data; 2) without alerting the user or the system's security programs; 3) the computer's clock changing to a specific date; 4) to move from one mainframe to another without permission; 5) opening infected email attachments; 6) privileged access to the system; 7) the ability to self-replicate; 8) to execute itself and spread by infecting other programs or files; 9) to be designed to appear as a legitimate program; 10) to collect information and data on users and observe their activity without users' knowledge.

b) into English:

1) функції та властивості, розроблені для особливої мети; 2) спостерігати за діяльністю користувача без його відома; 3) перевстановити операційну систему комп'ютера і всі додатки; 4) одержати доступ на рівні адміністратора до системи жертви; 5) вживати заходів для захисту мережі; 6) вимагати виплати викупу за розшифрування інформації; 7) надати зловмиснику віддалений доступ до системи; 8) шкідливе ПЗ зі здатністю до самовідтворення; 9) збирати інформацію про користувача; 10) звертатися за порадою до фахівця.

3. Choose from the box the appropriate Ukrainian equivalents of the following words and word combinations.

піддавати небезпеці; шкідливе ПЗ; витівка; шпигунське ПЗ; «чорний хід»/лазівка; троянський кінь; імітація з'єднання; черв'як; програма-вимагач; самовідтворюваний; резервна копія; центральний процесор (сервер/головний комп'ютер); вірус; встановлювальні носії; зомбі-мережа; програма-приховувач вторгнення (руткіт); атака для порушення нормального обслуговування користувачів; програма головного процесора; вказівка/інструкція; джерело (виконавець) загрози

1.	malware	
2.	botnet	
3.	denial of service attack	
4.	back door	

5.	spoofing	
6.	virus	
7.	worm	
8.	trojan horse	
9.	jeopardize	
10.	prank	
11.	backup	
12.	spyware	
13.	ransomware	
14.	rootkit	
15.	installation media	
16.	self-replicate	
17.	directive	
18.	mainframe	
19.	threat actor	
20.	host program	

4. What do we call:

1) a kind of malware that is designed to collect information and data on users and observe their activity without users' knowledge; 2) a program designed to breach the security of a computer system while ostensibly performing some innocuous function; 3) a type of malware that can self-replicate without a host program without human interaction ; 4) controls of a computer hardware or software (or of a device, equipment, or machine) as preset by its manufacturer ; 5) a malicious program that can execute itself and spreads by infecting other programs or files 6) malware designed to infect a user's system, encrypt the data and then demand a ransom payment from the victim in exchange for decrypting them; 7) a collection of compromised computers often referred to as "zombies" infected with malware that allows an attacker to control them; 8) a type of malware designed to obtain administrator-level access to the victim's system; 9) a malicious program that secretly creates an access into an infected system without alerting the user or the system's security programs; 10) programs that act without a user’s knowledge and deliberately alter the operations of computers and mobile devices.

5. a) Match the definitions with the following terms and terminological units; b) translate the terms into Ukrainian.

1.	Virus	a)	A program that hides within or looks like a legitimate program. Unlike a virus or worm, a trojan horse does not replicate itself to other computers or devices.
2.	Worm	b)	A program that hides in a computer or mobile device and allows someone from a remote location to take full control of the computer or device.
3.	Trojan horse	c)	A program placed on a computer or mobile device without the user’s knowledge that secretly collects information about the user and then communicates the information it collects to some outside source while the user is online.
4.	Rootkit	d)	A program that copies itself repeatedly, for example

			in memory or on a network, using up resources and possibly shutting down the computer, device, or network.
5.	Adware	e)	A potentially damaging program that affects, or infects, a computer or mobile device negatively by altering the way the computer or device works without the user's knowledge or permission.
6.	Spyware	f)	A program that displays an online advertisement in a banner, pop-up window, or pop-under window on webpages, email messages, or other Internet services.

6. Choose the correct answer.

1. According to the passage, a virus is…
   a) a kind of malware that is designed to secretly collect information and data on users.
   b) a kind of malware to infect mainframes on ARPANET.
   c) a malicious program that can execute itself and spreads by infecting other programs or files.
   d) is a type of malware that can self-replicate without a host program.
2. A type of malware designed to obtain administrator-level access to the victim's system is …
   a) a Troyan horse.
   b) a rootkit.
   c) a prank.
   d) a ransomware.
3. A script backdoor is…
   a) a ransom payment from the victim in exchange for decrypting the system's data.
   b) malware that typically spread without any human interaction or directives from the malware authors.
   c) a malicious program that once activated following installation, can execute its malicious functions.
   d) a malicious program that secretly creates an access to an infected system that allows threat actors to remote access it without alerting the user or the system's security programs.
4. The word *backup* in this text is closest in meaning to
   a) "a copy or duplicate version, especially of a file, program, or entire computer system, retained for use in the event that the original is in some way rendered unusable."
   b) "a person, plan, device, etc., kept in reserve to serve as a substitute, if needed."
   c) "an overflow or accumulation due to stoppage, malfunctioning, etc."
   d) "a ball that curves in a direction corresponding to the bowling hand of the bowler".
5. Any programs that act without a user's knowledge and deliberately alter the operations of computers and mobile devices is referred to as a …
   a) spyware
   b) ransomware
   c) malicious software
   d) cyberwarfare.
6. The word *prank* in the text is translated into Ukrainian as

a) прибутки
b) витівка, злий жарт
c) викуп
d) резервна копія.

7. The word *threat actor* in the text is closest in meaning to
   a) someone partially or wholly responsible for an incident that can impact an organization's security.
   b) a person who for some reason is not wanted or welcome.
   c) indication of impending danger or harm.
   d) a person or thing that is regarded as dangerous or likely to inflict pain or misery.

8. According to the text, the Creeper virus
   a) was created as an experiment to infect mainframes on ARPANET.
   b) to help identify security risks and implement safeguards on ARPANET.
   c) execute itself and spreads by infecting other programs.
   d) to remote access without alerting the system's security programs.

9. Which is the best way to translate the following sentence:

In an organization, network administrators usually take measures to protect a network from security risks.

a) В організації мережа адміністраторів вживає заходів для захисту мережі від ризиків безпеки.
b) В організації адміністратори мереж приймають міри щоб захистити мережі від безпеки ризиків.
c) В організації мережеві адміністратори зазвичай вживають заходів для захисту мережі від ризиків безпеки.
d) Зазвичай в організації мережі від ризиків безпеки вживають заходів для захисту мережевих адміністраторів.

10. The word combination *to demand a ransom payment* in the text is translated as:

a) вимагати сплати за викупом b) вимагати заплатити викуп c) вимагати викуп оплати d) викупити плату за вимогу.

7. a) Translate the following sentences:

- into Ukrainian.

1. The system is an in-house tool that aggregates and analyses threat intelligence information from a number of sources in order to detect and mitigate the impact of infected computers or local websites. 2. A threat analysis derived from intelligence on these networks leads to proposals for combating such cyberterrorism. 3 You must not load or transmit through the site any computer virus or anything designed to interrupt or disrupt the proper operation of the site. 4. Such events, as a rule, may occur as a consequence of a computer virus working or a careless handling of some programs. 5. One of the fundamental differences between a Trojan and a virus is that a virus on your computer executes autonomously, whereas a Trojan horse is constructed to be used directly by a remote intruder. 6. The materials accessible through this website will be free of bugs, viruses, worms, cancelbots, trojan horses or other harmful components. 7. Many organizations had not applied the required patch to protect against the MSBLAST worm when it struck corporate networks all over the world. 8. Additionally, mobile devices allow a new pathway into the network environment for hackers, as these can be compromised to allow a backdoor around security mechanisms. 9. *Rootkit Hunter* scans systems for known and unknown rootkits, backdoors,

sniffers and exploits. 10. A ransomware is a kind of malware that withholds some digital assets from victims and asks for payment for the assets' release.

- *into English*

1. Для захисту від мережевих атак підміни IP адрес усередині локальної мережі, можна додати статичні записи в таблицю. 2. Зомбі-мережі, як правило, також можуть атакувати сервери: відправляючи численні запити на сервер з багатьох заражених клієнтів. 3. Наші системні адміністратори шукатимуть потрібні резервні копії даних, скопіюють і налаштують сервер для вас або зроблять резервний файл доступним для вас. 4. Програма-вимагач – це тип шкідливого програмного забезпечення, який обмежує доступ до комп'ютерної системи, яку він заражає, і вимагає сплати викупу її творцю, для того, щоби зняти обмеження. 5. Шукайте універсальне багатогранне програмне забезпечення для ПК, яке захистить вас від вірусів, програм-шпигунів, рекламного ПЗ, хакерів, небажаних повідомлень електронної пошти, фішингу та крадіжки особистих даних. 6. Після дзвінка ваш друг отримає повідомлення з нашого сайту, що це був просто невинний жарт. 7. В оновленому випуску програми ми виправили помилку, знайдену в попередній версії програмного забезпечення. 8. Шпигунські програми в основному використовуються IT-корпораціями для маркетингових цілей. 9. Крім того, вважають експерти, зараз почалася нова ера в історії мобільного зловмисного програмного забезпечення, коли смартфони стають об'єктами шпигунських атак, так само як і звичайні комп'ютери. 10. Глобальна епідемія комп'ютерних вірусів порушувала роботу ділових та споживчих мереж протягом останніх двох десятиліть; і далі періодично з'являються особливо зловмисні нові «черви» та інші віруси.

*b) Translate the following terms (consult a dictionary). *Define their meaning.*

cancelbot _____
bug _____
patch _____
sniffer _____
exploit _____
adware _____
phishing _____
botnet _____
spoofing _____
threat intelligence _____

8. a) Read and translate the Information file below (use the dictionary if needed).

b) Be ready to categorize threat actors, explain the difference between them and the way they use malware.*

Information file

A threat actor, also called a malicious actor, is an entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an organization's security.

In threat intelligence*, actors are generally categorized as external, internal or partner. With external threat actors, no trust or privilege previously exists, while with internal or partner actors, some level of trust or privilege has previously existed. The actor may be an individual or an organization; the incident could be intentional or accidental and its purpose malicious or benign.

External actors are the primary concern of threat intelligence services not only because

they are the most common, but also because they tend to be the most severe in terms of negative impact. Such threat actors are sometimes categorized as either being commodity or advanced. A commodity threat actor launches a broad-based attack hoping to hit as many targets as possible, while an advanced threat actor targets an organization, often seeking to implement an advanced persistent threat (APT) in order to gain network access and remain undetected for a long time, stealing data at will.

Another type of external threat actor is the so-called hacktivist. Hacktivist groups such as *Anonymous* use many of the same tools employed by financially-motivated cybercriminals to detect website vulnerabilities and gain unauthorized access or carry out distributed denial-of-service (DDoS) attacks. The motivation of most hacktivists is to gain access to sensitive information that will negatively impact the reputation of an individual, a brand, a company or a government.

* сукупність процесів збору, аналізу інформації про кіберзагрози

*c)** **Internet Research**

- Browse the free web resources to search for:

'The most disastrous cyber attacks in the world: their reasons and consequences'.

'What are the latest malware threats?' (Search for: malware news).

- Analyze the information you found and be ready to present the results of your research in class in the form of PowerPoint Presentation / written (oral) report / 200-250-word essay (choose the form that suits you best).

9. a) Read the following to learn about how to determine if an email message has been spoofed.*

Information file

Determine if an email message has been spoofed

Spoofed email messages appear to originate from one source, but in reality originate from another source. Spoofed email messages are often sent by nefarious people attempting to obtain personal information. For example, an email message appearing to be sent from a reputable source, such as your financial institution, may ask you to reply with personal information, such as a password, Social Security number, or account number. If you reply, you will be sending personal information to an unknown third party that could use the information to steal your identity, make unauthorized purchases, and more. The following steps describe some ways to determine if an email message has been spoofed.

• The email message requests personal information, such as account numbers, passwords, Social Security numbers, and credit card numbers.

• The email message contains spelling and/or grammatical errors.

• The email message encourages you to tap or click a link that takes you to another website.

• The header in the email message contains a different domain in the MessageID than the domain of the supposed sender.

• The "From" and "Reply-To" email addresses do not match. If you ever are unsure of whether an email message was spoofed, contact the supposed sender either via phone or a new email message (do not reply to the original email message) to verify the authenticity of the message.

b) Consider This:

Have you ever received a spoofed email message? Did you know it was spoofed? What steps did you take?

10. Write a short summary of the text 'Play It Safe to Avoid Online Gaming Risks', p. 24 (see the scheme in ex.10, Unit 1).

Extended Reading

(1) Play It Safe to Avoid Online Gaming Risks

Gamers often understand general security issues regarding online behavior, but they may not be aware of a different set of technology and social risks they may encounter as they interact in the online world. Anyone experiencing the joys of playing games online or playing games with others through online services should realize that thieves and hackers lurking behind the scenes may take advantage of security holes and vulnerabilities that can turn a gaming session into a nightmare.

Viruses, worms, and malware can be hidden in downloaded game files, mobile apps, email message attachments, and messaging software. In addition, messages on online social networks may encourage gamers to visit fraudulent websites filled with malware. If the game requires a connection to the Internet, then any computer connected to the game's server is subject to security cyberthreats.

Thieves can take control of a remote computer that does not have a high level of security protection and use it to control other computers, or they could break into the computer and install malware to discover personal information.

Malicious users know that the gaming community uses social media intensely, so they also create accounts and attempt to mislead uninformed users into revealing personal information. The thieves may claim to have software updates and free games, when they really are luring users to bogus websites that ask users to set up profiles and accounts.

Gamers should follow these practices to increase their security:

• Before downloading any software or apps, including patches to games, or disclosing any private details, check the developer to be certain the website or the person making the request is legitimate.

• Read the permissions notices to learn what information is being requested or being collected. Avoid games requiring passwords to be saved to an online account on a smartphone.

• Exercise extreme caution if the game requires ActiveX or JavaScript to be enabled or if it must be played in administrator mode.

• Use a firewall and make exceptions to allow only trusted individuals to access your computer or mobile device when playing multiplayer online games.

• Do not share personal information with other gamers whom you meet online.

Consider This:

Have you played online games or downloaded gaming apps and followed the advice listed here? How will you change your gaming behavior now that you are aware of specific security threats?

(2)

A **botnet**, or *zombie army*, is a group of compromised computers or mobile devices connected to a network, such as the Internet, that are used to attack other networks, usually for

nefarious purposes. A compromised computer or device, known as a **zombie**, is one whose owner is unaware the computer or device is being controlled remotely by an outsider.

A *bot* is a program that performs a repetitive task on a network. Cybercriminals install malicious bots on unprotected computers and devices to create a botnet. The perpetrator then uses the botnet to send spam via email, spread viruses and other malware, or commit a distributed denial of service attack.

How can you tell if your computer or mobile device is functioning as a zombie? Your computer or mobile device may be a zombie if you notice an unusually high drive activity, a slower than normal Internet connection, or connected devices becoming increasingly unresponsive. The chances of your computer or devices becoming part of a botnet greatly increase if your devices are not protected by an effective firewall.

A **denial of service attack** (**DoS attack**) is an assault whose purpose is to disrupt computer access to an Internet service, such as the web or email. Perpetrators carry out a DoS attack in a variety of ways. For example, they may use an unsuspecting computer to send an influx of confusing data messages or useless traffic to a computer network. The victim computer network slows down considerably and eventually becomes unresponsive or unavailable, blocking legitimate visitors from accessing the network.

A more devastating type of DoS attack is the *distributed DoS attack* (*DDoS attack*) in which a zombie army is used to attack computers or computer networks. DDoS attacks have been able to stop operations temporarily at numerous websites, including powerhouses such as Yahoo!, eBay, Amazon.com, and CNN.com.

The damage caused by a DoS or DDoS attack usually is extensive. During the outage, retailers lose sales from customers, news websites and search engines lose revenue from advertisers, and time-sensitive information may be delayed. Repeated attacks could tarnish reputations, causing even greater losses.

Why would someone execute a Dos or DDoS attack? Perpetrators have a variety of motives for executing a DoS or DDoS attack. Hactivists, or those who disagree with the beliefs or actions of a particular organization, claim political anger motivates their attacks. Some perpetrators use the attack as a vehicle for extortion. Others simply want the recognition, even though it is negative.

A **back door** is a program or set of instructions in a program that allows users to bypass security controls when accessing a program, computer, or network. Once perpetrators gain access to unsecure computers, they often install a back door or modify an existing program to include a back door, which allows them to continue to access the computer remotely without the user's knowledge. A rootkit can be a back door. Some worms leave back doors, which have been used to spread other worms or to distribute spam from the unsuspecting victim computers.

Programmers often build back doors into programs during system development. These back doors save development time because the programmer can bypass security controls while writing and testing programs. Similarly, a computer repair technician may install a back door while troubleshooting problems on a computer. If a programmer or computer repair technician fails to remove a back door, a perpetrator could use the back door to gain entry to a computer or network.

Spoofing is a technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network. Two common types of spoofing schemes are IP and email spoofing.

• *IP spoofing* occurs when an intruder computer fools a network into believing its IP address is associated with a trusted source. Perpetrators of IP spoofing trick their victims into

interacting with the phony website. For example, the victim may provide confidential information or download files containing viruses, worms, or other malware.

• *Email spoofing* occurs when the sender's address or other components of an email header are altered so that it appears that the email message originated from a different sender. Email spoofing commonly is used in virus hoaxes, spam, and phishing scams.

Unit 3. Antivirus Programs

Pre-Reading activities:

1. What precautions do you take to prevent viruses and other malware from infecting your computer? 2. What new steps will you take to attempt to protect your computer? 3. Which programs on your computer should have access to the Internet? Which programs should not?

1. a) Read the texts using the dictionary; b) translate the underlined words and word combinations into Ukrainian (in writing); c) pay attention to the terminological units in bold type. Be sure you can give their definition in English and their Ukrainian equivalents.

(1) Protection from Viruses and Other Malware

In addition to protecting against viruses and other malware, many antivirus programs also include protection from DoS and DDoS attacks. It is impossible to ensure a virus or malware never will attack a computer, but you can take several steps to protect your computer.

• Use **virus protection software**. Install a reputable antivirus program and then scan the entire computer to be certain it is free of viruses and other malware. Update the antivirus program and the **virus signatures,** i.e. known specific patterns of viruses, regularly.

• Use a **firewall**. Set up a hardware firewall or install a software firewall that protects your network's resources from outside **intrusions**.

• Be suspicious of all unsolicited email and text messages. Never open an email message unless you are expecting it, and it is from a trusted source. When in doubt, ask the sender to confirm the message is legitimate before you open it. Be especially cautious when deciding whether to tap or click links in email and text messages or to open attachments.

• Disconnect your computer from the Internet. If you do not need Internet access, disconnect the computer from the Internet. Some security experts recommend disconnecting from the computer network before opening email attachments.

• Download software with caution. Download programs or apps only from websites you trust, especially those with music and video sharing software.

• Close spyware windows. If you suspect a **pop-up** or **pop-under window** may be spyware, close the window. Never tap or click an Agree or OK button in a suspicious window.

• Before using any removable media, scan it for malware. Follow this procedure even for **shrink-wrapped software** from major developers. Some commercial software has been infected and distributed to unsuspecting users. Never start a computer with removable media inserted in the computer unless you are certain the media are uninfected.

• Keep current. Install the latest updates for your computer software. Stay informed about new **virus alerts** and **virus hoaxes**.

• Back up regularly. In the event your computer becomes unusable due to a virus attack or other malware, you will be able to restore operations if you have a clean (uninfected) backup.

How can you determine if your computer or mobile device is **vulnerable** to an Internet or network attack? You could use an **online security service,** which is a web app that evaluates your computer or mobile device to check for Internet and email vulnerabilities. The online security service then provides recommendations of how to address the vulnerabilities.

(2) Firewalls

A **firewall** is hardware and/or software that protects a network's resources from intrusion by users on another network, such as the Internet. All networked and online users should implement a firewall solution.

Organizations use firewalls to protect network resources from outsiders and to restrict employees' access to sensitive data, such as payroll or personnel records. They can implement

a firewall solution themselves or outsource their needs to a company specializing in providing firewall protection.

Large organizations often route all their communications through a **proxy server**, which typically is a component of the firewall. A proxy server is a server outside the organization's network that controls which communications pass in and out of the organization's network. That is, a proxy server carefully screens all incoming and outgoing messages. Proxy servers use a variety of screening techniques. Some check the domain name or IP address of the message for legitimacy. Others require that the messages have **digital signatures**.

Home and small/home office users often protect their computers with a personal firewall. A **personal firewall** is a software firewall that detects and protects a personal computer and its data from unauthorized intrusions. Personal firewalls constantly monitor all transmissions to and from the computer and may inform a user of any attempted intrusions. Both Windows and Mac operating systems include firewall capabilities, including monitoring Internet traffic to and from installed applications.

Some small/home office users purchase a hardware firewall, such as a router or other device that has a built-in firewall, in addition to or instead of a personal firewall. Hardware firewalls stop malicious intrusions before they attempt to affect your computer or network.

2. a) Read and translate the following chains of related words. Determine what part of speech they belong to.

1) intrude – intruder – intrusion – intrusive; 2) outsource – outsourcer – outsourced – outsourcing; 3) route – router – routed; 4) suspect – suspected – unsuspecting – suspicion – suspicious; 5) connect – connection – connector – connective – unconnected – disconnect; 6) use – user – usage – usable – unusable 7) infect – infection – infected – uninfected; 8) repute – reputation – reputed – reputedly – reputable; 9) capable – incapable – capability; 10) attach – attached – attachment.

b) Match the words and their synonyms.

1.	uninfected	a)	reliable
2.	reputable	b)	to safeguard
3.	to scan	c)	legal
4.	to determine	d)	to renew
5.	to protect	e)	unsanctioned
6.	legitimate	f)	to specify
7.	to restore	g)	to harm
8.	to implement	h)	to perform
9.	unauthorized	i)	clean
10.	to affect	j)	to examine

3. Translate the following word combinations.

a) into Ukrainian:

1) to monitor all transmissions to and from the computer; 2) to be certain the computer is free of viruses and other malware; 3) to implement a firewall solution; 4) how to address the vulnerabilities; 5) to inform a user of any attempted intrusions; 6) a web app that evaluates your computer or mobile device; 7) to screen all incoming and outgoing messages; 8) to become unusable due to a virus attack; 9) to scan removable media for malware; 10) to restrict employees' access to sensitive data.

b) into English:

1) апаратні брандмауери зупиняють шкідливі вторгнення; 2) перевіряти ім'я домену або IP-адресу; 3) надавати рекомендації; 4) контролювати, які з'єднання проходять у мережі організації та виходять з неї; 5) мати чисту резервну копію; 6) відновити роботу системи; 7) захищати комп'ютер від несанкціонованого вторгнення; 8) робити спроби вплинути на роботу комп'ютера чи мережі; 9) обмежувати доступ до конфіденційних даних; 10) пристрій, що має вбудований брандмауер.

4. Give the appropriate Ukrainian equivalents of the following words and word combinations (in writing).

1.	virus protection software	
2.	virus signature	
3.	proxy server	
4.	pop-up/ pop-under window	
5.	shrink-wrapped software	
6.	intrusion	
7.	virus alert	
8.	vulnerable	
9.	online security service	
10.	virus hoax	
11.	legitimacy	
12.	router	
13.	removable media	
14.	outsource	
15.	unsolicited email	
16.	self-replicate	
17.	directive	
18.	mainframe	
19.	threat actor	
20.	host program	

5. What do we call:

1) a software firewall that detects and protects a personal computer and its data from unauthorized intrusions; 2) a server outside the network that controls which communications pass in and out of the network; 3) a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication; 4) a new window that opens quickly on a computer screen in front of what you are working on; 5) a piece of electronic equipment that connects computer networks to each other, and sends information between networks; 6) a computer program that can make copies of itself and is intended to prevent the computer from working normally; 7) to purchase (goods) or subcontract (services) from an outside supplier or source; 8) to observe, check, keep under systematic review the progress or quality of (something) over a period of time; 9) the low-level software that supports a computer's basic functions, such as scheduling tasks and controlling peripherals; 10) a flaw in a computer system that can leave it open to attack.

6. a) Match the definitions with the following terms and terminological units.

1.	virus signature	a)	the part of a network address which identifies it as belonging to a particular domain

2.	pop-up window	b)	an additional window, usually an advertisement, that is under a Web browser's main or current window and appears when a user tries to exit
3.	domain name	c)	a piece of equipment which allows access to other computers or networks, for example the Internet
4.	firewall	d)	make (something) more modern or up to date
5.	pop-under window	e)	a browser window appearing without having been requested, esp. for the purpose of advertising
6.	digital signature	f)	a message warning the recipients of a non-existent computer virus threat. The message is usually a chain e-mail that tells the recipients to forward it to everyone they know
7.	router	g)	commercial, off-the-shelf software sold in retail, in contrast to the specially-developed (unique) software written by a firm's own or contracted programmers
8.	to update	h)	a digital code (generated and authenticated by public key encryption) that is attached to an electronically transmitted document to verify its contents and the sender's identity
9.	virus hoax	i)	a distinctive pattern or characteristic feature of malicious software/virus
10.	shrink-wrapped software	j)	a part of a computer system or network which is designed to block unauthorized access while permitting outward communication

7. Choose the correct answer.

1. According to the passage, a personal firewall is …
   a) a software that detects and protects a personal computer and its data from unauthorized intrusions.
   b) a hardware firewall, such as a router or other device.
   c) a malicious program that can execute itself and spreads by infecting other programs or files.
   d) a server outside the organization's network that controls which communications pass in and out of the organization's network.
2. Hardware and/or software that protects a network's resources from intrusion by users on another network, such as the Internet is …
   a) a domain name.
   b) a router.
   c) a firewall.
   d) a pop-up window.
3. Organizations use firewalls …
   a) to carefully screen all incoming and outgoing messages.
   b) to protect network resources from outsiders and to restrict employees' access to sensitive data.
   c) to start a computer with removable media inserted in the computer.
   d) to recommend disconnecting from the computer network before opening email attachments.
4. The word *legitimacy* in this text is closest in meaning to

a) “conformity to the law or to rules.”
b) “ability to be defended with logic or justification.”
c) “validity.”
d) “honesty”.

5. A web app that evaluates your computer or mobile device to check for Internet and email vulnerabilities is referred to as …
   a) an online security service.
   b) a proxy-server.
   c) a backup.
   d) a shrink-wrapped software.
6. The word *transmission* in the text is translated into Ukrainian as
   a) передача.
   b) пересилка.
   c) коробка передач.
   d) трансмісія.
7. The word *signature* in the text is closest in meaning to
   a) a person's name written in a distinctive way as a form of identification.
   b) a distinctive pattern by which a certain malware can be identified.
   c) the part of a medical prescription that gives instructions about the use of the medicine or drug prescribed.
   d) the action of signing a document.
8. According to the text, personal firewalls
   a) restore operations if you have an uninfected backup.
   b) carefully screen all incoming and outgoing messages.
   c) constantly monitor all transmissions to and from the computer and may inform a user of any attempted intrusions.
   d) ask the sender to confirm the message is legitimate before you open it.
9. Which is the best way to translate the following sentence:

Hardware firewalls stop malicious intrusions before they attempt to affect your computer or network.

   a) Апаратні брандмауери зупиняють шкідливі проникнення, перш ніж вони намагаються погано вплинути на ваш комп'ютер або мережу.
   b) Апаратні брандмауери зупиняють зловмисні вторгнення, перш ніж вони здійснять спробу зашкодити вашому комп'ютеру або мережі.
   c) Хардверні фаєрволи зупиняють злостиві вторгнення, до того як вони спробують вразити на ваш комп'ютер або мережу.
   d) Апаратні міжмережеві екрани зупиняють шкідливі втручання, перш ніж вони спробують вплинути на ваш комп'ютер або мережу.
10. The word combination *removable media* in the text is translated as:
   a) пересувні засоби масової інформації.
   b) рухомі середовища.
   c) знімні середовища.
   d) знімні носії інформації.

8. a) Render the following:
- in Ukrainian.

You probably don't actually need anyone to tell you just how important it is these days to download the best antivirus software possible for your computer and mobile devices.

Protecting yourself and ensuring that your laptop is virus free is possibly even more crucial in 2018 than ever before, owing to how much information we now store online. Cybercriminials and the viruses, malware, Trojan Horses and phishing scams they try to con us with aren't going anywhere soon – that's why it is extremely important for you to get the best antivirus in the world.

Hackers are always coming up with new ways to gain access to your PC and other internet enabled devices (with your mobile phone and tablet included). Luckily the best antivirus companies are constantly updating their security software packages. We're already starting to see their 2019 packages come to market, with user experience tweaks and the latest protection against phishing scams, ransomware and all other types of viruses and malware.

You want to make sure you get a complete suite of security tools that the best antivirus software can provide. If you're looking for all-round protection against the latest cyber threats, then investing in the best antivirus download is the best solution you can hope for in 2018. That doesn't mean you have to start spending big money either, as our guide also gives you the best available prices for your PC's protection.

- *in English*:*

Поряд зі зростанням кіберзлочинності та обсягом збитків за результатами атак, відбувається вдосконалення і розробка нових «бізнес-моделей» кіберзлочинів. Крім того, постійно стираються кордони в кіберпросторі, що дозволяє зловмисникам легше масштабувати свої атаки.

Наприклад, такий вид кібератак, як поширення вірусу-шифрувальника (Ransomware), до останнього часу вважався однією з найсерйозніших загроз кібербезпеки у світі, він дозволяє зловмисникам вимагати величезні суми грошей з компаній, які були заражені цим вірусом. Суть Ransomware полягає в тому, що це шкідливе програмне забезпечення (ПЗ) під час проникнення до системи шифрує дані та блокує їх, тим самим вимагачі отримують предмет торгу і суттєві аргументи на користь виплати їм необхідної суми. Навіть більше, стали з'являтися спеціальні RaaS-сервіси, які пропонують кріптоблокери для скачування з прихованого веб-сервера, доступні будь-якому бажаючому, для отримання доходу від вимагань у криптовалюті.

b) Consider this:

Do you use free antivirus software for your PC's protection or do you pay for it? Does free software provide a complete protection against the latest cybersecurity threats? Do you trust your free antivirus software? Are you ready to invest in your PC's protection?

8. a) Read the Information file below (use the dictionary if needed).
b) Be ready to explain which programs on your computer should have access to the Internet and which programs should not. Motivate your answer.

Information file

Set Up a Personal Firewall

A personal firewall is a program that helps protect your computer from unauthorized access by blocking certain types of communications. For example, if somebody knows the IP address of your computer and attempts to access it using a browser or other program, the personal firewall can be configured to deny the incoming connection. The following steps describe how to set up a personal firewall.

1. Locate and purchase a personal firewall. You can purchase personal firewalls online and in stores that sell software. Many operating systems include a personal firewall. Computers typically can have only one active personal firewall running at a time. If you

purchase a personal firewall, you may need to disable the one that is included with the operating system.

2. If you purchase a personal firewall, follow the instructions to install the program on your computer.

3. Run the personal firewall.

4. If necessary, ensure the personal firewall is enabled.

5. Review the settings for the incoming and outgoing rules. Incoming rules display programs and services that are allowed to access your computer. Outgoing rules display programs and services on your computer that are allowed to communicate with other computers and mobile devices on your network or the Internet.

6. Back up or export your current list of incoming and outgoing rules. If your computer does not function properly after you adjust the rules (in Steps 7 and 8), you will be able to restore the current rules.

7. Adjust your incoming rules to disallow devices, programs, and services you do not want accessing your computer. Be careful adjusting these settings, as adding or removing rules may hinder a legitimate program's capability to work properly.

8. Adjust your outgoing rules to allow only appropriate programs on your computer to communicate with other computers and mobile devices on your network or the Internet. Examples include a browser, email program, or other communications programs.

9. Save your settings.

10. Test programs on your computer that require Internet access. If any do not function properly, restore the list of rules you backed up or exported in Step 6.

11. Exit the personal firewall.

*c)** **Internet Research**

- Browse the free web resources to search for:

'The most popular antivirus programs';

- 'AVG, Intel Security, and Symantec (or any other security product developers)';

- Analyze the information you found and be ready to present the PowerPoint Presentation or written (oral) report, or 200-250-word essay (choose the form that suits you best):"The antivirus protection that keeps my own personal computer secure". Give reasons and all necessary details to motivate your choice.

9. a) Read the Information file below to learn about how to make the analysis of the antivirus products efficiency.*

Information file

What's the Best Malware Protection?

Which antivirus should you choose? You have a wealth of options. In our hands-on tests, Norton AntiVirus Basic outscored every other recent product except Webroot. A single subscription for McAfee AntiVirus Plus lets you install protection on all of your Windows, Android, Mac OS, and iOS devices. And its unusual behavior-based detection technology means Webroot SecureAnywhere Antivirus is the tiniest antivirus around. We've named these five commercial antivirus products, but they're not the only ones worth consideration. Read the reviews of our top-rated products, and then make your own decision.

Bitdefender Antivirus Plus

Pros: Outstanding scores in independent lab tests and our web protection tests. Multi-layered ransomware protection. Password manager. Banking protection. Offers a virtual private network, or VPN. Many security-centered bonus features.

Cons: Unlimited VPN access requires separate subscription. With antivirus disabled, ransomware-specific features missed one uncommon sample.

Bottom Line: With outstanding antivirus test results and a collection of features that puts some security suites to shame, Bitdefender Antivirus Plus is a top choice.

Symantec Norton AntiVirus Basic

Pros: Perfect scores in our malware and exploit protection tests. Best score in our malicious URL blocking test. Includes spam filter, password manager, and other bonus features.

Cons: First full scan unusually slow. Limited tech support.

Bottom Line: Symantec Norton AntiVirus Basic blows the tires off our hands-on tests, and it offers a large collection of bonus features. It remains an antivirus Editors' Choice.

Webroot SecureAnywhere AntiVirus

Pros: Perfect score in malware protection test. Light on system resources. Good scores in malicious and fraudulent URL tests. Ransomware protection. Fastest scan. Advanced features.

Cons: No lab test results.

Bottom Line: Small, speedy Webroot SecureAnywhere AntiVirus hardly uses any of your system's resources. It aces our hands-on malware protection test, and it can even roll back ransomware activity.

McAfee AntiVirus Plus

Pros: Cross-platform, multi-device protection. Good scores in hands-on tests. Includes firewall, file shredder, and many other bonus features.

Cons: Some so-so scores from independent labs. WebAdvisor's Site Report didn't work consistently in testing.

Bottom Line: A single subscription for McAfee AntiVirus Plus lets you protect every Windows, Android, macOS, and iOS device in your household. It's quite a deal.

Avast Pro Antivirus

Pros: Excellent scores in our hands-on tests. Good scores from independent labs. Wi-Fi inspector. Password manager. Numerous useful, security-related bonus features. Pro-only Sandbox and Real Site features.

Cons: Password manager features limited. Some bonus features require separate purchase. Pro-only features don't merit the price.

Bottom Line: Avast Pro Antivirus 2017 offers the same wealth of features as its free edition, and not a lot more. It's an excellent product, but for most people the free version will suffice.

ESET NOD32 Antivirus

Pros: Good scores from independent testing labs. New UEFI scanner finds malware in firmware. HIPS component blocks exploits. Speedy full scan. Comprehensive device control.

Cons: So-so phishing protection. Device control too complex for most users.

Bottom Line: ESET NOD32 Antivirus gets good scores in lab tests and our own tests, and its unusual new UEFI scanner can detect a malware infestation in your PC's firmware.

b) Consider This:

1) Which of the antivirus products mentioned above have you tried on your PC? Was it effective? 2) What antivirus software do you use to protect your PC now? What features of this software did you consider when making your choice? 3) After reading the passage above, which of the products analysed there would you choose to protect your PC (if you had to decide it right now)? Give your reasons. 4) Describe all pros and cons of the antivirus software you use now.

10. Write a short summary of the text 'Multilayered Malware Protection', p. 36 (see the scheme in ex.10, Unit 1).

Extended Reading

(1) Malware, Spyware, and Adware Protection

Hackers trying to affect election returns have an arsenal of tools. They can fool officials using directed fraudulent emails (called spear phishing), infect a horde of computers with bots that then participate in DDoS attacks on government sites, or install malware directly on voting machines. You can't do much about duped officials or hacked machines, but you can keep your own systems from being co-opted by installing and maintaining a powerful antivirus utility. How do you select the one that's best for you? We've thoroughly evaluated more than 40 antivirus tools; refer to our reviews and pick the one that's right for you.

We call it antivirus, but in truth it's unlikely you'll get hit with an actual computer virus. Malware these days is about making money, and there's no easy way to cash in on spreading a virus. Ransomware and data-stealing Trojans are much more common, as are bots that let the bot-herder rent out your computer for nefarious purposes. Modern antivirus utilities handle Trojans, rootkits, spyware, adware, ransomware, and more. PCMag has reviewed more than 40 different commercial antivirus utilities, and that's not even counting the many free antivirus tools. Out of that extensive field we've named five Editors' Choice products.

Several other commercial antivirus utilities proved effective enough to earn an excellent four-star rating. We eliminated two special-purpose products that aren't really like the rest: **The Kure** and VoodooSoft **VoodooShield**. Also, Check Point's **ZoneAlarm PRO** uses antivirus licensed from **Kaspersky**, with almost no lab test results for **ZoneAlarm** itself. That leaves the ten excellent products you see above. If you have malware, one of these products should do the job. All of them are traditional, full-scale, antivirus tools, with the ability to scan files for malware on access, on demand, or on schedule.

These commercial products offer protection beyond the antivirus built into Windows 10; the best free antivirus utilities also offer more. However, Microsoft Windows Defender Security Center is looking a bit better lately, with some very good scores from independent testing labs. In our hands-on tests, it showed a marked improvement since our previous review, enough to finally bring it up to three stars.

Listen to the Labs. We take the results reported by independent antivirus testing labs very seriously. The simple fact that a particular vendor's product shows up in the results is a vote of confidence, of sorts. It means the lab considered the product significant, and the vendor felt the cost of testing was worthwhile. Of course, getting good *scores* in the tests is also important. We follow four labs that regularly release detailed reports: SE Labs, AV-Test Institute, MRG-Effitas, and AV-Comparatives. We also note whether vendors have contracted with ICSA Labs and West Coast labs for certification. We've devised a system for aggregating their results to yield a rating from 0 to 10.

We Test Malware, Spyware, and Adware Defenses. We also subject every product to our own hands-on test of malware protection, in part to get a feeling for how the product works. Depending on how thoroughly the product prevents malware installation, it can earn up to 10 points for malware protection.

Our malware protection test necessarily uses the same set of samples for months. To check a product's handling of brand-new malware, we test each product using 100 extremely new malware-hosting URLs supplied by MRG-Effitas, noting what percentage of them it

blocked. Products get equal credit for preventing all access to the malicious URL and for wiping out the malware during download.

Some products earn absolutely stellar ratings from the independent labs, yet don't fare as well in our hands-on tests. In such cases, we defer to the labs, as they bring significantly greater resources to their testing. Want to know more? You can dig in for a detailed description of how we test security software.

(2) Multilayered Malware Protection

Antivirus products distinguish themselves by going beyond the basics of on-demand scanning and real-time malware protection. Some rate URLs that you visit or that show up in search results, using a red-yellow-green color-coding system. Some actively block processes on your system from connecting with known malware-hosting URLs or with fraudulent (phishing) pages.

Software has flaws, and sometimes those flaws affect your security. Prudent users keep Windows and all programs patched, fixing those flaws as soon as possible. The vulnerability scan offered by some antivirus products can verify that all necessary patches are present, and even apply any that are missing.

Spyware comes in many forms, from hidden programs that log your every keystroke to Trojans that masquerade as valid programs while mining your personal data. Any antivirus should handle spyware, along with all other types of malware, but some include specialized components devoted to spyware protection.

You expect an antivirus to identify and eliminate bad programs, and to leave good programs alone. What about unknowns, programs it can't identify as good or bad? Behavior-based detection can, in theory, protect you against malware that's so new researchers have never encountered it. However, this isn't always an unmixed blessing. It's not uncommon for behavioral detection systems to flag many innocuous behaviors performed by legitimate programs.

Whitelisting is another approach to the problem of unknown programs. A whitelist-based security system only allows known good programs to run. Unknowns are banned. This mode doesn't suit all situations, but it can be useful. Sandboxing lets unknown programs run, but it isolates them from full access to your system, so they can't do permanent harm. These various added layers serve to enhance your protection against malware.

Firewalls, Ransomware Protection, and More. Firewalls and spam filtering aren't common antivirus features, but some of our top products include them as bonus features. In fact, some of these antivirus products are more feature-packed than certain products sold as security suites.

Among the other bonus features you'll find are secure browsers for financial transactions, secure deletion of sensitive files, wiping traces of computer and browsing history, credit monitoring, virtual keyboard to foil keyloggers, cross-platform protection, and more. You'll even find products that enhance their automatic malware protection with the expertise of human security technicians. And of course we've already mentioned sandboxing, vulnerability scanning, and application whitelisting.

We're seeing more and more antivirus products adding modules specifically designed for ransomware protection. Some work by preventing unauthorized changes to protected files. Others keep watch for suspicious behaviors that suggest malware. Some even aim to reverse the damage. Given the growth of this scourge, any added protection is beneficial.

(https://www.pcmag.com/article2/0,2817,2372364,00.asp)

Unit 4. Authorized and Unauthorized Access and Use

4.1. Authorized Access

Pre-Reading Activity

1. Answer the questions.

1. What devices and objects are used to secure access to data and places? 2. What do you use your ATM bank card for? 3. How do you lock/unlock your smartphone? 4. What devices are called biometric? Where are they used?

2. a) Read and translate the texts using the dictionary. b) Translate the underlined words and word combinations into Ukrainian (in writing); c) Pay attention to the terminological units in bold type. Be sure you can give their definition in English and their Ukrainian equivalents.

Possessed Objects and Biometric Devices

A **possessed object** is any item that you must possess, or carry with you, in order to gain access to a computer or **computer facility**. Examples of possessed objects are badges, cards, smart cards, and keys. The card you use in an ATM (automated teller machine), for example, is a possessed object that allows access to your bank account.

A **biometric device** authenticates a person's identity by translating a personal characteristic, such as a fingerprint, into a digital code that is compared with a digital code stored in a computer or mobile device verifying a physical or behavioral characteristic. If the digital code in the computer or mobile device does not match the personal characteristic code, the computer or mobile device denies access to the individual.

Biometric devices grant access to programs, computers, or rooms using computer analysis of some **biometric identifier**. Examples of biometric devices and systems include fingerprint readers, face recognition systems, hand geometry systems, voice verification systems, signature verification systems, iris recognition systems, and retinal scanners.

A **fingerprint reader**, or fingerprint scanner, captures curves and indentations of a fingerprint. Organizations use fingerprint readers to secure doors, computers, and software. With the cost of fingerprint readers often less than $100, some home and small business users install fingerprint readers to authenticate users before they can access a personal computer.

The reader also can be set up to perform different functions for different fingers; for example, one finger starts a program and another finger shuts down the computer. External fingerprint readers usually plug into a USB port. Some laptops, smartphones, and smartwatches have a built fingerprint reader. Using their fingerprint, users can unlock the computer or device, sign in to programs and websites via their fingerprint instead of entering a user name and password, and on some devices, even test their blood pressure and heart rate.

A **lock screen** is a screen that restricts access to a computer or mobile device until a user performs a certain action. Some simply require a user to swipe the screen to unlock it. Others verify a user's identity by requiring entry of a password, PIN, or passcode, a fingerprint scan or a gesture swipe. Gestures are motions users make on a touch screen with the tip of one or more fingers or their hand. For example, to unlock the screen on a phone, a user could connect the dots on the screen using a pattern previously defined by the user.

A **face recognition system** captures a live face image and compares it with a stored image to determine if the person is a legitimate user. Some buildings use face recognition systems to secure access to rooms. Law enforcement, surveillance systems, and airports use face recognition to protect the public. Some mobile devices use face recognition systems to unlock

the device. Face recognition programs are becoming more sophisticated and can recognize people with or without glasses, makeup, or jewelry, and with new hairstyles.

A **hand geometry system** measures the shape and size of a person's hand. Because hand geometry systems can be expensive, they often are used in larger companies to track workers' time and attendance or as security devices. Colleges use hand geometry systems to verify students' identities. Daycare centers and hospital nurseries use them to identify parents who pick up their children.

A **voice verification system** compares a person's live speech with their stored voice pattern. Larger organizations sometimes use voice verification systems as time and attendance devices. Many companies also use this technology for access to **sensitive** files and networks. Some financial services use voice verification systems **to secure** phone banking transactions.

A **signature verification system** recognizes the shape of your handwritten signature, as well as measures the pressure exerted and the motion used to write the signature. Signature verification systems use a specialized pen and tablet. Signature verification systems often are used to reduce fraud in financial institutions.

High security areas use **iris recognition systems**. The camera in an iris recognition system uses iris recognition technology to read patterns in the iris of the eye. These patterns are as unique as a fingerprint. Iris recognition systems are quite expensive and are used by government security organizations, the military and financial institutions that deal with highly sensitive data. Some organizations use retinal scanners, which work similarly but instead scan patterns of blood vessels in the back of the retina.

3. Translate the following word combinations.

a) into Ukrainian:

1) to verify a physical or behavioral characteristic; 2) to translate a personal characteristic into a digital code; 3) to capture curves and indentations; 4) to set up a reader; 5) a tip of the finger; 6) to measure the shape and size; 7) back of the retina; 8) to verify students' identities; 9) to reduce fraud; 10) to deal with highly sensitive data.

b) into English:

1) забороняти/надавати доступ; 2) обмежувати доступ; 3) убезпечити доступ в приміщення; 4) проводити пальцем по екрану, щоб розблокувати екран; 5) відстежувати час роботи та відвідуваність працівників; 6) доступ до конфіденційних файлів і мереж; 7) для безпеки телефонних банківських операцій; 8) для ідентифікації батьків, які забирають своїх дітей; 9) для охорони дверей, комп'ютерів та ПЗ; 10) поєднувати точки на екрані, застосовуючи попередньо визначену користувачем схему.

4. Choose from the box appropriate Ukrainian equivalents to the following words and word combinations.

Комп'ютерна установка, екран блокування, жива мова, система розпізнавання райдужної оболонки ока, система розпізнавання мовця, система розпізнавання по геометрії долоні, система розпізнавання обличчя, пристрій для зчитування відбитків пальців, система перевірки справжності підпису, пристрій біометричної ідентифікації, код індивідуальної характеристики, ускладнений, власний об'єкт, підключити в USB порт, рух жестом, власноручний підпис, надзвичайно конфіденційна інформація, спеціальна ручка та планшет, система спостереження, вимкнути комп'ютер

1.	hand geometry system	
2.	signature verification system	

3.	computer facility	
4.	to shut down the computer	
5.	possessed object	
6.	live speech	
7.	specialized pen and tablet	
8	lock screen	
9.	handwritten signature	
10.	biometric identifier	
11.	sophisticated	
12.	iris recognition system	
13.	personal characteristic code	
14.	voice verification system	
15.	plug into a USB port	
16.	face recognition system	
17.	surveillance system	
18.	fingerprint reader	
19.	highly sensitive data	
20.	gesture swipe	

5. What do we call:

1) a system that measures the shape and size of a person's hand; 2) the opaque contractile diaphragm perforated by the pupil and forming the colored portion of the eye; 3) kept secret or with restrictions on disclosure to avoid endangering security; 4) a technology to read patterns in the iris of the eye; 5) a system that compares a person's live speech with their stored voice pattern; 6) a system captures a live face image and compares it with a stored image to determine if the person is a legitimate user; 7) a device that captures curves and indentations of a fingerprint; 8) a screen that restricts access to a computer or mobile device until a user performs a certain action; 9) a device that authenticates a person's identity by translating a personal characteristic, such as a fingerprint, into a digital code; 10) the impression of a fingertip on any surface.

6. Choose the correct answer.

1. According to the passage, ...
   a) there are not many ways to secure data;
   b) possessed objects are biometric identifiers;
   c) biometric devices include a hand geometry system, a signature verification system, an iris recognition system, a voice verification system, a face recognition system and a fingerprint reader;
   d) biometric devices are costly, that's why they are used by few people.
2. The word *sophisticated* in the text is closest in meaning to:
   a) complex; b) beautiful; c) fine; d) intellectually appealing.
3. Signature verification systems often are used…
   a) to verify students' identities;
   b) to reduce fraud in financial institutions;
   c) to secure phone banking transactions;
   d) to identify parents who pick up their children.
4. The word with the opposite meaning to the word *sensitive*:

a) secret; b) delicate; c) easily upset; d) known about.

5. People don't use their fingerprint while using a built fingerprint reader to:
   a) unlock the computer or device;
   b) sign in to programs and websites;
   c) test their blood pressure and heart rate;
   d) scan patterns of blood vessels in the back of the retina.
6. Signature verification systems use…
   a) a specialized pen and tablet;
   b) a smartwatch;
   c) a pen and a notebook;
   d) some red ink.
7. According to the passage, ...
   a) biometric devices are widely used at many organizations for many purposes;
   b) biometric passports are being issued in Ukraine;
   c) there are still organizations that hesitate implementing biometric devices;
   d) fingerprints are the same on all five fingertips.
8. … is an affordable biometric device and can be easily installed at home.
   a) an iris recognition system;
   b) a hand geometry system;
   c) a fingertip reader;
   d) a signature verification system.
9. Which is the best way to translate the following sentence:

A signature verification system recognizes the shape of your handwritten signature, as well as measures the pressure exerted and the motion used to write the signature.

a) Система підтвердження підпису визнає форму вашого власноручного підпису, а також вимірює тиск і рух, який використовується для написання підпису.

b) Система перевірки справжності підпису розпізнає форму вашого рукописного підпису, а також вимірює докладений натиск і розчерк, який використовується для написання підпису.

c) Система підтвердження підпису вивчає форму вашого рукописного підпису, а також тиск і рух, який використовується для написання підпису.

d) Система підтвердження підпису вимірює форму вашого рукописного підпису, а також тиск і рух, який використовується для написання підпису.

10. Biometric data are:
   a) sophisticated;
   b) unique;
   c) dependent on the personality type;
   d) easy to obtain.

7. a) Translate the following sentences:

- into Ukrainian.

1. Biometric data cannot be lent and hacking of Biometric data is complicated hence it makes it safer to use than traditional methods of authentication like passwords which can be lent and shared. 2. Passwords don't have the ability to judge the user but rely only on the data provided by the user, while Biometrics works on the uniqueness of each individual. 3. Passwords can be forgotten and recovering them can take time, whereas Biometric devices rely on biometric data, which tends to be unique to a person, hence there is no risk of forgetting the authentication data. 4. Passwords are still extremely popular because a password

is static in nature while Biometric Data can be subject to change (person's voice becoming heavier due to puberty, accidents to the face could lead to improper reading of facial scan data). 5. Accuracy is a major issue with Biometric Devices and a major reason why corporations and people are hesitant to implement them deeper into their working. 6. Biometric spoofing is a method of fooling a biometric identification management system, where a counterfeit mold is presented in front of the biometric scanner. 7. This counterfeit mold emulates the unique biometric attributes of an individual so as to confuse the system between the artifact and the real biological target and gain access to sensitive data/materials. 8. Researchers are targeting the drawbacks of present-day biometric devices and developing to reduce problems like biometric spoofing and inaccurate intake of data. 9. Using the principle of pulse oximetry the liveliness of the test subject is taken into account by measure of blood oxygenation and the heart rate. 10. These methods aren't commercially applicable as costs of implementation are high that reduces their real world application and hence makes biometrics insecure until these methods are commercially viable.

- *into English*

1. Біометричні прилади – пристрої безпеки, за якими ідентифікація особи здійснюється за допомогою індивідуальних фізіологічних характеристик (відбитки пальців, малюнок сітківки ока, тембр голосу, підпис). 2. Біометричні замки діють за допомогою сенсора, який сканує необхідну для ідентифікації ділянку і дозволяє або обмежує доступ. 3. Особливість біометричного паспорта в тому, що це посвідчення особи містить електронний носій даних, на якому вписано інформацію про біометричні показники власника документа з метою його ідентифікації. 4. Дана технологія активно використовується в міжнародних аеропортах, на водійських правах, в паспортах з біометричною ідентифікацією, а в деяких країнах навіть для голосування на виборах. 5. Майже третина сучасних ноутбуків оснащена вбудованою системою зчитування відбитків пальця. 6. Між частинами обличчя обчислюється відстань і будується множина варіантів у залежності від повороту обличчя, нахилу, зміни міміки. 7. При скануванні сітківки ока всередину ока направляється пучок світла (іноді інфрачервоного), а обличчя повинно бути розташоване з високою точністю відносно сканера, що вважається одним із недоліків методу. 8. Малюнок райдужної оболонки ока абсолютно унікальний. 9. Біометричні пристрої доцільно використовувати у системах захисту інформації. 10. Дактилоскопічна система *Futronic* складається з напівпровідникового сканеру розміром із сірникову коробку та з програми, вбудованої у меню входу до операційної системи, які виконують ідентифікацію користувачів за відбитком пальця та вводом паролю через клавіатуру.

8. a) Read the Information file below (use the dictionary if needed).

Information file

How popular are biometric devices?

Biometric devices are gaining popularity as a security precaution because they are a virtually foolproof method of identification and authentication. For example, some grocery stores, retail stores, and gas stations use biometric payment, where the customer's fingerprint is read by a fingerprint reader that is linked to a payment method, such as a checking account or credit card. Users can forget their user names and passwords.

Possessed objects can be lost, copied, duplicated, or stolen. Personal characteristics, by contrast, are unique and cannot be forgotten or misplaced. Biometric devices do have disadvantages. If you cut your finger, a fingerprint reader might reject you as a legitimate user. Hand geometry readers can transmit germs. If you are nervous, a signature might not

match the one on file. If you have a sore throat, a voice recognition system might reject you. Many people are uncomfortable with the thought of using an iris scanner.

b) Consider this:

1. Where are biometric devices widely used? 2. Why are biometric devices so popular now? Motivate your answer. 3. What are the main advantages of biometric methods? 4. Are there any disadvantages of these methods? Describe them. 5. Do you use any of biometric methods? When? What gadgets do you use for that?

9. a) Read the Information file below and determine the verification steps.

Information file

Two-Step Verification

In an attempt to further protect personal data and information from online thieves, many organizations such as financial institutions or universities that store sensitive or confidential items use a two-step verification process. With two-step verification, also known as *two-factor verification*, a computer or mobile device uses two separate methods, one after the next, to verify the identity of a user.

ATMs (automated teller machines) usually require a two-step verification. Users first insert their ATM card into the ATM (Step 1) and then enter a PIN (Step 2) to access their bank account. Most debit cards and some credit cards use PINs. If someone steals these cards, the thief must enter the user's PIN to access the account.

Another use of two-step verification requires a mobile phone and a computer. When users sign in to an account on a computer, they enter a user name and a password (Step 1). Next, they are prompted to enter another authentication code (Step 2), which is sent as a text or voice message or via an app on a smartphone. This second code generally is valid for a set time, sometimes only for a few hours. If users do not sign in during this time limit, they must repeat the process and request another verification code. Microsoft and Google commonly use two-step verification when you sign in to their websites. If you sign in from a device you use frequently, you can elect to bypass this step.

Users should register a landline phone number, alternate email address, or other form of contact beyond a mobile phone number so that they still can access their accounts even if they lose their mobile phone.

b) Consider this:

1. What is a two-step verification? Describe the process, giving examples. 2. Can users circumvent the two-step verification process? Why/ Why (not)?

c) Internet Research*

- Browse the free web resources to search for two-step verification websites.

- Analyze the information you found and be ready to present the results of your research in class in the form of oral presentation / written (oral) report / 200-250-word essay (choose the form that suits you best).

10. Write a short summary of the text 'Techniques for face acquisition', p. 48 (see the scheme in the box: ex.10, Unit 1).

4.2. Unauthorized Access

Pre-Reading activities:

1. Do you use a password manager? 2. If so, do you feel secure storing all your sign in and password information in this service? 3. If not, how do you keep track of your passwords?

11. a) Read and translate the texts using the dictionary; b) translate the underlined words and word combinations into Ukrainian (in writing); c) pay attention to the terminological units in bold type. Be sure you can give their definition in English and their Ukrainian equivalents.

Unauthorized access is the use of a computer or network without permission. **Unauthorized use** is the use of a computer or its data for unapproved or possibly illegal activities.

Home and business users can be a target of unauthorized access and use. Unauthorized use includes a variety of activities: an employee using an organization's computer to send personal email messages, an employee using the organization's word processing software to track his or her child's soccer league scores, or a **perpetrator** gaining access to a bank computer and performing an unauthorized transfer.

Safeguards against Unauthorized Access and Use

Organizations take several measures to prevent unauthorized access and use. At a minimum, they should have a written **acceptable use policy (AUP)** that outlines the activities for which the computer and network may and may not be used. An organization's AUP should specify the acceptable use of technology by employees for personal reasons.

Some organizations prohibit such use entirely. Others allow personal use on the employee's own time, such as a lunch hour. Whatever the policy, an organization should document and explain it to employees. The AUP also should specify the personal activities, if any, that are allowed on company time. For example, can employees check personal email messages or respond to personal text messages during work hours? To protect your personal computer from unauthorized **intrusions**, you should disable file and printer sharing in your operating system. This security measure attempts to ensure that others cannot access your files or your printer. You also should be sure to use a firewall.

There are other techniques for protecting against unauthorized access and use. The technique(s) used should correspond to the **degree of risk** that is associated with the unauthorized access.

Access Controls

Many organizations use **access controls** to minimize the chance that a perpetrator intentionally may access or an employee accidentally may access confidential information on a computer, mobile device, or network. An *access control* is a security measure that defines who can access a computer, device, or network; when they can access it; and what actions they can take while accessing it. In addition, the computer, device, or network should maintain an **audit trail** that records in a file both successful and unsuccessful access attempts. An unsuccessful access attempt could result from a user mistyping his or her password, or it could result from a perpetrator trying thousands of passwords.

Organizations should investigate unsuccessful access attempts immediately to ensure they are not intentional breaches of security. They also should review successful access for irregularities, such as use of the computer after normal working hours or from remote

computers. The security program can be configured **to alert** a security administrator whenever suspicious or irregular activities are suspected. In addition, an organization regularly should review users' **access privilege** levels to determine whether they still are appropriate.

12. a) Match the words and their synonyms.

1.	to determine	a)	to warn
2.	to alert	b)	worker
3.	employee	c)	violation
4.	breach	d)	to trail
5.	to track	e)	to define

b) find in the text and write the antonyms of the following:

1.	appropriate	
2.	to prohibit	
3.	approved	
4.	legal	
5.	successful	
6.	regularity	
7.	authorized	
8.	intentional	
9.	to enable	

13. Translate the following word combinations.

a) into Ukrainian:

1) to result from a perpetrator trying thousands of passwords; 2) to respond to personal text messages during work hours; 3) to accidentally access confidential information on a computer, mobile device, or network; 4) the organization's word processing software; 5) to specify the personal activities, if any; 6) use of technology by employees for personal reasons; 7) to review successful access; 8) suspicious or irregular activities; 9) to use a computer or network without permission; 10) to determine whether they still are appropriate.

b) into English:

1) неправильно набирати пароль; 2) зменшити шанси зловмисника; 3) невдалі спроби доступу; 4) користування комп'ютером після завершення робочого часу; 5) визначати, хто може мати доступ до комп'ютера, пристрою чи мережі; 6) мати доступ до конфіденційної інформації; 7) заходи безпеки; 8) одержати несанкціонований доступ до банківського комп'ютера; 9) підозрювати про неправомірні дії; 10) повідомляти адміністратора системи безпеки.

14. Write the appropriate Ukrainian equivalents to the following words and word combinations.

1.	unauthorized access	
2.	audit trail	
3.	to alert	
4.	acceptable use policy (AUP)	
5.	access controls	
6.	perpetrator	
7.	access privilege	
8.	unauthorized use	

9.	intrusion	
10.	degree of risk	

15. What do we call:

1) any unauthorized activity on a computer network, particularly when it threatens security; 2) a series of records of computer events, about an operating system, an application, or user activities; 3) a person who carries out a harmful, illegal, or immoral act; 4) the delegation of authority over a computer system, such as the ability to create a file in a directory, or to read or delete a file, access a device, or for communicating over the Internet, etc.; 5) extent or level of uncertainty in a given situation; 6) a document stipulating constraints and practices that a user must agree to for access to a corporate network or the Internet; 7) a process by which users are granted access and certain privileges to systems, resources or information.

16. Choose the correct answer.

1. According to the passage, unauthorized access is …
   a) the use of a computer or network without permission.
   b) the use of a computer or its data for unapproved activities.
   c) an unsuccessful access attempt.
   d) a successful access attempt.
2. A security measure that defines who, can access a computer or network; when they can access it; and what they can do while accessing it, is …
   a) a domain name.
   b) a router.
   c) an access control.
   d) a pop-up window.
3. Organizations should investigate unsuccessful access attempts immediately …
   a) to ensure they are not intentional breaches of security.
   b) to respond to personal text messages during work hours.
   c) to start a computer with removable media inserted in the computer.
   d) to alert a security administrator whenever unsuccessful access attempts are suspected.
4. The word *intrusion* in this text is closest in meaning to
   a) “unauthorized access with the aim of malicious activity or violations.”
   b) “an illegal act of entering, seizing, or taking possession of another's property.”
   c) “forcing a body of igneous rock between existing formations, without reaching the surface.”
   d) “offence, crime”.
5. The use of a computer or its data for unapproved or possibly illegal activities is referred to as …
   a) an online security service.
   b) a unauthorized use.
   c) a backup.
   d) an invasion.
6. The word *perpetrator* in the text is translated into Ukrainian as
   a) перпетратор.
   b) виконавець.
   c) порушник.
   d) зловмисник.

7. The word *safeguard* in the text is closest in meaning to
   a) convoy, guard.
   b) precaution.
   c) cutout, pawl, protector.
   d) safe conduct.
8. According to the text, an access control…
   a) is a security measure that defines who, when and why can access a computer, device, or network.
   b) records in a file both successful and unsuccessful access attempts.
   c) should specify the personal activities, if any, that are allowed on company time.
   d) outlines the activities for which the computer and network may and may not be used.
9. Which is the best way to translate the following sentence:

The security program can be configured to alert a security administrator whenever suspicious or irregular activities are suspected.

   a) Програма безпеки може бути конфігурована стривожити адміністратора безпеки, коли б не підозрювалися підозрілі або аморальні дії.
   b) Охоронна програма може бути налагоджена на приведення у стан готовності адміністратора безпеки, коли підозрюються підозрілі або неправильні заходи.
   c) Програма контролю безпеки може бути налаштована повідомляти адміністратора системи безпеки про підозрілу чи нестандартну активність.
   d) Безпечна програма може бути сконфігурована попереджати безпечного адміністратора, якщо підозріла чи нерегулярна діяльність підозрюється.
10. The word combination *degree of risk* in the text is translated as:
   a) ступінь ризику.
   b) градус ризику.
   c) ранг ризику.
   d) звання ризику.

17. a) Render the following:

- in Ukrainian.

Unauthorized access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a password or username for an account that was not theirs until they gained access it is considered unauthorized access. Unauthorized access could also occur if a user attempts to access an area of a system they should not be accessing. When attempting to access that area, they would be denied access and possibly see an unauthorized access message.

Some system administrators set up alerts to let them know when there is an unauthorized access attempt, so that they may investigate the reason. These alerts can help stop hackers from gaining access to a secure or confidential system. Many secure systems may also lock an account that has had too many failed login attempts. It should be noted that if you have gained unauthorized access to any account or service it is considered illegal in all parts of the world.

Most users are interested in taking steps to prevent others from accessing their computer. Whether you wish to protect yourself from malware or to ensure that your private information is safe, having a secure computer can definitely provide peace of mind.

- in English:*

Найчастіше питання про те, як захистити комп’ютер від вірусів або від несанкціонованого доступу виникає у людей тільки після того, як вони на власному

досвіді переконуються в тому, що якщо комп'ютер не має захисту, то це загрожує непоправними і неприємними наслідками. Користувачі помиляються, коли думають, що антивірусне програмне забезпечення здатне захистити персональний комп'ютер від усіх вірусів. Хибними є також висновки про той чи інший «антивірусник», коли їх комп'ютер усе одно заражається шкідливим кодом. Однак, треба усвідомлювати, що антивірусна система захищає лише від тих вірусів, які їй відомі. Тобто новий вірус повинен заразити хоча б один комп'ютер, на якому встановлене антивірусне ПЗ. Тоді антивірусна програма повинна або сама виявити підозрілий файл, відправивши його розробникам, або це повинен зробити сам користувач. Тепер розробник повинен проаналізувати отримані дані і знайти так звані «ліки». І лише після цього «ліки» доходять до вас у вигляді оновлення антивірусної програми. Потрібно близько 7 днів з моменту відправки підозрілих файлів до антивірусної компанії, щоб нові елементи захисту з'явилися в базах антивірусної програми. З одного боку це досить швидко, але з іншого – цього цілком достатньо, щоб заразити щонайменше кілька тисяч комп'ютерів, серед яких може опинитися і ваш. Отже, сама лиш антивірусна програма – далеко не ідеальний засіб захисту комп'ютера.

b) Consider this:*

1. If antivirus program only is not enough to secure your system from unauthorized access or viruses, what else should be done to keep your PC safe? 2. How to prevent unauthorized computer access to be sure your system is protected? Consider various ways (e.g., hardware and software firewalls, passwords, handling e-mails with care, system and software patches and updates, system scanning for vulnerabilities, two-factor authentication, etc.).

*c)** **Internet Research**

- Browse the free web resources to search for: 'How to protect the computer from unauthorized access'.

- Analyze the information you found and be ready to present the written (oral) report, or 200-250-word essay (choose the form that suits you best):"What keeps my own personal computer secure". Give reasons and all necessary details to motivate your choice.

18. Write a short summary of the text 'Digital forensics', p. 47 (see the scheme in ex.10, Unit 1).

Extended Reading

(1) Digital forensics

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data. With roots in the personal computing revolution of the late 1970s and early 1980s, the discipline evolved in a haphazard manner during the 1990s, and it was not until the early 21st century that national policies emerged.

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil (as part of the electronic discovery process) courts. Forensics may also feature in the private sector; such as during internal

corporate investigations or intrusion investigation (a specialist probe into the nature and extent of an unauthorized network intrusion).

The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved; computer forensics, network forensics, forensic data analysis and mobile device forensics. The typical forensic process encompasses the seizure, forensic imaging (acquisition) and analysis of digital media and the production of a report into collected evidence.

As well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources (for example, in copyright cases), or authenticate documents. Investigations are much broader in scope than other areas of forensic analysis (where the usual aim is to provide answers to a series of simpler questions) often involving complex time-lines or hypotheses.

A digital forensics examiner must have knowledge of the law, technical experience with many types of hardware and software products, superior communication skills, familiarity with corporate structures and policies, willingness to learn and update skills, and a knack for problem solving.

(2) Techniques for face acquisition

Some face recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Other algorithms normalize a gallery of face images and then compress the face data, only saving the data in the image that is useful for face recognition. A probe image is then compared with the face data. One of the earliest successful systems is based on template matching techniques applied to a set of salient facial features, providing a sort of compressed face representation.

Recognition algorithms can be divided into two main approaches: geometric, which looks at distinguishing features, and photometric, which is a statistical approach that distills an image into values and compares the values with templates to eliminate variances.

A newly emerging trend, claimed to achieve improved accuracy, is three-dimensional face recognition. This technique uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin. One advantage of 3D face recognition is that it is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles, including a profile view. Three-dimensional data points from a face vastly improve the precision of face recognition. 3D research is enhanced by the development of sophisticated sensors that do a better job of capturing 3D face imagery. The sensors work by projecting structured light onto the face. Up to a dozen or more of these image sensors can be placed on the same CMOS chip – each sensor captures a different part of the spectrum...

Even a perfect 3D matching technique could be sensitive to expressions. For that goal a group at the *Technion* applied tools from metric geometry to treat expressions as isometries.

A different form of taking input data for face recognition is by using thermal cameras, by this procedure the cameras will only detect the shape of the head and it will ignore the subject accessories such as glasses, hats, or make up. A problem with using thermal pictures for face recognition is that the databases for face recognition is limited.

(https://en.wikipedia.org/wiki/Facial_recognition_system)

(3) How to protect yourself while on the Internet

(by Computer Hope)

Below are all of the steps and suggestions everyone should follow to keep their computers and their personal information safe while being connected to the Internet.

Verify data is encrypted. When sending confidential information over the Internet, such as usernames, passwords, or credit card numbers, only send it securely. To verify this, look for a small lock in the bottom right corner of your browser window or next to the address bar. If visible, this lock should also be in the locked position and not unlocked.

Secure address bar. We also suggest making sure the URL begins with *https*. While the lock is in the locked position, data is encrypted, which helps anyone from understanding the data if it's intercepted. When no lock is visible or it is in the unlocked position, all information is plain text and could be read if intercepted. If a web page is not secure, such as an online forum, use a password you wouldn't use with protected sites, such as your online banking website.

Use a safe password. Websites that store confidential data, such as an online bank site, need to use strong passwords. Also, it is highly recommended that you use a different password for each website that requires a login.

Two-factor authentication adds additional protection by requiring an additional step in verifying a login. Typically with two-factor authentication, after verifying your password, if the service does not recognize your computer, it sends your phone a text message with a verification code. If someone had your password but did not have your phone, even with a valid password, they cannot access your account.

Keep your operating system and software up-to-date. Many of the updates that are released by developers of operating systems are related to computer security-related issues. Make sure your operating system is always running the latest updates and that you're running an operating system that is still supported by the developer.

Always be cautious of e-mail links and attachments. One of the most common methods of spreading viruses and malware is through e-mail attachments and hyperlinks sent through e-mail. Always be extremely cautious when dealing with any attachments or links in e-mails you've received from anyone (even friends and family). Never transmit confidential data over e-mail, such as passwords, credit card information, etc. E-mail is not encrypted, and if intercepted by a third-party, it could be read.

Be aware of phishing scams. Familiarize yourself with phishing scams and techniques, which are used to trick you into divulging your account information. Online banking sites, *Paypal, eBay, Amazon*, and other popular sites that require logins are popular targets.

Use caution when accepting or agreeing to prompts. When you're prompted to install any program or add-on, make sure to read and understand the agreement before clicking on the ‘Ok’ button. If you do not understand the agreement or feel it is not necessary to install the program, cancel or close the window. Additionally, when installing any program, watch for any check box that asks if it's ok to install a third-party program, toolbar, etc. These are never required and often cause more issues than good.

Be cautious where you're logging in from. Your place of work can install key loggers or use other methods of monitoring the computer while online. Someone who has access to this information could read these logs and gather usernames and passwords. Also, do not store any passwords in your browser if your computer is shared with other co-workers.

Wireless network. When on a wireless network, realize that all information being sent to and from your computer can be intercepted and read by someone nearby. Prevent this from happening by only logging onto a secure network. If this is a home wireless network, make sure it is secure.

Friends house. Be concerned when logging into an account on a friend's computer. A computer or network you are not familiar with could intentionally or unintentionally log usernames and passwords. Finally, when logging into any site on a friend's computer, never save the password information on their browser.

Use an alternative browser. Older versions of Internet Explorer are notoriously insecure. If you are using Internet Explorer as your browser, consider an alternative browser such as Google Chrome or Mozilla Firefox.

Always think before you share something. Social networking sites like Facebook are a great place to connect with friends and family online. However, it is also very easy for people to overshare personal information about themselves or others. Before sharing something on a social network or any place on the Internet make sure it is something you wouldn't mind if everyone saw. Everything you share on the Internet should be thought of as public because it is possible for something you believe is shared privately to be leaked out publicly. If you're thinking about sharing something you think could offend someone or embarrass you if someone else saw maybe you should not share it on the Internet.

Be aware of those around you. While at work, school, library, or anywhere in the public that has people around you that could look at your screen, be cautious of anyone shoulder surfing. Someone could watch you type in your password, which would give them access to your account. If you need information displayed on the screen to remain private, consider a privacy filter for the display.

Secure saved passwords. Make sure to store passwords and login information in a secure area. Never write login information on a sticky note or in a text file that is not encrypted. When saving password information in a browser, it may be visible to anyone who has access to your Internet browser. For example, without a master password setup in Firefox, anyone can see all stored passwords.

Protect yourself against malware, spyware, and viruses. Protect your computer from viruses by installing an anti-virus program on the computer. If you do not want to install anti-virus protection and your computer is running a newer version of Windows, at least have Windows Defender running on the computer.

Verify the checksum of downloaded files. If you've downloaded a program from a website that also lists a file checksum, make sure the checksum matches the file that you've downloaded. Verifying the checksum of a downloaded program can help verify that the program you are installing is what you want to install.

Don't always trust what you read online. Realize that it's possible for anyone to create a website on the Internet and that someone may only be creating a site for malicious intentions. For example, a website could be created to help spread fear, lies, or malware.

Unit 5. User Names and Passwords

Pre-Reading activities:

1. Do you use a password manager? 2. If so, do you feel secure storing all your sign-in and password information in this service? 3. If not, how do you keep track of your passwords?

1. a) Read the texts using the dictionary; b) translate the underlined words and word combinations into Ukrainian (in writing); c) pay attention to the terminological units in bold type. Be sure you can give their definition in English and their Ukrainian equivalents.

A **user name –** also called a **user ID** (identification), **log-on name**, or **sign-in name** – is a unique combination of characters, such as letters of the alphabet or numbers, that identifies one specific user. When you enter your user name into a **single sign on (SSO)** account, such as for Microsoft, Google, Twitter, and Facebook, you automatically are signed in to other accounts and services. Many also recognize your information to provide additional customized content.

A **password** is a private combination of characters associated with the user name that allows access to certain computer resources.

Most operating systems that enable multiple users to share computers and devices or that access a home or business network require users to enter a user name and a password correctly before they can access the data, information, and programs stored on a computer, mobile device, or network. Many systems that maintain financial, personal, and other confidential information also require a user name and password as part of their sign-in procedure.

Some systems assign a user name and/or password to each user. For example, a school may use a combination of letters from a student's first and last names as a user name, e.g.*, Brittany Stearn's user name might be 'stearns_brit'. Some websites use your email address as the user name. Information technology (IT) departments may assign passwords so that they have a record in case the employee leaves or forgets the password.

With other systems, users select their own user names and/or passwords. Many users select a combination of their first and last names for their user names. Many online social networks, media sharing sites, and retail and other websites allow you to choose your own user name. You might select a name that is formed from parts of your real name or **nickname** and possibly some numbers, if the name you want is taken. If you wish to remain more anonymous, choose a user name that combines common words, or reflects your interests (such as guitarboston27).

Once you select a password, change it frequently. If a program or device has **a default or preset password**, such as admin, be sure to change it to prevent unauthorized access. Do not **disclose** your password to anyone or write it on a slip of paper kept near the computer, especially taped to the monitor or under the keyboard. Email and telemarketing scams often ask unsuspecting users to disclose their credit card numbers, so be **wary** if you did not **initiate the inquiry** or phone call.

Safe Use of a Password Manager

If you use the same password to access your banking, shopping, online social networks, and school accounts, you are not alone. Many people think one password is sufficient protection for all their vital online **accounts**, but **cyberthieves** are aware of this flawed thinking and take advantage of this practice. Security experts recommend using different user names and passwords for every account and changing the passwords frequently.

Keeping track of all these accounts can be an overwhelming task. A **password manager**, also called a password organizer, is a convenient service that stores all your account information securely. Once you select a service, you download and install the software and create one **master password**. The first time you view a password-protected website and enter your user name and password, the password manager saves this information. The next time you visit one of these websites or apps, the software supplies the account information automatically. Password managers use two-step verification and advanced encryption techniques to ensure information is stored securely.

Some managers offer the option to generate random passwords, which have a unique combination of jumbled numbers and letters that are difficult for criminals to steal, for each account. Other features include the ability to auto-fill information, such as your name, address, and phone number, on forms and **to provide a hint** if you have forgotten your master password. For example, in addition to a user name and password, some systems ask users to enter some personal information, such as your mother's first name, your favorite food, your first pet's name, etc. These items should be facts that you easily remember but are not easy for others to discover about you when using a search engine or examining your profiles on online social networks. As with a password, if the user's response does not match information on file, the system denies access.

Password manager services can be free to use or may require a small annual fee. Some security experts recommend using a service that charges a fee, stating that these companies may provide more features. Before using any manager, call the company and ask about security measures, the ability to sync with multiple mobile devices, 24-hour customer service via **live chat** or phone, and limits on the number of passwords that can be saved.

*e.g. – for example (from Lat. *exempli gratia*)

2. a) Read and translate the following chains of related words. Determine what part of speech they belong to.

1) provide – provider – provision; 2) inform – informer – informed – information; 3) generate – generator – generation; 4) use – user – usage – useful – usable – unusable; 5) verify – verified – verification; 6) protect – protector – protection – protected; 7) select – selection – selected – selectivity; 8) assign – assignment; 9) convenient – convenience – inconvenience – conveniently; 10) possible – impossible – possibility – possibly.

b) Match the words and their synonyms.

1.	random	a)	intimation
2.	hint	b)	to divulge
3.	to require	c)	secret
4.	to verify	d)	careful
5.	to disclose	e)	muddle
6.	confidential	f)	to produce
7.	to generate	g)	to demand
8.	to assign	h)	to appoint
9.	jumble	i)	haphazard
10.	wary	j)	to confirm

3. Translate the following word combinations.

a) into Ukrainian:

1) to sync with multiple mobile devices; 2) to deny access; 3) to choose a user name that combines common words, or reflects your interests; 4) limits on the number of passwords that can be saved; 5) to take advantage of something; 6) the software supplies the account information automatically; 7) to store all your account information securely; 8) to enter a user name and a password correctly; 9) to require a small annual fee; 10) the ability to auto-fill information.

b) into English:

1) унікальна комбінація довільних букв та цифр; 2) вдосконалена методика шифрування; 3) призначати ім'я користувача і пароль; 4) вебсайт, захищений паролем; 5) запобігати несанкціонованому доступу; 6) надзвичайно складне завдання; 7) забувати свій головний пароль; 8) скориставшись пошуковою системою чи переглядаючи ваш профіль у соцмережі; 9) на моніторі чи під клавіатурою; 10) інформація та програми, збережені на комп'ютері, мобільному пристрої чи в мережі.

4. Give the appropriate Ukrainian equivalents of the following words and word combinations (in writing). Learn them.

1.	to provide a hint	
2.	password manager	
3.	(online) accounts	
4.	user name	
5.	single sign on	
6.	live chat	
7.	master password	
8.	cyberthief	
9.	initiate the inquiry	
10.	a default / preset password	
11.	to disclose password	
12.	to be wary	
13.	log-on name	
14.	sign-in procedure	
15.	customized content	

5. What do we call:

1) a Web service that allows visitors to communicate with the operator, usually through real-time live support; 2) a slight or indirect indication or suggestion; 3) one who steals financial and/or personal information through the use of computers for making its fraudulent or other illegal use; 4) a password that is used to access other passwords; 5) a password assigned to a program or hardware device by the developer or manufacturer; 6) a unique sequence of characters used to identify a user and allow access to a computer system, computer network, or online account; 7) a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications; 8) a software app or a hardware device used to store and manage a person's passwords and strong passwords, typically encrypted ones, requiring the user to create a master password to access all managed passwords; 9) careful, cautious; 10) the means by which a user can access a computer system.

6. Choose the correct answer.

1. According to the passage, a password manager is …

a) a default or preset password, such as admin.
b) a vital online account.
c) a malicious program that can execute itself.
d) a convenient service that stores all your account information securely.

2. A unique combination of characters, such as letters of the alphabet or numbers, that identifies one specific user is …
a) a user name.
b) a password.
c) a live chat.
d) a nickname.

3. Security experts recommend …
a) to have one password for all their vital online accounts.
b) to write passwords on a slip of paper kept near the computer, especially taped to the monitor or under the keyboard.
c) to use different user names and passwords for every account and change the passwords frequently.
d) to enable multiple users to share computers and devices.

4. The word *inquiry* in this text is closest in meaning to
a) "an attempt to find information that is performed by questioning electronically."
b) "a seeking or request for truth, information, or knowledge."
c) "an investigation, as into an incident."
d) "asking questions".

5. A private combination of characters associated with the user name that allows access to certain computer resources is referred to as …
a) log-on name.
b) a password.
c) a user name.
d) a single sign on.

6. The word *account* in the text is translated into Ukrainian as
a) рахунок.
b) звіт.
c) обліковий запис користувача.
d) кредит.

7. The word *default* in the text is closest in meaning to
a) to fail to do something, such as pay a debt, that you legally have to do.
b) a preselected option adopted by a computer program(mer) when no alternative is specified by the user.
c) winning the competition because the other side didn't compete.
d) the fact of not keeping to an agreement or contract.

8. According to the text, the first time you enter your user name and password the password manager …
a) generates random passwords.
b) carefully screens all incoming and outgoing messages.
c) saves this information.
d) limits on the number of passwords that can be saved.

9. Which is the best way to translate the following sentence:

You might select a name that is formed from parts of your real name or nickname and possibly some numbers, if the name you want is taken.

a) Ви можете обрати ім’я, яке складається частково з вашого справжнього імені чи прізвиська і, можливо, якихось цифр, якщо ім’я, яке вам подобається, уже використовується.
b) Ви можете вибрати ім’я, яке буде сформоване з частин вашого реального імені чи клички і, можливо, кількох цифр, якщо ім’я, яке ви хочете, уже взяте.
c) Ви можете обрати ім’я, яке буде складатися з частини вашого дійсного імені чи імені «Коля» і, можливо, якихось номерів, якщо ім’я, яке ви хочете, уже зайняте.
d) Ви можете селекціонувати ім’я, яке буде формувати з частин вашого реального імені чи прізвиська і, може, якихось чисел, якщо ім’я, яке ви хочете, уже забране.

10. The word combination *to provide a hint* in the text is translated as:
a) гарантувати пораду.
b) пропонувати підказку.
c) забезпечувати можливість.
d) постачати натяки.

7. a) Render the following:
- in Ukrainian.

No two users can have the same email address; that is, your email address is unique to you. This means you can use your email address and password from one website to validate your identity on another website. Facebook, Google, and Twitter, for example, are three popular websites that provide authentication services to other applications. By using your email address from one of these websites to access other websites, you do not have to create or remember separate user names and passwords for the various websites you visit.

Instead of passwords, some organizations use passphrases to authenticate users. A *passphrase* is a private combination of words, often containing mixed capitalization and punctuation, associated with a user name that allows access to certain computer resources. Passphrases, which often can be up to 100 characters in length, are more secure than passwords, yet can be easy to remember because they contain words.

A PIN (personal identification number), sometimes called a *passcode*, is a numeric password, either assigned by a company or selected by a user. PINs provide an additional level of security if they are selected carefully and protected as any other password. For example, PINs should not contain the same four digits, sequential digits, or dates others could easily determine, such as birth dates.

- in English:*

Паролі повинні бути вибрані з розумом, тому що вони захищають доступ до більшості послуг, даних і місць. Основне правило, це тримати їх в секреті, але якщо пароль буде занадто складним, то і запам'ятати його буде непросто.

Іншим важливим принципом є часта зміна паролів, особливо тих ключових, які використовуються для роботи компанії. Рекомендується замінювати їх кожні кілька тижнів, в залежності від того, наскільки важлива послуга або інформація ними захищається. 2-3 місяці – це достатній час для менш важливих облікових записів. Для найбільш важливих термін придатності обмежується одним днем.

Крім того, складність пароля повинна бути адаптована до послуги. На форумі, на який ви зайдете лише один раз, достатньо і простого слова. Більш складні паролі повинні захищати пошту і доступ до комп'ютера або корпоративних даних.

Якщо ви не можете встановити окремий пароль для кожного сайту, застосовуйте кілька варіантів, які підійдуть до різноманітних послуг: наприклад, прості паролі – для рідко відвідуваних сторінок, складніші –для улюблених сайтів, ще складніші – для пошти і найважчі – для банківських послуг.

b) Consider this:

1. Why do some websites allow you to use your email address as a user name? Is it safe? 2. What other ways to authenticate the user are used by some organizations? 3. Have you ever tried hints provided by some sites in case a user forgets his password? Was it helpful?

8. a) Read the Information file below (use the dictionary if needed).
b) Be ready to explain the importance of a strong password and ways of creating it.

Information file

Passwords Help Keep Personal Data Secure

Most of us rely on passwords for every day activities; accessing the internet, using a credit card, or gaining access to our workplace. A secure password is the key that unlocks details of your bank account, your social media accounts and your social security benefits. Your password is more valuable than gold to thieves. It can be used to steal your money or to gain access to personal information that can be used to scam you and others.

You should guard your passwords in the same way as your house keys. At home, you have a different key for each door and only lend them out to trusted family and friends. If you lose your house keys, you immediately get all the locks changed. Likewise, for passwords you should have a unique key for each account. If you "lend" the combination to a colleague, make sure you change the password on your return.

A strong password is one that is difficult to guess or unravel. An expert computer hacker will be able to crack most passwords given enough time. Your aim is to make a password long enough and complex enough to deter all but the most tenacious of thieves.

The advice from Microsoft is that a good password…:

- is at least eight characters long
- doesn't contain your user name, real name, or company name
- doesn't contain a complete word
- is significantly different from previous passwords
- contains uppercase letters, lowercase letters, numbers, and symbols.

The results of research revealed the following facts about our online password use.

1) One in five of us use online passwords that haven't been changed in a decade.
2) Almost half (47%) rely on at least one password that has not been changed for five years.
3) 73% of online accounts are activated by the same password that is also used for another account.
4) On average just six unique passwords are used to protect 24 online accounts.
5) In the past year, a third of consumers (30%) had an account hacked or password stolen or received a notice that their personal information had been compromised.
6) As a result, more than three quarters (80%) of consumers are worried about their online security.
7) More than half (54%) use five or fewer passwords across their entire online life, while a fifth (22%) use three or fewer. (The sample size was 2,000 UK and US consumers).

It is good practice to change your password every 30 days or so. That way if it is stolen, the hacker has only a limited amount of time to access your account. If you have not changed yours lately, do it now before you forget! Be especially worried if your password is something

obvious like 123456.

Consider this:

1. Are you sure all your passwords strong and secure? What makes you so sure that they are (aren't)? 2. How frequently do you change your passwords? Why? 3. Do you classify your accounts into 'more' and 'less important' before inventing passwords for them? What types of strong password creation methods do you prefer when generating passwords? Why?

*c)** **Internet Research**

- Browse the free web resources to search for:

'The most popular strong password generating programs';

- Analyze the information you found and be ready to present the PowerPoint Presentation or written (oral) report, or 200-250-word essay (choose the form that suits you best):"The antivirus protection that keeps my own personal computer secure". Give reasons and all necessary details to motivate your choice.

9. a) Read the following to learn about the use of* a CAPTCHA.

Some websites use, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart. A CAPTCHA is a program developed at Carnegie Mellon University that displays an image containing a series of distorted characters for a user to identify and enter in order to verify that user input is from humans and not computer programs.

A CAPTCHA is effective in blocking computer-generated attempts to access a website, because it is difficult to write programs for computers to detect distorted characters, while humans generally can recognize them. For visually impaired users or if words are too difficult to read, the CAPTCHA text can be read aloud; you also have the option of generating a new CAPTCHA.

b) Consider This:

1) Why do some websites display distorted characters you must reenter along with your password? 2) Are you always able to recognize the distorted characters? Can the characters displayed be changed in case the user experiences difficulties in recognizing them? 3) Is the CAPTCHA technique efficient in verifying that the user is a human not a bot? Why (not)? Give your reasons.

10. Write a short summary of the text 'How to Create a Strong Password', p. 57 (see the scheme in ex.10, Unit 1).

Extended Reading

(1) How to Create a Strong Password

by Nick Douglas

The U.S. government recently revamped its password recommendations, abandoning its endorsement of picking a favorite phrase and replacing a couple characters with symbols, like **c4tlo^eR**. These short, hard-to-read passwords look complicated to humans but very simple to computers.

Instead, you want long, weird strings that neither computers nor people can guess. Humans are bad at coming up with these – we all pick the same "random" words, and we're

bad at remembering actually random strings. Follow this guide to make good passwords, or better yet, let an app make and remember them for you.

Make your passwords very long. Your enemy isn't some guy in a ski mask trying to guess your password one try at a time. It's a program that automatically runs through massive databases of common passwords or random combinations of characters. The best answer to that is a very long string of words. As the webcomic **xkcd*** famously pointed out, a bunch of plain words is pretty good. But as many hackers use "dictionary attacks" to guess regular words, it's best to add some capital letters, special characters, or numbers.

Don't use a common phrase. But don't use the same bunch of plain words as everyone else. If your password consisted of the entire script of Hamlet, it would still be unsafe if everyone else had the same password. "When in the course of human events" is a shitty password. So is a famous movie line, or a Bible verse, or even an acronym of a Bible verse.

And don't get clever with thematic or personally meaningful passwords. Sometimes humans do try to crack passwords, so don't help them out by using your son's birthday or the phrase printed on your favorite coffee mug.

Test your password. If you use a password manager, it'll test your password in real time, on the safety of your computer. The sites 'How Secure Is My Password?', 'How Big Is Your Password?', and 'How Strong Is Your Password?' test if your password is long enough. But they won't warn you about common guessable phrases, like those Bible verses.

Of course, typing your passwords into unfamiliar sites is a bad habit. These sites are safe, as they're all publicly run by trusted developers who promise that your entered text never leaves your computer. Still, to be safe, just use these sites to get the gist before you make your real password.

Don't reuse your password. When your password on some web service gets hacked (and it will), you'd better hope you didn't use the same password on three other services. Don't use a weak password for services that "don't matter," because some day you might give one of those services your credit card info, or use it to authorize more important services, and you won't think to beef up your password.

Use a password manager. Until you do this, no matter how hard you try all the rules above, you will keep picking bad passwords. Here's how:

- Your "random" string of words will be something like "**monkey dragon baseball princess**," four extremely common password words, and a computer will guess it.

- You'll pick something memorable, which will limit your options, and a computer will guess it.

- You'll manage to make a password a computer can't guess, and you'll forget it, and you'll have to replace it with a weaker password, and a computer will guess it.

- You'll pick something identifiable to anyone who follows you on Twitter or Facebook – like your dog's name – and a human will guess it.

Instead, get your computer to make and remember your passwords for you. This is the only reliable but convenient way to manage the vast quantity of passwords that modern life requires. The current best in class is **1Password**. If you don't care about the detailed differences between managers, just grab this one.

There are several other fantastic, full-featured password managers for Windows and OS X. All these apps will create and remember your passwords. And all of them tell you how secure each of your passwords are. Some even alert you when the services you use get hacked, whether or not you were personally exposed. Of these top picks, the most distinctive is the open-source **KeePass**. It focuses on local storage rather than cloud solutions, and it even lets you use a file to unlock it, so you could turn a physical thumb drive into your "password."

Cloud-based services like **1Password** and **LastPass** are more vulnerable to remote attacks. But because they heavily encrypt your data and don't store your master password, you're still safe even if those services are hacked – as long as your master password is too hard to crack. (You can also sync your encrypted password file with *Dropbox* or *Google Drive*; a hacker would still need your master password to unlock it). You just need to remember one password: The one that locks your password manager. Follow all the rules above to create a strong master password, especially if you sync your data. Otherwise, if your password service ever gets hacked, the hackers will also guess your weak master password, and they will swim around in all your accounts as in a silo of Scrooge McDuck money.

Now if you just have to write that master password down, do it on paper, and keep it somewhere safe like your wallet. Don't write "MASTER PASSWORD" on it. Rip it up as soon as you've memorized it (which will take just a day or two, thanks to the muscle memory of typing it in every time you log into anything). Don't forget your master password, or you could be completely and utterly screwed.

(https://lifehacker.com/how-to-create-a-strong-password-1797681069)

*a webcomic created by American author Randall Munroe. The comic's tagline describes it as "A webcomic of romance, sarcasm, math, and language". Munroe states on the comic's website that the name of the comic is not an initialism but "just a word with no phonetic pronunciation".

(2) How to Create the Perfect Screen/Username

by Brandon De Hoyos

Generate a cool username for Instagram, Twitter, YouTube, Snapchat, and others!

A username is your identity online, whether you use it for your online bank or just to meet new people through a chat room. Creating a username, screen name, handle, login ID, etc., is serious business. Not only will this new moniker become tied to your online identity, it will affect other people's perception of you, much like how your hair and clothes might during an in-person meeting. Your handle might even affect the results of your job search or dating profile if it refers to something racy or inappropriate. On the flip side, being associated with a unique and attention-grabbing screen name is a great way to showcase your personality and create a memorable impression.

Indeed, screen name creation is probably more important than most of us realize. Don't fret, though! Below are a few ideas to help you score a terrific username.

Add Favorite Things to Your Username. Do you like the color purple, dinosaurs, candy, and the number 7? Something like **SweetPurpleDinosaur7** will go a long way. Jot down a few of your favorite things and consider your job or career aspirations, favorite foods, celebrities, sports teams, movies... Just be creative!

Consider What's Around You. Have you exhausted your lists of favorite things? Consider school mascots, your town, or other things relative to where you live and what you are about. However, be very careful not to give away too much information. Internet predators could potentially identify your location by your screen name. Something like **SweetTexarkanaHighDinosaurGirl91** might seem innocent at first until you realize that it can probably be deciphered as a *Texarkana, TX, high school girl* who graduated or was born in *1991*. On that note, maybe you should choose something specific that doesn't actually apply to you, for even more anonymity.

Use a Screen Name Generator. One of the most easy ways to create a screen name with the least amount of effort is to let your computer do it for you. There are several screen name generators available that are easy and fun to use. Here's our top picks:

(1) SpinXO: Generates names using information like your hobbies, important words, name, numbers, and things you like. You can get 30 usernames immediately, and refresh for more. Click a username at *SpinXO* to see if they're available on different platforms like Reddit, Tumblr, YouTube, Twitter, or Instagram.

(2) Screen Name Generator: Enter two words at *The Screen Name Generator* to have it generate a unique screen name that's a combination of your words plus something random in between them. This is a good tool to use if you have specific words that you'd like to include in your username.

(3) Rum and Monkey: *Rum and Monkey*'s online name generator is broken down into categories to help you find the best login ID. Get an ancient Greek name or something in military code. You can even go for a Minion or Korean name. Select a category and your gender, and then enter your name to get a fun and unique username.

(4) The Cool Name Generator: Make a random male, female, or gender-neutral screen name at *The Cool Name Generator*. You also have the option to put in your own name for a personal gender-specific username.

(5) Fake Name Generator: This website not only gives you a username but even a whole identity, including a first and last name, address, birthday, physical attributes, employment information, and more. A bit much? Maybe so, but the usernames are pretty random and the other details are fun to read.

What to Do When Your Screen Name Is Unavailable. Have you hit the "*this username is taken*" roadblock and need creative inspiration? A used screen name doesn't mean it wasn't meant to be. Just like when creating strong passwords that are hard to guess, you can also use non-English word combinations to build unlikely usernames. Consider substituting symbols and letters that are similar: @=a, 3=e, $=5, S=5. Most messaging apps and social networks will let you use symbols in a username and, with many to choose from, the possibilities are nearly endless. For example, if **SweetPurpleDinosaur7** is already being used, consider making it **$weetPurpleD1nOsaur7**.

(https://www.lifewire.com/create-perfect-screen-name-1949903)

Unit 6. Software Theft

Pre-Reading Activities

Answer the questions.

1. Have you ever used pirated software or done illegal registration/activation? Why? 2. Why do some people use unlicensed software? 3. Who mostly uses unlicensed software? 4. Who will never use unlicensed software? 5. What are the drawbacks of using stolen software from the user's and software manufacturer's perspective? 6. What is software theft? List some examples.

1. a) Read the texts using the dictionary. b) translate the underlined words and word combinations into Ukrainian (in writing); c) pay attention to the terminological units in bold type. Be sure you can give their definition in English and their Ukrainian equivalents.

(1) Software Theft

Software theft occurs when someone steals software media, intentionally erases programs, **illegally** registers and/or activates a program, or illegally copies a program.

• **Physically stealing software**: A perpetrator physically **steals the media** that contains the software, or steals the hardware that contains the media that contains the software. For example, an unscrupulous library patron might steal a game CD/DVD.

• **Intentionally erasing software**: A perpetrator erases the media that contains the software. For example, a **software developer** who is terminated from a company may retaliate by removing or disabling the programs he or she has written from company computers.

• **Illegal registration/activation**: A perpetrator illegally obtains registration numbers and/or activation codes. A program called a ***keygen***, short for **key generator**, creates software registration numbers and sometimes activation codes. Some unscrupulous individuals create and post keygens so that users can install software without legally purchasing it.

• **Illegal copying**: A perpetrator copies software from manufacturers. Software piracy, often referred to simply as piracy, is the unauthorized and illegal **duplication** of copyrighted software. Piracy is the most common form of software theft.

(2) Safeguards against Software Theft

To protect software media from being stolen, owners should keep original software boxes and media or the online confirmation of purchased software in a secure location, out of sight of prying eyes. All computer users should back up their files and drives regularly, in the event of theft. When some companies terminate a software developer or if the software developer quits, they escort the employee off the premises immediately. These companies believe that allowing terminated employees to remain on the premises gives them time **to sabotage** files and other network procedures.

Many manufacturers incorporate an **activation process** into their programs to ensure the software is not installed on more computers than legally licensed. During the product activation, which is conducted either online or by phone, users provide the software product's identification number to associate the software with the computer or mobile device on which the software is installed. Usually, the software can be run a preset number of times, has limited functionality, or does not function until you activate it.

To further protect themselves from **software piracy**, software manufacturers issue users **license agreements**. A license agreement is the right to use software. That is, you do not own the software. The most common type of license included with software purchased by individual users is a ***single-user license agreement***, also called an ***end-user license***

agreement (*EULA*). The license agreement provides specific conditions for use of the software, which a user must accept before using the software. These terms usually are displayed when you install the software. Use of the software constitutes acceptance of the terms on the user's part.

To support multiple users' access of software, most manufacturers sell **network versions** or **site licenses** of their software, which usually costs less than buying individual stand-alone copies of the software for each computer.

A **network license** is a legal agreement that allows multiple users to access the software on the server simultaneously. The network license fee usually is based on the number of users or the number of computers attached to the network. A site license is a legal agreement that permits users to install the software on multiple computers – usually at a volume discount.

3. Translate the following word combinations.

a) into Ukrainian:

1) to erase programs; 2) to steal software media; 3) to contain the software; 4) to remove the program; 5) to disable the program; 6) out of sight of prying eyes; 7) to sabotage files and network procedures; 8) to protect oneself from software piracy; 9) to issue users license agreements; 10) to permit users to install the software.

b) into English:

1) ліцензійна угода кінцевого користувача; 2) генератор серійних номерів/ключів; 3) обмежений набір функціональних можливостей; 4) програмне забезпечення, захищене авторським правом; 5) ліцензія на локальне використання ПЗ; 6) включити в программу процес активації; 7) запускати ПЗ; 8) надавати особливі умови використання програмного забезпечення; 9) прийняття умов з боку користувача; 10) ідентифікаційний номер програмного продукту.

4. Choose from the box the appropriate Ukrainian equivalent to the following words and word combinations.

Крадіжка ПЗ, фізичне викрадення ПЗ, навмисне видалення ПЗ, незаконна реєстрація/активація, незаконне копіювання, програмне забезпечення захищене авторським правом, плата за ліцензію мережі, законна угода, недобросовісний, оптова знижка, ліцензійна угода кінцевого користувача, одночасно, приєднаний до мережі, умови договору, однокористувацька ліцензійна угода, піратство ПЗ, генератор ключів, задана кількість разів, обмежена функціональність, окремі копії програмного забезпечення.

1.	an end-user license agreement	
2.	intentionally erasing software	
3.	simultaneously	
4.	a preset number of times	
5.	software theft	
6.	copyrighted software	
7.	attached to the network	
8.	physically stealing software	
9.	a network license fee	
10.	limited functionality	

11.	agreement terms	
12.	illegal registration/activation	
13.	a legal agreement	
14.	software piracy	
15.	unscrupulous	
16.	a key generator	
17.	at a volume discount	
18.	illegal copying	
19.	a single-user license agreement	
20.	stand-alone copies of the software	

5. What do we call:

1) stealing software media, intentionally erasing programs, illegally registering and/or activating a program, or illegally copying a program; 2) a program that creates software registration numbers and sometimes activation codes; 3) the unauthorized and illegal duplication of copyrighted software; 4) the right to use software; 5) a legal agreement that allows one user to access the software; 6) a legal agreement that allows multiple users to access the software on the server simultaneously; 7) a legal agreement that permits users to install the software on multiple computers; 8) is a license validation procedure required by some proprietary computer software programs; 9) having or showing no moral principles; not honest or fair; 10) not according to or authorized by law.

6. Choose the correct answer:

1. The most common type of license included with software purchased by individual users is:
   a) a network license;
   b) a site license;
   c) a single-user license;
   d) a license agreement.
2. Which collocation is correct?
   a) to issue a license;
   b) to accompany a license;
   c) to present a license;
   d) to write out a license.
3. A person is not considered a penetrator when he/she:
   a) registers and/or activates a program using keygens;
   b) unintentionally erases software;
   c) illegally copies a program;
   d) purposefully removes or disables a program.
4. The word with an opposite meaning to *multiple* is:
   a) unscrupulous;
   b) diverse;
   c) single;
   d) more than one.
5. The passage states:
   a) that all perpetrators should be fined and punished;
   b) that software piracy is prohibited by law;
   c) that you must use a license for product activation or registration;
   d) what is considered to be a software theft and lists types of licenses.

6. If your software is registered and activated, …

a) it'll be run a preset number of times;

b) it'll have a limited functionality;

c) it'll function well;

d) you'll need to enter a registration or activation number every time you run your program.

7. The word *simultaneously* means:

a) at the same time;

b) independently;

c) individually;

d) incidentally.

8. Specific conditions for use of the software…

a) may be declined;

b) must be accepted at the start of the activation process;

c) are never displayed;

d) are useless.

9. Which is the best way to translate the following sentence into Ukrainian:

Use of the software constitutes acceptance of the terms on the user's part.

a) Використання ПЗ означає прийняття умов у частині користувача.

b) Використання ПЗ становить частку прийняття умов користувачем.

c) Використання ПЗ означає прийняття умов зі сторони користувача.

d) Прийняття умов користувачем є невід'ємним для користування ПЗ.

10. The word combination *volume discount* in the text is translated as:

a) суттєва знижка;

b) знижена гучність;

c) об'ємна знижка;

d) дисконт обсягу.

7. Eranslate the following sentences into Ukrainian. Use the dictionary if necessary.

1. The most widely used method to prevent software piracy is the license key; code that is built into an application to require a valid key to unlock the software. 2. Some shopping cart providers include licensing capabilities, offering an end-to-end method for everything from hosting a store, to distributing software, to managing licensing keys. 3. Some organizations encrypt the source code within an application so it can't be reverse engineered or stolen in any other way. 4. When dealing with Web applications, corporations should think about running PHP code using a tool like Zend Technologies Inc.'s Zend Guard, which provides a run-time environment to compile Web applications and thus shield the source code from the browsers. 5. Illegal and improperly used software hurts the economy in general, the software industry specifically and it can cause harm to your computer. 6. The EULA's terms and conditions define how you can legally use the software, how many computers you can install the software on, and whether or not you can make a backup copy. 7. Register your software to prevent others from attempting to install your software on their computers. 8. Report piracy if you discover that software you purchased is not authentic or if you suspect that an online reseller or retail establishment is selling counterfeit software. 9. Never download software from a peer-to-peer file-sharing sites. 10. Check the manufacturer's website to see what kind of authentication markings they include to guarantee that the software is genuine.

8. *a) Render the following text in English.*

b) Be ready to dwell on the topic Internet piracy in Ukraine.

Суть Інтернет-піратства полягає у відтворенні і розповсюдженні мережею Інтернет фільмів, музичних творів, комп'ютерних програм, іграшок, інших об'єктів інтелектуальної власності без дозволу автора або іншої особи, яка має авторське право і/або суміжні права, або без виплати винагороди за використання творів у встановленому законом порядку. На думку провідних юристів в сфері IT права, в Україні дуже складно притягнути до відповідальності за Інтернет-піратство. Адже, суб'єктом правопорушення у таких справах визнають не приватного користувача, а адміністратора мережевого ресурсу, який дозволив і сприяв поширенню контрафакту. Порушення авторського права має економічний характер, тому для його подолання необхідно припинити кримінальне переслідування і ввести штрафи відносно розповсюджувачів піратського контенту. Одним із головних нововведень є досудова можливість видалення або обмеження доступу до інформації, що порушує авторське право. При цьому передбачено штрафні санкції в розмірі від 500 до 1000 неоподатковуваних мінімумів доходу громадян за невиконання добросовісної вимоги щодо блокування нелегального контенту. Аналогічні штрафи загрожують у випадку відмови ідентифікувати користувача, який розмістив контент, що порушує авторські права. Інтернет-піратство має глобальний характер, його неможливо побороти в окремій країні. Японські дослідники з університету Aizu і американські – з університету Deakin розробили нові цифрові водяні знаки, які допоможуть вичистити Інтернет від нелегальної музики. Причинами невпинного розвитку та поширенню Інтернет-піратства є, перш за все, відношення громадськості до порушення авторських прав, продиктоване менталітетом та погіршенням економічного стану країни.

*c)** **Internet Research**

- Browse the free web resources to search for: 'What are the penalties for piracy?'

- Be ready to present the results of your research in class in the form of a written (oral) report / 200-250-word essay (choose the form that suits you best).

9. *a) Read the Information file below (use the dictionary if needed).*

b) Be ready to describe the process of product activation.

Information file

Product activation

Product activation is the act of verifying protected electronic data and involves the required activation by the consumer shortly or directly after purchasing the software or service. Activation verifies licensure and protects the copyright of the owners of digital products while helping to combat piracy.

There are a number of ways in which activation of products or services can take place. Sometimes it is simply a matter of using a code given to the buyer via email or physically printed on the product or its packaging. These codes are often called "product keys", "activation codes", "key codes" "activation keys" and there are usually instructions in the install process on how to activate the product. Some sophisticated software vendors require a telephone confirmation call at which time the activation code is given.

During the product activation process, codes/product keys are usually entered into a form and the product serial number which may also need to be entered is checked against the code. A mathematical algorithm aligns the two sequences and if they meet the conditions the product or service will be activated and can be used.

There are often requirements to agree to terms and conditions of the software license at

the time that the activation is made. Some activations are more lengthy than others; it often depends upon the value of the product or service being activated.

https://www.techopedia.com/definition/4065/product-activation

Consider this:

1. Why does software need activation? 2. How do you activate your software? 3. Can a keygen provide product activation?

10. Write a short summary of the text 'What Is Product Activation?', p. 66 (see the scheme in ex.10, Unit 1).

Extended Reading

(1) What Is Product Activation?

Some software programs require activation before they can be used

by Tim Fisher

Product activation (often just activation) is the procedure by which a piece of software or operating system is proven to be legitimately installed. From a technical perspective, product activation usually means combining a product key or serial number with unique information about a computer and sending that data to the software maker over the internet. Then, the software manufacturer can validate whether the information matches up with their records of a purchase, and any features (or lack of features) can then be placed on the software.

Why Does Software Need Activated? Product activation helps prove that the product key or serial number being used is not pirated and that the software is being used on an appropriate number of computers... usually, but not always, one. In other words, activating a product prevents users from copying a program to other devices without paying for the additional instances, something that's remarkably easy to do otherwise.

Depending on the software or operating system, choosing not to activate might prevent the software from running entirely, reduce the functionality of the software, watermark any output from the program, cause regular (usually very annoying) reminders, or may not have any effect at all. For example, while you can most definitely download a free version of the popular *Driver Booster* driver updater program, you cannot use all of its features because there's a professional version of the same program. Driver Booster Pro lets you download drivers faster and gives you access to a larger collection of drivers, but only if you insert a *Driver Booster Pro* license key.

How Do I Activate My Software? Keep in mind that not all programs need activated before they can be used. A general example is most freeware programs. Applications that are 100% free to download and use as often as you like do not normally need to be activated since they are, by definition, free for almost anyone to use. However, software limited in one or more aspects, like by time or use, often use product activation as a way for the user to lift those restrictions and use the program past its free trial date, use it on more computers than the free edition allows, etc. These programs often fall under the term shareware.

It'd be impossible to provide instructions on how to activate every single program and operating system, but in general, product activation works basically the same no matter what needs activated... If you're installing an operating system, you're often given the opportunity to provide an activation key during installation, maybe even with the option to delay activation until later. Once you've started the OS and are using it, there's most likely an area in the settings where you can enter the product key to activate it.

The same is true, for software programs though most even let you use the professional edition for a period of time (like 30 days) for free, with or without limitations depending on the application. However, when it's time to activate the program, some or all features are completely disabled until you paste in a product key. If you're not given the chance to enter a series of numbers and/or letters for activation, that program might instead use an activation key file that you get over an email or download from your online account. Some software programs don't use a traditional activation method and might instead make you log in to your account through the program because your activation status is stored in your online account.

In some situations, usually in commercial business settings only, multiple devices connect to a local server on the network to obtain the license information needed for a particular program. The devices are able to use the software in this way because the license server, which communicates directly with the manufacturer, can validate and activate each instance of the program. Look for a key icon, lock button, license manager tool, or option in the *File menu* or in the settings. It's usually there that you're given the option to load a license file, enter an activation code, etc. Activating an operating system or program can sometimes be accomplished over the phone or email as well.

Can a Keygen Provide Product Activation? Some websites offer free product keys or license files that trick a program into thinking that it's been purchased legally, letting you use a trial or expired program or operating system to its full capacity. They're normally provided through what's known as a keygen, or key generator. It's important to know that these types of programs do not provide valid licenses, even if they do actually work and let you use the software with no limitations. Entering a product key that works, but that was not purchased legally, is likely illegal in most cases, and certainly unethical.

It's always best to purchase programs from the manufacturer. In most situations, you can get your hands on a free trial copy of any program or OS so that you can test it out for a limited time. Just remember to buy a genuine license if you want to keep using it. Some license files and product keys are designed to be used more than once until a limit is reached, and some can be used as many times as possible but will only work if the simultaneous use of the license remains below a predefined number. For example, in the second instance where the same key can be used as often as you like, the license may only support, say, 10 seats at once. In this scenario, the key or key file could be loaded into the program on 10 computers and all of them could be activated, but not even a single one more. However, if three computers closed down the program or withdrew their license information, three more could begin using that same product activation information because the license permits 10 simultaneous uses.

(https://www.lifewire.com/what-is-product-activation-2625971)

(2) End-User License Agreement (“Agreement”)

Please read this End-User License Agreement (“Agreement”) carefully before clicking the “I Agree” button, downloading or using My Application (“Application”).

By clicking the “I Agree” button, downloading or using the Application, you are agreeing to be bound by the terms and conditions of this Agreement. If you do not agree to the terms of this Agreement, do not click on the “I Agree” button and do not download or use the Application.

License

My Company grants you a revocable, non-exclusive, non-transferable, limited license to download, install and use the Application solely for your personal, non-commercial purposes strictly in accordance with the terms of this Agreement.

Restrictions

You agree not to, and you will not permit others to license, sell, rent, lease, assign, distribute, transmit, host, outsource, disclose or otherwise commercially exploit the Application or make the Application available to any third party.

Modifications to Application

My Company reserves the right to modify, suspend or discontinue, temporarily or permanently, the Application or any service to which it connects, with or without notice and without liability to you.

Term and Termination

This Agreement shall remain in effect until terminated by you or My Company.

My Company may, in its sole discretion, at any time and for any or no reason, suspend or terminate this Agreement with or without prior notice.

This Agreement will terminate immediately, without prior notice from My Company, in the event that you fail to comply with any provision of this Agreement. You may also terminate this Agreement by deleting the Application and all copies thereof from your mobile device or from your desktop.

Upon termination of this Agreement, you shall cease all use of the Application and delete all copies of the Application from your mobile device or from your desktop.

Severability

If any provision of this Agreement is held to be unenforceable or invalid, such provision will be changed and interpreted to accomplish the objectives of such provision to the greatest extent possible under applicable law and the remaining provisions will continue in full force and effect.

Amendments to this Agreement

My Company reserves the right, at its sole discretion, to modify or replace this Agreement at any time. If a revision is material we will provide at least 30 days' notice prior to any new terms taking effect. What constitutes a material change will be determined at our sole discretion.

(https://termsfeed.com/blog/sample-eula-template/)

Software Piracy

Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries. According to the Business Software Alliance (BSA), about 36% of all software in current use is stolen. Software piracy causes significant lost revenue for publishers, which in turn results in higher prices for the consumer.

When you purchase a commercial software package, an end user license agreement (EULA) is included to protect that software program from copyright infringement. Typically, the license states that you can install the original copy of software you bought on one computer and that you can make a backup copy in case the original is lost or damaged. You agree to the licensing agreement when you open the software package (this is called a shrink wrap license), when you open the envelope that contains the software disks, or when you install the software.

Software piracy applies mainly to full-function commercial software. The time-limited or function-restricted versions of commercial software called shareware are less likely to be pirated since they are freely available. Similarly, freeware , a type of software that is copyrighted but freely distributed at no charge, also offers little incentive for piracy.

Types of software piracy include:

Softlifting: Borrowing and installing a copy of a software application from a colleague.

Client-server overuse: Installing more copies of the software than you have licenses for.

Hard-disk loading: Installing and selling unauthorized copies of software on refurbished or new computers.

Counterfeiting: Duplicating and selling copyrighted programs.

Online piracy: Typically involves downloading illegal software from peer-to-peer network, Internet auction or blog. (In the past, the only place to download software was from a bulletin board system and these were limited to local areas because of long distance charges while online.)

(http://whatis.techtarget.com/definition/piracy)

Unit 7. Information Theft

Pre-Reading Activities
Answer the questions.

1. Have you ever heard of victims of information theft? What has happened to them? 2. How can a specialist secure the data transferred online? 3. How do you check if a site is secure? 4. What are some risks of using not secure sites? 5. Why do people have concerns about information theft?

1. a) Read the texts using the dictionary. b) translate the underlined words and word combinations and terminological units in bold type into Ukrainian (in writing). Be sure you can give their definition in English.

Information Theft

Information theft occurs when someone steals personal or confidential information. Both business and home users can fall victim to information theft. An unethical company executive may steal or buy stolen information to learn about a competitor. A corrupt individual may steal credit card numbers to make fraudulent purchases. Information theft often is linked to other types of cybercrime. For example, an individual first might gain unauthorized access to a computer and then steal credit card numbers stored in a firm's accounting department.

Safeguards against Information Theft

Most organizations will attempt to prevent information theft by implementing the user **identification** and **authentication controls**. These controls are best suited for protecting information on computers located on an organization's premises. To further protect information on the Internet and networks, organizations and individuals use a variety of **encryption techniques**.

Encryption is the process of converting data that is readable by humans into **encoded characters** to prevent unauthorized access. You treat encrypted data just like any other data. That is, you can store it or send it in an email message. To read the data, the recipient must **decrypt**, or **decode** it. For example, users may specify that an email application encrypts a message before sending it securely. The recipient's email application would need to decrypt the message in order for the recipient to be able to read it.

In the encryption process, the unencrypted, readable data is called **plaintext**. The encrypted (scrambled) data is called **ciphertext**. An **encryption algorithm**, or *cypher*, is a set of steps that can convert readable plaintext into unreadable ciphertext. A simple encryption algorithm might switch the order of characters or replace characters with other characters. Encryption programs typically use more than one encryption algorithm, along with an **encryption key**. An *encryption key* is a set of characters that the **originator** of the data uses to encrypt the plaintext and the recipient of the data uses to decrypt the ciphertext.

Two basic types of encryption are **private key** and **public key**. With *private key encryption*, also called *symmetric key encryption*, both the originator and the recipient use the same secret key to encrypt and decrypt the data. *Public key encryption*, also called *asymmetric key encryption*, uses two encryption keys: a public key and a private key.

Public key encryption software generates both the private key and the public key. A message encrypted with a public key can be decrypted only with the corresponding private key, and vice versa. The public key is made known to message originators and recipients. For example, public keys may be posted on a secure webpage or a public-key server, or they may be emailed.

The private key, by contrast, should be kept confidential. Some operating systems and email programs allow you to encrypt the contents of files and messages that are stored on your computer. You also can purchase an encryption program to encrypt files. Many browsers use encryption when sending private information, such as credit card numbers, over the Internet.

Mobile users today often access their company networks through a **virtual private network** (*VPN*). When a mobile user connects to a main office using a standard **Internet connection**, a VPN provides the mobile user with a secure connection to the company network server, as if the user has a private line. VPNs help ensure that data is safe from being **intercepted** by unauthorized people by encrypting data as it transmits from a laptop, smartphone, or other mobile device.

Digital Signatures and Certificates. A **digital signature** is an encrypted code that a person, website, or organization **attaches to** an electronic message to verify the identity of the message sender. Digital signatures often are used to ensure that an **impostor** is not participating in an Internet transaction. That is, digital signatures can help to prevent email **forgery**. A digital signature also can verify that the content of a message has not changed.

A **digital certificate** is a notice that guarantees a user or a website is legitimate. E-commerce applications commonly use digital certificates. Browsers often display a warning message if a website does not have a valid digital certificate. A website that uses encryption techniques to secure its data is known as a secure site. Web addresses of secure sites, such as the Amazon.com checkout, often begin with *https* instead of *http*. Secure sites typically use digital certificates along with **security protocols**. Browsers also often display **a lock symbol** in the window, which you usually can tap or click to see the associated digital certificate.

3. Translate the following word combinations.

a) into Ukrainian:

1) to fall victim to information theft; 2) an unethical company executive; 3) a secure connection to the company network server; 4) to prevent information theft; 4) to implement the user identification and authentication controls; 5) to verify the identity of the message sender; 6) encryption techniques; 7) to convert data into; 8) to treat encrypted data like; 9) to transmit data; 10) virtual private network.

b) into English:

1) запобігти підробці електронних листів; 2) перевірити, що зміст повідомлення не змінився; 3) зробити відомим; 4) відобразити попередження; 5) тримати в секреті; 6) відобразити символ блокування; 7) легко вдарити по або натиснути на символ блокування; 8) міняти порядок символів; 9) заміняти символи; 10) бути перехопленим неавторизованими особами.

4. Choose from the box the appropriate Ukrainian equivalent to the following words and word combinations.

Покупки по шахрайській схемі, методи шифрування, закодовані символи, одержувач/відправник інформації, шифрувати/розшифровувати дані, незашифрований/зашифрований текст, шифрування з закритим ключем, шифрування з відкритим ключем, віртуальна приватна мережа, читабельні дані, набір символів, цифровий підпис, людина, яка видає себе за іншу особу, цифровий сертифікат, надійний сайт, захищений сайт, зареєстрований/законний користувач, протокол безпеки, перевірка сайту, дійсний цифровий сертифікат.

1.	encryption techniques	
2.	readable data	
3.	a legitimate site	
4.	a digital signature	
5.	a security protocol	
6.	fraudulent purchases	
7.	a recipient/ an originator	
8.	encoded characters	
9.	a set of characters	
10.	a virtual private network	
11.	a legitimate user	
12.	private key encryption	
13.	an impostor	
14.	a digital certificate	
15.	encrypt/ decrypt data	
16.	a secure site	
17.	a valid digital certificate	
18.	a site checkout	
19.	plaintext/ ciphertext	
20.	public key encryption	

5. What do we call:

1) controls that are used for protecting information on computers located on an organization's premises; 2) the process of converting data that is readable by humans into encoded characters to prevent unauthorized access; 3) the unencrypted, readable data in the encryption process; 4) the encrypted (scrambled) data in the encryption process; 5) a set of steps that can convert readable plaintext into unreadable ciphertext; 6) a type of encryption when both the originator and the recipient use the same secret key to encrypt and decrypt the data; 7) a type of encryption that uses two encryption keys: a public key and a private key; 8) an encrypted code that a person, website, or organization attaches to an electronic message to verify the identity of the message sender; 9) a notice that guarantees a user or a website is legitimate; 10) a website that uses encryption techniques to secure its data.

6. Choose the correct answer:

1. The text describes:

a) types of securing data; b) techniques for sending data; c) several secure sites;
d) the difference between an impostor and a legitimate user.

2. According to the text, there are:

a) 1 type of data encryption; b) 2 types of data encryption; c) 3 types of data encryption; d) 4 types of data encryption.

3. The word *technique* in this text is closest in meaning to

a) skill, art; b) capability, ability; c) method, approach; d) expertise, proficiency.

4. A person who pretends to be someone else in order to deceive others, especially for fraudulent gain:

a) a fraud; b) an impostor; c) a scam; d) a corrupt individual.

5. A virtual private network (VPN) provides the mobile user with:

a) a secure connection to the company network server; b) a private telephone line;

c) the access to forbidden in the country sites; d) a digital certificate.

6. Which of the following features is not typical for a secure site:

a) it uses encryption techniques;

b) web addresses of secure sites often begin with https;

c) it uses a digital certificate along with security protocols;

d) web addresses of secure sites often begin with http.

7. Which is the odd one? Different safeguards against information theft help prevent:

a) an unauthorized access; b) an email forgery; c) information theft; d) fraudulent purchases.

8. The word with an opposite meaning to *scrambled* is:

a) plain; b) encrypted; c) unethical; d) legitimate.

9. Which is the best way to translate the following sentence:

A message encrypted with a public key can be decrypted only with the corresponding private key, and vice versa.

a) Повідомлення, зашифроване з допомогою відкритого ключа, може бути розшифроване лише відповідним приватним ключем, і навпаки.

b) Повідомлення, зашифроване відкритим ключем, може бути розшифровано лише відповідним секретним ключем, і навпаки.

c) Це зашифроване відкритим ключем повідомлення відкривається тільки приватним ключем, і навпаки.

d) Зашифрованому відкритим ключем повідомленню відповідає тільки секретний ключ.

10. The word combination *convert readable data into encoded characters* in the text is translated as:

a) конвертувати розбірливі дані в закодовані символи;

b) перетворювати читабельні дані в закодовані символи;

c) обертати зчитувані дані в закодовані символи;

d) конвертувати зчитувані дані в закодовані символи.

7. a) Render the text below in Ukrainian. Use the dictionary if necessary.

1. RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message. RSA is a relatively slow algorithm, and because of this it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed. The idea of an asymmetric public-private key cryptosystem is attributed to Whitfield Diffie and Martin Hellman, who published the concept in 1976. They also introduced digital signatures and attempted to apply number theory.

b) browse the Internet for additional information concerning the RSA algorithm.*

Consider this:

1. What does the abbreviation RSA stand for? 2. What is the history of this cryptosystem?

*8. a) Render the text in English.**

b) Make up a summary of the text in English.

Чому не можна цупити інформацію

Репутація кожного з нас – дуже важлива й часто цілком матеріальна річ, варта того, щоби про неї дбати.

Якщо хтось, наприклад, вкраде смартфон в іншої людини, такі дії будуть кваліфікуватися як кримінальний злочин (крадіжка), за котрий передбачено, зокрема, позбавлення волі на строк до трьох років. Якщо хтось поцупить технічну документацію до нового смартфона, дизайн моделі тощо, видаватиме його за свій винахід і продаватиме, це кваліфікується як шахрайство та порушення прав на винахід, що також може «забезпечити» винному позбавлення волі на строк до двох років. Те саме стосується й крадіжки інформації – як носіїв інформації (журналів, збірок та навіть сайтів), так і привласнення самої інформації, або ж недобросовісне її використання – без посилань на автора, джерело першого оприлюднення тощо. Отож, якщо в судовому порядку буде доведено, що ті, хто незаконно використовував чужі твори, завдали істотної шкоди автору, їх може бути покарано ув'язненням строком до двох років.

В інших випадках на крадіїв та незаконних поширювачів лягає цивільна або адміністративна відповідальність, яка вимірюється фінансово – у вигляді штрафу. Слід мати на увазі, що це стосується також незаконного розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних тощо.

Щоби не втрапити в халепу, варто пам'ятати бодай одне просте правило: поширювати можна лише той продукт, ліцензія якого дозволяє це робити, або ж якщо його створено не менше 75 років тому, або якщо з часу смерті його автора минуло щонайменше 75 років (стосовно українських об'єктів чи авторів – 70років). Поширювати інформацію можна із обов'язковим посиланням на автора та на першоджерело, де цю інформацію було опубліковано.

(http://mediadriver.online/vse_shcho_potribno_znaty_pro_copyright/chomu-ne-mozhna-krasti-informatsiyu-etichni-ta-yuridichni-aspekti/)

9. Internet Research

Browse the free web resources to search for: 'Different algorithms of securing data'.
Be ready to present the results of your research in class in the form of PowerPoint Presentation / written (oral) report / 200-250-word essay (choose the form that suits you best).

10. Write a short summary of the text 'Cloud Data Privacy', p. 74 (see the scheme in ex.10, Unit 1).

Extended Reading

(1) Cloud Data Privacy

Privacy and security concerns arise when consumers and businesses consider moving their data to an online storage service. While the cloud offers a tremendous amount of storage space at a relatively low cost, the security of data and the reliability of cloud companies trigger concerns.

When people register for a cloud computing service, they sign a written contract or tap or click an online OK or Agree button to affirm they read and understand the terms of the agreement. Any data saved on the cloud is entrusted to the third-party provider, which has a legal obligation to protect the data from security breaches. The company also must guard

against data loss due to physical disasters, such as power outages, cooling failures, and fire. When data has been compromised, many states require the company to disclose the issue to the data owner promptly.

The Cloud Security Alliance (CSA) warns of hackers who register for the service with a credit card or for a free trial period and then unleash malware in an attempt to gain access to passwords. Because the registration and validation procedure for accessing the cloud is relatively anonymous, authorities can have difficulty locating the abusers.

Another concern arises when transferring data over a network to the cloud. When the data is traveling to or from a computer and the cloud service, it is subject to interception. To minimize risk, security experts emphasize that the web address of the website you are visiting must begin with https, and the data should be encrypted and authenticated.

Law enforcement's access to the data raises another security issue. Email messages stored on a private server belong to the company or individual who owns the computer, so law enforcement officials must obtain a search warrant to read a particular user's messages. In contrast, law enforcement officials can access email messages stored on the cloud by requesting the information from the company that owns the cloud service. The user might not be notified of the search until up to 90 days after the search occurred; moreover, the search may occur without limitations and may include continuous monitoring of an individual's email communications.

International laws and industry regulations protect sensitive and personal data. Germany has some of the strictest cloud data privacy laws, and, in general, the European Union's privacy regulations are more protective that those in the United States. In much of Europe, for example, consumers must agree to have their personal information collected, and they can review the data for accuracy. The education, health care, and financial services industries in the United States have strict data privacy regulations that affect cloud storage. For example, the Family Educational Rights and Privacy Act (FERPA) regulates the confidentiality of students' educational records, so colleges must obtain students' consent to share data with cloud storage providers and other third parties.

Cloud storage companies have increased their privacy and security features in recent years. Many allow consumers and businesses to protect files with passwords or require two-step authentication to access files, to delete data if a mobile device has been stolen or lost, and to delete data that has been stored past an expiration date.

Consider This:

1. How much of your personal data is stored on the cloud? 2. Do you have concerns about the security of this data? 3. Have you ever received a notice that any of your online data has been compromised? 4. Should online social networks or email providers give more explicit notice that data is stored on the cloud? 5. Should law enforcement officials be able to access your data without your consent? Why or why not?

(2) Who Is Responsible for Data Left on the Cloud?

Businesses often contract with cloud storage providers for data storage. Many businesses also use cloud storage providers to store customer data. This data could include contact information, credit card numbers, and ordering history.

Ownership of cloud data becomes an issue when a cloud storage provider or the business using the cloud services closes. Other issues include what happens if the business fails to pay the cloud storage provider, or when a contract ends. Many feel that it is the responsibility of the business owner to remove and destroy company data before a contract ends. Supporters of

this argument believe that cloud storage providers should not be accessing data they host. Others contend that if a business fails to remove and destroy its data before its cloud storage contract ends, cloud storage providers should return the data, or remove the data permanently.

An ongoing debate exists related to who is responsible for cloud data security. Many experts put the responsibility of securing data in the hands of the data owner. Others advocate for a shared security model, in which the cloud storage provider includes security tools, but the company provides additional security as needed. Ownership and security of data should be included in any contract between a business and cloud storage provider. Contracts also should specify what happens in a variety of scenarios, including if either party stops its operations, or if hackers access the data.

Consider This:

1. If a business stops its operations, who should remove its data from cloud storage? Why? 2. If a customer does not remove its data before a contract ends, should a cloud storage provider return the data, or can it remove or sell the data? Why or why not? 3. Who is responsible for data security? Why?

Unit 8. Hardware Theft, Vandalism, and Failure

Pre-Reading Activities

Answer the questions.

1. How do you understand the notions of hardware theft and hardware vandalism? 2. Do you know anyone who fell victim to hardware theft or vandalism? 3. Have you ever damaged hardware? 4. What are physical ways to protect data? 5. Do you back up data?

1. a) Read the texts using the dictionary. b) Translate the underlined words and word combinations and terminological units in bold type into Ukrainian (in writing). Be sure you can give their definition in English.

Hardware Theft, Vandalism, and Failure

Users rely on computers and mobile devices to create, store, and manage important information. You should take measures to protect computers and devices from theft, vandalism, and failure.

Hardware theft is the act of stealing digital equipment. **Hardware vandalism** involves defacing or destroying digital equipment. Hardware can fail for a variety of reasons: aging hardware, natural or man-made disasters, or random events such as electrical power problems, and even errors in programs or apps.

The hardware theft and vandalism safeguards consist in **physical access controls** (i.e., locked doors and windows); **alarm system**; **physical security devices** (i.e., cables and locks), and **device-tracking apps**, while the hardware failure safeguards are provided by **surge protector**; **uninterruptible power supply** (UPS); **duplicate components** or duplicate computers and **fault-tolerant computers**.

To protect against data loss caused by hardware/software/information theft or system failure, users should **back up** computer and mobile device files regularly. As previously described, a *backup* is a duplicate of a file, program, or media that can be used if the original is lost, damaged, or destroyed; and to back up a file means to make a copy of it. In the case of system failure or the discovery of corrupted files, you restore the files by copying the backed up files to their original location on the computer or mobile device.

If you choose to back up locally, be sure to use high-quality media. A good choice for a home user might be optical discs or an **external hard drive**. Keep your backup media in a fireproof and heatproof safe or vault, or offsite. *Off-site* means in a location separate from where you typically store or use your computer or mobile device. Keeping backup copies off-site minimizes the chance that a single disaster, such as a fire, would destroy both the original and the backup media. An off-site location can be a safe deposit box at a bank, a briefcase, or **cloud storage** or **cloud backup**.

Cloud storage provides storage to customers, usually along with synchronization services but often on smaller amounts of data. By contrast, *cloud backup* provides not only backup and retrieval services, but generally provides **continuous data protection** to the cloud. More customers are opting for cloud backup because it saves them the cost of maintaining hardware. Backup programs are available from many sources. Most operating systems include a backup program. Backup devices, such as external disk drives, also include backup programs. Numerous stand-alone backup tools exist. Cloud storage providers may offer backup services. Users of a cloud backup service install software on their computers that backs up files to the cloud as they are modified.

Business and home users can perform four types of backup: **full, differential, incremental**, or **selective**. A fifth type, continuous data protection, often is used only by large

enterprises to back up data to an **in-house network storage device** purchased and maintained by the enterprise. Cloud backup services, a sixth option, are providing continuous data protection capabilities at a lower cost. Some users implement a **three-generation backup policy** to preserve three copies of important files. The *grandparent* is the oldest copy of the file. The *parent* is the second oldest copy of the file. The *child* is the most recent copy of the file. When a new backup is performed, the child becomes the parent, the parent becomes the grandparent, and the media on which the grandparent copy was stored may be erased and reused for a future backup.

2. Translate the following word combinations.

a) into Ukrainian:

1) to create, store, and manage important information; 2) to deface or destroy digital equipment; 3) to fail for a variety of reasons; 4) to erase and reuse the media; 5) to provide flexibility; 6) to maintain backup hardware; 7) to require a great amount of storage; 8) to back up locally; 9) marked for backup; 10) continuous data protection.

b) into English:

1) вживати заходів; 2) збій в системі; 3) виявлення пошкоджених файлів; 4) відновити файли; 5) вогнетривкий і теплостійкий сейф; 6) послуги резервного копіювання та одержання даних; 7) природні або техногенні катастрофи; 8) змінювати файл; 9) виконувати резервне копіювання; 10) зберегти копії.

3. Choose from the box the appropriate Ukrainian equivalenti ща the following words and word combinations.

Викрадення апаратного забезпечення, акт вандалізму стосовно апаратного забезпечення, головний запобіжний захід, сигналізація, хмарне сховище, резервне копіювання файлів трьох поколінь, стабілізатор напруги, повне резервне копіювання, безперебійний блок живлення, диференційне резервне копіювання, контроль фізичного доступу, додаткове резервне копіювання, окремі інструменти резервного копіювання, вибіркове резервне копіювання, метод відновлення, хмарне резервне копіювання, застаріле обладнання, безперервний захист даних, місце для зберігання, програма відстеження пристрою

1.	storage space	
2.	aging hardware	
3.	alarm system	
4.	physical access controls	
5.	cloud storage	
6.	hardware theft	
7.	recovery method	
8.	surge protector	
9.	hardware vandalism	
10.	device-tracking app	
11.	ultimate safeguard	
12.	incremental backup	
13.	selective backup	
14.	three-generation backup	
15.	stand-alone backup tools	

16.	differential backup	
17.	cloud backup	
18.	uninterruptible power supply	
19.	full backup	
20.	continuous data protection	

4. What do we call:

1) the act of stealing digital equipment; 2) the act of defacing or destroying digital equipment; 3) a type of backup that copies all of the files on media in the computer; 4) a type of backup that copies only the files that have changed since the last full backup; 5) a type of backup when users choose which folders and files to include in a backup; 6) in a location separate from where you typically store or use your computer or mobile device; 7) a type of backup that is used only by large enterprises to back up data to an in-house network storage device purchased and maintained by the enterprise; 8) a type of backup when files are backed up to the cloud as they change; 9) a type of backup that copies only the files that have changed since the last full or incremental backup; 10) a duplicate of a file, program, or media that can be used if the original is lost, damaged, or destroyed.

5. Choose the correct answer.

1. The aim of the text is to describe...
   a) the process of hardware theft and vandalism;
   b) different physical access controls;
   c) different safeguards against hardware theft, vandalism and data loss;
   d) a device-tracking app.
2. The text highlights that …
   a) backing up is the ultimate safeguard against data loss;
   b) alarm system is the ultimate safeguard against data loss;
   c) cloud storage is the ultimate safeguard against data loss;
   d) physical security devices are the ultimate safeguard against data loss.
3. The disadvantage of differential backup is that …
   a) it has the longest backup time;
   b) it requires minimal storage space to back up;
   c) the recovery is time-consuming;
   d) it's the least manageable of all the backup methods.
4. The advantage of continuous data protection is that …
   a) the recovery of data is very fast;
   b) it's very expensive;
   c) it requires a great amount of storage;
   d) it requires an Internet connection.
5. A three-generation backup policy consists of three stages referred to as …
   a) the great-grandparent, the parent, the sibling;
   b) the grandparent, the parent, the child;
   c) the father, the mother, the kid;
   d) the cousin, the nephew, the child.
6. More customers are opting for cloud backup because …
   a) it saves them the cost of maintaining hardware;
   b) it's the best backup ever;
   c) it's the most reliable and confidential;

d) it provides only backup and retrieval services.

7. The word *random* in this text is closest in meaning to:

a) made, done, or happening without method or conscious decision;

b) governed by or involving equal chances for each item;

c) unfamiliar or unspecified;

d) unexpected or unusual.

8. The word with an opposite meaning to *continuous* is:

a) perfect;

b) intermittent;

c) permanent;

d) ongoing.

9. Which is the best way to translate the following sentence into Ukrainian:

Keeping backup copies off-site minimizes the chance that a single disaster, such as a fire, would destroy both the original and the backup media.

a) Зберігання резервних копій за межами сайту знижує імовірність того, що така катастрофа, як пожежа, знищить як оригінальні, так і резервні носії.

b) Зовнішнє зберігання резервних копій зменшує імовірність того, що таке окреме лихо, як пожежа, знищить як оригінальні, так і резервні носії.

c) Позасистемне зберігання резервних копій зменшує імовірність окремих пожеж та знищення оригінальних та резервних носіїв.

d) Зберігання резервних копій за межами сайту знижує імовірність того, що така катастрофа, як пожежа, знищить обидва – оригінальний і резервний носії.

10. Which is the odd one?

You should take measures to protect computers and devices from …

a) theft;

b) vandalism;

c) failure;

d) bugs.

6. Translate the following sentences into Ukrainian. Use the dictionary if necessary.

1. It is very difficult to prevent both theft and vandalism for one piece or set of hardware. 2. Hardware vandalism can take form from someone aimlessly smashing computers at an institution, to someone cutting a computer cable. 3. The people, who are mainly at risk in this area, are organizations that house many computers, and people with mobile devices as the size makes it especially easy to steal. 4. Thieves often aim for notebooks of company executives, as they can access confidential company information for their own personal gain. 5. Software and information or identity theft, can be associated with hardware theft. 6. Physical access controls, such as locked doors and windows, are a good way to protect a mass amount of hardware equipment. 7. Alarm systems go off when someone enters a room. 8. Physical security devices, such as cables, allow a user to lock their equipment to a desk, drawer or even the floor. 9. Implementing the requiry of a password or biometrics, to unlock mobile devices makes the device useless to the thieves. 10. It does not guard against vandalism.

7. a) Render the text in English.

Для сучасної людини банкомат є звичним способом використання банківських послуг. Важко повірити, що ще 49 років тому отримати гроші можна було тільки в банку, заздалегідь зробивши запит до установи. Першими скористались можливістю знімати кошти з рахунків за допомогою банкомату мешканці Лондона 27 червня 1967

року. З того часу кількість банкоматів на планеті зросла до понад 3 мільйонів та збільшується в середньому на 280 нових пристроїв щодня. Як наслідок, банкомати почали привертати увагу не тільки користувачів, але й злочинців. Потенційна нажива штовхала злочинців на спроби дістатися до грошей у будь-який спосіб – від'єднавши пристрій від стіни чи забравши все разом, застосувавши фізичну силу.

З часом деякі зловмисники почали обирати більш складні методи, такі як створення фіктивних частин для приладів, скімерів, які досить важко виявити. До них відносяться підроблені панелі, дисплеї, PIN-підкладки, прорізи для прийняття картки, приховані камери або ж комбінації методів. Таким чином злочинці отримували можливість використовувати вкрадені дані, щоб від імені жертви зняти гроші з рахунку або ж продати інформацію онлайн. Сучасні ж зловмисники, крім перевірених часом схем, використовують також недоліки програмного забезпечення банкоматів. У деяких випадках злам приладу не потребує значних зусиль. Багато банкоматів усе ще працюють на застарілому або незахищеному програмному забезпеченні, такому як Windows XP або Windows XP Embedded (станом на 2014 рік дане програмне забезпечення було інстальоване на 95% приладів всього світу).

Нині для викрадення готівки кіберзлочинці вдаються до різних хитрощів. Одна з них полягає в підключенні через USB-порти банкомата, приховані за зовнішньою оболонкою, з подальшим встановленням шкідливого програмного забезпечення, яке видаватиме гроші. Деякі банкомати все ще автоматично запускають будь-які підключені пристрої USB і тому вразливі до інфікування. Минулого року скімери винайшли новий тип шахрайства – «чорний ящик». Після відключення банкомата від ядра пристрою, вони з'єднують з ним власний портативний комп'ютер, який надає команди для видачі готівки.

(https://eset.ua/ua/news/view/464/Cash-machines)

b) Consider this:

1. Do you know any other ways, except those described in the text, used by cybercriminals to steal money from the ATMs? 2. What measures should be taken by cybersecurity experts of the bank to protect their equipment and money from thieves? 3. What should users do not to become victims of information theft when withdrawing money from ATMs?

8. a) Look throug the table below; b) study the information concerning the main pros and cons of different backup methods; c) prepare a short presentation based on the results of this analysis (suggest the best backup method and substantiate your choice with all necessary characteristics).*

Various Backup Methods

Type of Backup	Description	Advantages	Disadvantages
Full backup	Copies all of the files on media in the computer	Fastest recovery method. All files are saved.	Longest backup time.
Differential backup	Copies only the files that have changed since the last full backup.	Fast backup method. Requires minimal storage space to back up.	Recovery is time-consuming because the last full backup plus the differential backup are needed.
Incremental backup	Copies only the files that have changed since the last full or incremental backup	Fastest backup method. Requires minimal storage space to back up. Only most recent changes	Recovery is most time-consuming because the last full backup and all incremental backups since

		saved.	the last full backup are needed.
Selective backup	Users choose which folders and files to include in a backup.	Fast backup method. Provides great flexibility.	Difficult to manage individual file backups. Least manageable of all the backup methods.
Continuous data protection (CDP)	All data is backed up whenever a change is made	The only real-time backup. Very fast recovery of data.	Very expensive and requires a great amount of storage.
Cloud backup	Files are backed up to the cloud as they change	Cloud backup provider maintains backup hardware. Files may be retrieved from anywhere with an Internet connection on any device.	Requires an Internet connection, otherwise files are marked for backup when the computer goes back online

*9. * Internet Research*

- Browse the free web resources to search for: 'News about hardware theft and vandalism'. - be ready to present the results of your research in class in the form of written (oral) presentation or report, or 200-250-word essay (choose the form that suits you best).

10. Write a short summary of the text 'A Back Up Site', p. 84 (see the scheme in ex.10, Unit 1).

Extended Reading

(1) A Disaster Recovery Plan

A disaster recovery plan is a written plan that describes the steps an organization would take to restore its computer operations in the event of a disaster. A disaster can be natural or man-made (hackers, viruses, etc.). Each company and each department or division within an organization usually has its own disaster recovery plan. The following scenario illustrates how an organization might implement a disaster recovery plan.

Considerations for Disaster Recovery

Disaster Type	*What to Do First*	*What Might Occur*	*What to Include in the Plan*
Natural (earthquake, hurricane, tornado, etc.)	- Shut off power - Evacuate, if necessary - Pay attention to advisories - Do not use phone lines if lightning occurs	- Power outage - Phone lines down - Structural damage to building - Road closings, transportation interruptions - Flooding -Equipment damage	- Generator - Satellite phone, list of employee phone numbers - Alternate worksite - Action to be taken if employees are not able to come to work/leave the office - Wet/dry vacuums - Make and model numbers and vendor information to get replacements
Man-made (hazardous material spill, terrorist	- Notify authorities (fire departments, etc.) of immediate threat - Attempt to suppress fire	- Data loss - Dangerous conditions for employees - Criminal activity,	- Backup data at protected site - Protective equipment and an evacuation plan - Contact law enforcement

attacks, fire, hackers, malware, etc.)	or contain spill, if safe to do so - Evacuate, if necessary	such as data hacking and identity theft - Equipment damage	- Make and model numbers and vendor information to obtain replacements

Rosewood Associates is a consulting firm that helps clients use social media for marketing and customer outreach. Last week, a fire broke out in the office suite above Rosewood. The heat and smoke, along with water from the sprinkler system, caused extensive damage. As a result, Rosewood must replace all computers, servers, and storage devices. Also, the company lost all of the data it had not backed up. Rosewood currently backs up its systems daily to an internal server and weekly to a remote cloud server. Because of damage to the internal server, the company lost several days of data. Rosewood does not have a plan for replacing hardware. Thus, they will lose several additional days of productivity while purchasing, installing, and configuring new hardware. To minimize the chance of this type of loss in the future, the company hired you as a consultant to help create a disaster recovery plan. You first discuss the types of disasters that can strike, as shown in the table. You then explain that the goal of a disaster recovery plan is to prevent, detect, and correct system threats, and to restore the most critical systems first.

A disaster recovery plan typically contains these four components: emergency plan, backup plan, recovery plan, and test plan.

Emergency Plan: An emergency plan specifies the steps Rosewood will take as soon as a disaster strikes. The emergency plan is organized by type of disaster, such as fire, flood, or earthquake, and includes:

1. Names and phone numbers of people and organizations to notify (company management, fire and police department, clients, etc.)
2. Computer equipment procedures, such as equipment or power shutoff, and file removal; employees should follow these procedures only if it is safe to do so
3. Employee evacuation procedures
4. Return procedures (who can enter the facility and what actions they are to perform)

Backup Plan: The backup plan specifies how Rosewood will use backup files and equipment to resume computer operations, and includes:

1. The location of backup data, supplies, and equipment
2. Who is responsible for gathering backup resources and transporting them to an alternate computer facility
3. The methods by which data will be restored from cloud storage
4. A schedule indicating the order and approximate time each application should be up and running

Recovery Plan: The recovery plan specifies the actions Rosewood will take to restore full computer operations. As with the emergency plan, the recovery plan differs for each type of disaster. You recommend that Rosewood set up planning committees. Each committee would be responsible for different forms of recovery, such as replacing hardware or software.

Test Plan: The test plan includes simulating various levels of disasters and recording Rosewood's ability to recover. You run a test in which the employees follow the steps in the disaster recovery plan. The test uncovers a few needed recovery actions not specified in the plan, so you modify the plan. A few days later, you run another test without giving the employees any advance notice to test the plan again.

Consider This: 1. What kinds of natural and man-made disasters should a company take into consideration? 2. What roles can cloud storage providers play in helping to recover from

a disaster? 3. How involved should employees be in developing and testing disaster recovery plans?

(2) A Back Up Site

A backup site or work area recovery site is a location where an organization can relocate following a disaster, such as fire, flood, terrorist threat or other disruptive event. This is an integral part of the disaster recovery plan and wider business continuity planning of an organization. A backup, or alternate, site can be another data center location operated by the organization, or contracted via a company that specializes in disaster recovery services. In some cases, one organization will have an agreement with a second organization to operate a joint backup site. In addition, an organization may have a reciprocal agreement with another organization to set up a warm site at each of their data centers.

There are three types of backup sites, including cold sites, warm sites, and hot sites. The differences between the types are determined by the costs and effort required to implement each. Cold sites are mere empty operational spaces with basic facilities like raised floors, air conditioning, power and communication lines etc. On occurring of an incident and if the operations can do with a little down time, alternate facilities are brought to and set up in the cold site to resume operations. A cold site is the least expensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. The lack of provisioned hardware contributes to the minimal start-up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster. In some cases, a cold site may have equipment available, but it is not operational.

A warm site is a compromise between hot and cold. These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites might have backups on hand, but they may not be complete and may be between several days and a week old. The recovery will be delayed while backup tapes are delivered to the warm site, or network connectivity is established and data is recovered from a remote backup site.

A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Following a disruption to the original site, the hot site exists so that the organization can relocate with minimal losses to normal operations in the shortest recovery time. Ideally, a hot site will be up and running within a matter of hours. Personnel may have to be moved to the hot site, but it is possible that the hot site may be operational from a data processing perspective before staff has relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organization's requirements. This type of backup site is the most expensive to operate. Hot sites are popular with organizations that operate real time processes such as financial institutions, government agencies and eCommerce providers. The most important feature offered from a hot site is that the production environment(s) is running concurrently with the main datacenter. This syncing allows for minimal impact and downtime to business operations. In the event of a significant outage event, the hot site can take the place of the impacted site immediately. However, this level of redundancy does not come cheap, and businesses will have to weigh the cost-benefit-analysis (CBA) of hot site utilization. Nowadays if the backup site is down and misses the "proactive" approach it may not be considered a hot site depending on the level of maturity of the organization regarding the ISO 22301 approach (international standard for Business

Continuity Management). Generally, an Alternate Site refers to a site where people and the equipment that they need to work is relocated for a period of time until the normal production environment, whether reconstituted or replaced, is available.

(https://en.wikipedia.org/wiki/Backup_site)

(3) Ex-Telstra employee jailed for $250k hardware theft

A former *Telstra* account executive has been sentenced to three years' imprisonment after stealing more than $250,000 worth of hardware. Judge Julia Wager handed Jaime Kim Guan Neoh his sentence at a Perth district court on last week, ruling he will be eligible for parole after serving 18 months. "It costs the company and the community a lot if those they employ are not honest - and it's for these reasons that significant terms of imprisonment must result," Wager said. The court heard that over nine months, Neoh entered hardware purchase requests under the name of two *Telstra* customers: IT services provider *Swift Technology and Tap Oil Limited*, an oil and gas exploration company headquarted in Perth.

A total of 263 mobile phones, 13 tablets, four electronic devices and a tablet case were received by Neoh, who then resold or gave out the items as gifts. The stolen devices added up to a total value of $256,466. Of this, $231,054 was entered under the Swift Technology account alone. "You wanted to impress others and give the appearance of being highly successful," Wager said in sentencing Neoh. "You used the items you obtained to give out as gifts to your family, to others or to pay for meals and present a lavish lifestyle to others including clients." Telstra declined to comment on the case.

The thefts occurred between January and September 2014. Neoh placed the orders through his sales team, by telephone, on the internet and other means, even instructing a junior staff member to create a second account in the name of an existing customer and change the details later. Neoh claimed his actions were in order to maintain a "certain lifestyle". At Telstra, he was on a $99,000 yearly salary. He pocketed up to $90,000 from the sale of the stolen devices. Neoh joined Telstra in 2003 as a contractor and switched to permanent full time in 2005. He was promoted several times until eventually landing the account executive role in February 2013, for which he was responsible for more than 70 business customers. It was only when Tap Oil requested to terminate its contract with Telstra and a negative balance related to a loyalty program appeared that the telco started internal investigations. The enquiry discovered that Neoh had forged an authorised signature for that account. Neoh was interviewed three times on the matter before he admitted his acts to a manager. After several meetings, Telstra terminated his employment on October 2014.

(https://www.itnews.com.au/news/ex-telstra-employee-jailed-for-250k-hardware-theft-430251)

Unit 9. Wireless Security

Pre-Reading Activities
Answer the questions.

1. Why might it be a good idea to secure your wireless network in addition to safeguarding the data and information on your computers from others,? 2. Can you detect if someone is accessing your wireless home network? 3. What are some safeguards to secure a wireless network? 4. Have you got a wireless home network? 5. What are some guidelines to protect your mobile device data?

1. a) Read the texts using the dictionary; b) translate the underlined words and word combinations into Ukrainian (in writing); c) pay attention to the terminological units in bold type. Be sure you can give their definition in English and their Ukrainian equivalents.

Wireless Security

Billions of home and business users have laptops, smartphones, and other mobile devices to access the Internet, send email and Internet messages, chat online, or share network connections – all **wirelessly**. Home users set up **wireless home networks**. Mobile users access wireless networks in hot spots at airports, hotels, shopping malls, bookstores, restaurants, and coffee shops. Schools have wireless networks so that students can access the school network using their mobile computers and devices as they move from building to building.

Although wireless access provides many conveniences to users, it also poses additional **security risks**. Some perpetrators connect to other's wireless networks to gain free Internet access; others may try to access an organization's confidential data. To access a wireless network, the individual must be in range of the wireless network. Some intruders intercept and monitor communications as they transmit through the air. Others connect to a network through an **unsecured wireless access point** (WAP) or **combination router**.

Secure Your Wireless Network

When you set up a wireless network, it is important to secure the network so that only your computers and mobile devices can connect to it. Unsecured wireless networks can be seen and accessed by neighbors and others nearby, which may make it easier for them to connect to and access the data on the computers and mobile devices on your network. The following list provides suggestions for securing your wireless network.

• Immediately upon connecting your **wireless access point** and/or **router**, change the password required to access administrative features. If the password remains at its default setting, others may possibly be able to connect to and configure your wireless network settings.

• Change the SSID (**service set identifier**), which is a network name, from the default to something that uniquely identifies your network, especially if you live in close proximity to other wireless networks.

• Do not broadcast the SSID. This will make it more difficult for others to detect your wireless network. When you want to connect a computer or mobile device to your wireless network, it will be necessary to enter the SSID manually.

• Enable an **encryption method** such as WPA2 (**Wi-Fi Protected Access** 2), and specify a password or passphrase that is difficult for others to guess. The most secure passwords and passphrases contain more than eight characters, uppercase and lowercase letters, numbers, and special characters.

• Enable and configure the **MAC (Media Access Control) address control feature**. A MAC address is a unique hardware identifier for your computer or device. The MAC address control feature specifies the computers and mobile devices that can connect to your network. If a computer or device is not specified, it will not be able to connect.

• Choose **a secure location** for your wireless router so that unauthorized people cannot access it. Someone who has physical access to a wireless router can restore factory defaults and erase your settings.

If you notice the speed of your wireless connection is slower than normal, it may be a sign that someone else is accessing your network. You also may notice indicator lights on your wireless router flashing rapidly when you are not connected to your wireless network. Most wireless routers have a built-in utility that allows you to view the computers currently connected to your network. If you notice a computer that does not belong to you, consult your wireless router's documentation to determine how to remove it from the network.

3. Translate the following word combinations.

a) into Ukrainian:

1) to set up wireless home networks; 2) to provide conveniences to users; 3) to pose additional security risks; 4) to be in range of the wireless network; 5) to monitor communications; 6) to access administrative features; 7) to remain at its default setting; 8) to configure wireless network settings; 9) to change the SSID (service set identifier); 10) to uniquely identify one's network.

b) into English:

1) жити дуже близько від; 2) поширювати ідентифікатор безпровідної мережі; 3) виявити безпровідну мережу; 4) увімкнути метод шифрування; 5) встановити пароль або фразу-пароль, який іншим важко розгадати; 6) містити більше восьми символів, великих та малих літер, цифр та спеціальних символів; 7) увімкнути та налаштувати функцію керування адресою MAC; 8) визначити комп'ютери та мобільні пристрої, які можуть підключатися до вашої мережі; 9) мати фізичний доступ до; 10) відновити заводські налаштування за замовчуванням.

4. Choose from the box the appropriate Ukrainian equivalent to the following words and word combinations.

Видалити налаштування, вбудована утиліта, в межах, ідентифікатор безпровідної мережі, безпечне місце розташування, керування доступом до середовища передачі, функція керування, вручну, безпечний пароль, спеціальні символи, розповсюджувати, задіяти, комбінований маршрутизатор, незахищені безпровідні мережі, незахищена точка безпровідного доступу, великі літери, малі літери, перехоплювати і відстежувати, мати доступ до адміністративних функцій, світловий індикатор

1.	uppercase letters	
2.	unsecured wireless networks	
3.	a secure location	
4.	a combination router	
5.	in range of	
6.	unsecured wireless access point	
7.	Media Access Control	
8.	to erase settings	
9.	lowercase letters	

10.	built-in utility	
11.	indicator light	
12.	manually	
13.	to broadcast	
14.	special characters	
15.	to intercept and monitor	
16.	a secure password	
17.	service set identifier	
18.	to access administrative features	
19.	to enable	
20.	a control feature	

5. What do we call:

1) the address that is a unique hardware identifier for your computer or device; 2) a network name; 3) a preselected option adopted by a computer program or other mechanism when no alternative is specified by the user or programmer; 4) by hand rather than automatically or electronically; 5) a network having no wire; 6) a word or other string of characters, sometimes kept secret or confidential, that must be supplied by a user in order to gain full or partial access to a computer, computer system, or electronic device; 7) a capital letter; 8) a hardware device that routes data (hence the name) from a local area network (LAN) to another network connection; 9) the manner in which something is set; 10) a networking hardware device that allows a Wi-Fi device to connect to a wired network.

6. *Choose correct answers.*

1. The text (ex.1) describes…
   a) ways to secure a wireless network;
   b) the advantages of a wireless network over a physical network;
   c) the most reliable passwords and password phrases;
   d) a secure location for your wireless router.
2. To access a wireless network, the individual must …
   a) intercept wireless signals;
   b) be in range of the wireless network;
   c) choose a secure location;
   d) enable an encryption method.
3. The MAC address control feature …
   a) changes the SSID;
   b) changes the password required to access administrative features;
   c) specifies the computers and mobile devices that can connect to your network;
   d) broadcasts the SSID.
4. While configuring a wireless network, we shouldn't …
   a) change the SSID;
   b) enable and configure the MAC;
   c) choose a secure location for your wireless router;
   d) broadcast the SSID.
5. The word *required* is opposite in meaning to …
   a) all-important;
   b) essential;
   c) unnecessary;

d) needed.

6. The word *manual* is close in meaning to…

a) done by hand;

b) automatic;

c) artificial;

d) guided.

7. According to the text, if the password remains at its default setting…

a) others may possibly be able to connect to your wireless network;

b) others may possibly have physical access to a wireless router;

c) others may possibly access wireless networks in hot spots at airports, hotels, cafes, etc.;

d) others may possibly determine how to remove it from the network.

8. The most secure password should contain …

a) less than eight lowercase letters;

b) more that eight different uppercase characters;

c) less than eight lowercase numbers and uppercase asterisks;

d) more than eight characters, uppercase and lowercase letters, numbers, and special characters.

9. WPA2 is …

a) an encryption method;

b) a router identifier;

c) a wireless access point;

d) a special software.

10. Which is the best way to translate the following sentence into Ukrainian:

If the password remains at its default setting, others may possibly be able to connect to and configure your wireless network settings.

a) Якщо пароль залишається на своїх замовчуваних налаштуваннях, інші можуть, можливо, мати змогу підключитися та налаштовувати параметри бездротової мережі.

b) Якщо замовчувати залишений пароль налаштувань, то інші, можливо, спроможуться підключитися та конфігурувати параметри безпровідної мережі.

c) Якщо залишити пароль, встановлений за замовчуванням, інші зможуть під'єднатися до вашої безпровідної мережі і змінити її налаштування.

d) Зміни пароль за замовчуванням налаштування і ніхто можливо не зможе під'єднатися до мережі та змінити налаштування.

7. a) Render the text below in Ukrainian. Use the dictionary if necessary.

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks.

The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Hackers had not yet had time to latch on to the new technology, and wireless networks were

not commonly found in the work place. However, there are many security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Hacking methods have become much more sophisticated and innovative with wireless access. Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A hacker could sit out in the parking lot and gather information from it through laptops and/or other devices, or even break in through this wireless card-equipped laptop and gain access to the wired network.

b) Consider this:

1. What are other types of wireless security? (*Browse the Internet to find the necessary information*). 2. Why is it so important to address wireless security concerns nowadays? Give your reasons. 3. Do you use the possibility of wireless networking? Do you enter the corporate wireless network or do you have this popular technology at your service at home? 4. Do you care for your wireless network security? What do you do to ensure your network security?

8. a) Render the following text in English.

WEP (Wired Equivalent Privacy) – технологія, розроблена спеціально для шифрування потоку даних в локальній мережі. Це застаріла технологія, але до 2003 року вона було єдиною.

WPA (WiFi Protected Access) має більш стійкий алгоритм шифрування, ніж WEP. Високий рівень безпеки досягається за рахунок використання протоколів TKIP і MIC. MIC – технологія перевірки цілісності повідомлень – захищає від перехоплення пакетів і їх перенаправлення. Стандарт TKIP використовує автоматично підібрані 128-бітні ключі, які створюються непередбачуваним способом, і їх загальна варіація сягає 500 млрд. Складна ієрархічна система алгоритму підбору ключів і їх динамічна зміна через кожні 10 КБ роблять систему максимально захищеною. *WPA2* створений на основі попередньої версії, WPA. Враховуючи деякі зміни і доповнення в цьому методі шифрування, вважають, що він зможе ще більше підвищити безпеку мереж. WPA2 не має недоліків (відомих на сьогоднішній день), а тому єдиний спосіб проникнення в мережу – прямий підбір пароля. І тут уже все залежить від якості пароля.

Використання технологій *приватних віртуальних тунелів (VPN)* вважають найкращим методом захисту в WiFi мережах. І хоч ця технологія розроблялась для захищеного підключення до Інтернету через загальнодоступні канали, вона непогано зарекомендувала себе і в бездротових локальних мережах. Суть цієї технології полягає в тому, що створюються «безпечні» канали від клієнта до заданого вузла. Для шифрування трафіка в VPN використовується протокол IPSec. На сьогоднішній день не зафіксовано випадків злому VPN-мереж. Застосування цієї технології рекомендується в корпоративних мережах, тому що для домашнього користування встановлення і налаштування може виявитись важким і громіздким. Крім того, при використанні цієї технології доведеться пожертвувати близько 35% пропускної здатності каналу.

b) Think of the possible title to the text.

c) Browse the Internet to find more information about VPNs. Present the results of your search.*

*9. * Internet Research*

- Browse the free web resources to search for: 'Wireless security at organizations'.

- Be ready to present the results of your research in class in the form of oral presentation / 200-250-word essay (choose the form that suits you best).

10. *Write a short summary of the text 'How Mobile Security Works', p. 92 (see the scheme in ex.10, Unit 1).*

Extended Reading

(1) Mobile Security

The consequences of losing a smartphone or mobile device are significant given the amount of storage and the variety of personal and business data stored. Symantec, one the world's leading online security companies, projects that only one-half of lost or stolen phones eventually will be returned to their owners. Chances are that the people who find the missing phones likely will have viewed much of the content on the devices in a quest to find the owners and possibly to gain access to private information. The goal, therefore, for mobile device users is to make their data as secure as possible. Follow these steps to protect sensitive and personal data and to fight mobile cybercrime.

Be extra cautious locating and downloading apps.

Any device that connects to the Internet is susceptible to mobile malware. Cyberthieves target apps on widely used phones and tablets. Popular games are likely candidates to house malware, and it often is difficult to distinguish the legitimate apps from the fake apps. Obtain mobile device apps from well-known stores, and before downloading anything, read the descriptions and reviews. Look for misspellings and awkward sentence structure, which could be clues that the app is fake.

If something looks awry, do not download. Scrutinize the number and types of permissions the app is requesting. If the list seems unreasonable in length or in the personal information needed, deny permission and uninstall the app.

Use a PIN.

Enable the passcode feature on a mobile device as the first step in stopping prying eyes from viewing contents. This four-to-eight-digit code adds a layer of protection. Only emergency functions can be accessed without entering the correct sequence of numbers. This strong code should not be information easily guessed, such as a birthdate.

Turn off GPS tracking.

GPS technology can track the mobile device's location as long as it is transmitting and receiving signals to and from satellites. This feature is helpful to obtain directions from your current location, view local news and weather reports, find a lost device, summon emergency personnel, and locate missing children. Serious privacy concerns can arise, however, when the technology is used in malicious ways, such as to stalk individuals or trace their whereabouts. Unless you want to allow others to follow your locations throughout the day, disable the GPS tracking feature until needed.

Use mobile security software.

Protection is necessary to stop viruses and spyware and to safeguard personal and business data. Mobile security apps can allow you to lock your mobile device and SIM card remotely, erase the memory, and activate the GPS function. Other apps prevent cyberthieves from hijacking your phone and taking pictures, making recordings, placing calls to fee-imposed businesses, and sending infected messages to all individuals in your contact list. Look for security software that can back up data to a cloud account, set off a screeching alarm

on the lost or stolen mobile device, offer live customer service, and provide theft, spam, virus, and malware protection.

Avoid tapping or clicking unsafe links.

Tapping or clicking an unknown link can lead to malicious websites. If you receive a text message from someone you do not know or an invitation to tap or click a link, resist the urge to fulfill the request. Your financial institution never will send you a message requesting you to enter your account user name and password. Malicious links can inject malware on the mobile device to steal personal information or to create toll fraud, which secretly contacts wireless messaging services that impose steep fees on a monthly bill.

Consider This:

1. As the number of smartphones and mobile devices in use increases, the possibility of security breaches and lost devices increases proportionally. How can manufacturers and wireless carriers emphasize the importance of mobile security and convince users to take the precautions suggested in this mini feature? 2. What mobile security safeguards have you taken to protect your smartphone or mobile device? 3. What steps will you take after reading this mini feature?

(2) How Mobile Security Works

by Dave Roos

You'd protect your computer from hackers and other online predators, and it may be time to consider the security of your smart phone. Unfortunately, consumers aren't the only ones making the shift to mobile devices. Malicious hackers and identity thieves are following close behind. As more and more people use their smartphones and other mobile devices to do online banking, pay bills, and store critical personal and business information, more and more bad guys are trying to crack into this mobile gold mine.

Mobile security will be the key to winning the war against this new generation of cyber thieves. Mobile security can come in many shapes and forms. Some protections are built directly into the device you're using. For example, the iPhone ships with a default Autolock feature that requires the user to enter a password after a few minutes of inactivity [source: Sacco]. Other mobile security protections are built into the network, such as strong encryption standards for data travelling across cellular networks. But perhaps no mobile security device is as powerful as an educated consumer who keeps his or her personal information protected and avoids downloading suspicious applications or clicking on booby-trapped links.

Is Mobile Security Necessary? Mobile security is as critical as the PIN number on your ATM card or the lock on your front door. The sad truth is that there are people in this world who will exploit any security vulnerability if there's money behind the door. As mobile devices become mobile wallets, we are already seeing the rise of virtual pickpockets.

The good news is that, at least for the moment, mobile security is staying ahead of the hackers. The Internet has been widely used for 15 years, and over that time, computer security researchers and companies have devised a set of strong standards for locking out attackers. Most of these same standards have already been applied to mobile devices and data networks.

Even with mobile security standards like encryption and passcodes, mobile device users need to be aware of common mobile security threats and how to defend themselves. Keep reading for a rundown of the major mobile security threats and alerts.

Mobile Security Risks and Alerts. Malware continues to be the most dangerous threat to mobile device users. Malware is malicious software code that can steal sensitive information

like passwords and account numbers, rack up charges on your phone bill, or spread itself through your address book like a virus.

Loss and theft are two serious security threats to mobile devices. As devices get smaller, they become easier and easier to lose. And the more we rely on these devices to send and store messages, access our bank accounts and conduct business, the greater the consequences if they fall into the wrong hands. Two of the most effective mobile security measures are *remote lock* and *remote wipe*. Enterprise mobile security systems invariably include this feature, which allows a user or an IT administrator to lock the phone if lost, and even to wipe its entire memory remotely. Many devices also include GPS tracking features to locate the phone or even activate "screaming" alarms that can be heard from the bottom of a user's laundry basket.

Network security is less of a threat, since most communications over cellular data networks are strongly encrypted. One remaining threat is communicating over an unencrypted WiFi network. Be careful when sending e-mails or texts over a public WiFi network at the local café. It's possible that a WiFi "sniffer" could be listening in on the traffic and trolling for useful information.

Other security threats are common to anyone who uses e-mail or the Web. In a phishing scam, for example, a hacker will send an email posing as a legitimate bank or business and ask for the user to enter his password or some other piece of sensitive account information. As more people access their e-mail from mobile devices, they need to use the same caution they would at home or the office.

https://money.howstuffworks.com/personal-finance/online-banking/mobile-security.htm

Unit 10. Online Banking Security

Pre-Reading Activities
Answer the questions.

1. Why is online banking security important for people? 2. How often do you use it? 3. What online banking scams should people be aware of? 4. What measures do you take for secure online banking? 5. Is online banking safe in Ukraine?

1. a) Read the texts using the dictionary; b) translate the underlined words and word combinations and terminological units in bold type into Ukrainian (in writing). Be sure you can give their definition in English.

Online Banking Security

Online banking allows people to undertake traditional banking activities, like account transfers, payment of bills and requests for stopping payments, via the Internet. Customers can also keep tabs on the account balance from the comfort of their home. In this day and age, online banking has become an indispensable facility for people who are hard pressed for time and find it difficult, if not impossible, to reschedule their busy lives for the sake of making a few withdrawals and deposits. However, there are a few issues that have to be borne in mind in order to avoid being **cyberscammed**.

An online bank account is accessed with the help of a username and a password. The username and the password can be obtained by a **trickster** in one of the following ways:

Phishing: Phishing is the attempt to acquire potentially sensitive information via email, instant messages, cellphones or through **fraudulent websites** and social networking websites. Generally, a link **spoofing** the authentic bank website is sent via email, by **scammers**, to unsuspecting customers forcing the latter to divulge confidential information like username and password.

Malicious Software: Internet address redirection, which results in redirecting customers to a **copycat website** that closely resembles the original site, occurs when a malicious software has sneaked into the computer.

Weak Wireless Network Security: Most people, who access the Internet from their home, are not tech savvy. They may inadvertently allow others to access their wireless network and retrieve confidential information.

Banks usually use different means of securing transactions and personal information. A **Fraud Detection System**, for instance, looks for patterns of transactions and new behaviour which may indicate that a transaction is fraudulent. The sophisticated technology monitors your transactions and identifies suspicious activity. If fraudulent activity is detected, you'll be contacted, and your Internet Banking will temporarily be frozen in order to prevent further fraudulent transactions. Encryption is used to turn words and numbers into a coded language. Encryption prevents unauthorized users from being able to change or read your data. *TLS v1.0* (Transport Layer Security) is one of encryption technologies that are widely used. If you have not logged out your banking session, your session will be automatically **timed-out** to protect your sensitive banking information. Sending **SMS notifications** for certain high risk transactions is one such measure to ensure you have a safer, more secure banking experience. The SMS will provide you with the transaction amount, the last four digits of the payee account number and the channel. Some banks have developed **security apps** that provide you with extra security to unlock extra Internet Banking features. These security apps are compatible for Android and iPhone devices. They, for instance, allow you to generate a **one-time pass code** to authenticate certain Internet Banking payments and activities.

Safe Online Banking Practices

Using virtual keyboards: Banks provide the option of using the virtual keyboard as a measure to counteract **keylogging malware**. The customer should always use the virtual keyboard instead of the physical keyboard.

URL beginning with "https://": The website's URL should begin with "https://" rather than "http://" since the former allows the user to log in by creating a **secure channel** over an unsecured network.

Safe access: One should avoid accessing the online bank account from public computers. One should also avoid accessing the account via a public Wi-Fi from one's laptop. Moreover, a home network ensures safe and secured online banking services.

Choosing a strong password: A strong password that is at least eight characters long and uses a combination of upper and lower case letters, number, and symbols, is ideal.

Choosing **security questions**: Most bank sites allow the user to choose security questions and answers in addition to the username and password. One will be forced to answer this question in case one is accessing the account from a different/unrecognized computer. This provides additional security.

Thwarting phishing: One should avoid logging into one's account via a link that has been received in an incoming email requesting a change of username or password. This may help ward off phishing.

3. Translate the following word combinations.

a) into Ukrainian:

1) to undertake traditional banking activities, like account transfers, payment of bills and requests for stopping payments; 2) to keep tabs on the account balance; 3) to be hard pressed for time; 4) to reschedule busy lives for the sake of making a few withdrawals and deposits; 5) to be cyber scammed; 6) to acquire potentially sensitive information; 7) to divulge confidential information; 8) to retrieve confidential information; 9) to prevent further fraudulent transactions; 10) to log out or exit a banking session.

b) into English:

1) переривати сесію по часу; 2) щоб розблокувати додаткові функції Інтернет-банкінгу; 3) для автентифікації певних платежів в Інтернет-банку; 4) протидіяти шкідливому ПЗ, яке стежить за натиснутими клавішами клавіатури; 5) уникати доступ до рахунку через загальнодоступний Wi-Fi; 6) забезпечувати додаткову безпеку; 7) перешкоджати фішингу; 8) забезпечувати безпечні онлайн-банківські послуги; 9) надавати можливість використання; 10) вибрати надійний пароль.

4. Choose from the box the appropriate Ukrainian equivalent to the following words and word combinations.

Невід'ємна послуга, сайт-підробка, імітація підключення, випитування (конфіденційної інформації), технологічно «підкований», секретне/контрольне запитання, безпечний канал, система виявлення шахрайства, безпекове ПЗ, номер рахунку одержувача платежу, шахрай, прокрастися, шахрайські веб-сайти, ПЗ, яке стежить за натиснутими клавішами клавіатури, SMS-сповіщення, ризиковані транзакції, нерозпізнаний комп'ютер, одноразовий код доступу, сумісний в роботі, уникнути, ненавмисно, складна технологія.

1.	one-time pass code	
2.	phishing	

3.	to sneak	
4.	copycat website	
5.	security questions	
6.	high risk transactions	
7.	indispensable facility	
8.	SMS notifications	
9.	tech savvy	
10.	fraudulent websites	
11.	spoofing	
12.	secure channel	
13.	keylogging malware	
14.	unrecognized computer	
15.	fraud detection system	
16.	compatible	
17.	payee account number	
18.	ward off	
19.	inadvertently	
20.	security app	
21.	sophisticated technology	
22.	scammer	

5. What do we call:

1) the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication; 2) a type of scam where an intruder attempts to gain unauthorized access to a user's system or information by pretending to be the user; 3) is at least eight characters long and uses a combination of upper and lower case letters, number, and symbols; 4) a question answered in case one is accessing the account from a different/unrecognized computer; 5) malware that records the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored; 6) someone who makes money using illegal methods, especially by tricking people; 7) an app that provides you with extra security to unlock extra features; 8) obtained, done by, or involving deception, especially criminal deception; 9) a communications protocol for secure communication over a computer network which is widely used on the Internet; 10) any software that brings harm to a computer system.

6. *Choose correct answers (see the text, ex.1).*

1. The text deals with …
   a) some ways of obtaining bank account password and username;
   b) safe online banking practices;
   c) measures undertaken by a bank to prevent banking scams;
   d) types of banking transactions.
2. The main items discussed in the text are:
   a) the importance of online banking in our daily life;
   b) the questions why we should follow safe online banking practices;
   c) fishing and writing emails;
   d) phishing and spoofing.

3. The main idea of the text is:
a) to educate students on online banking threats and safe practices;
b) to encourage people to use online banking services;
c) to show some statistics and data of online banking practices;
d) to entertain students.
4. The word *inadvertently* in similar in meaning to:
a) accidentally;
b) unintentionally;
c) purposefully;
d) intentionally.
5. The word *savvy* means:
a) intelligent;
b) clever;
c) canny;
d) unaware of.
6. A word combination similar to *sophisticated technology* is:
a) complex technology;
b) simple technology;
c) skillful technology;
d) rare technology.
7. According to the text:
If you have not logged out your banking session, your session will be automatically timed-out to protect your sensitive banking information.
a) True;
b) False.
8. One should log into one's account via a link that has been received in an incoming email requesting a change of username or password.
a) True;
b) False.
9. Fraud Detection System…
a) traces patterns of transactions and new behaviour which may indicate that a transaction is fraudulent;
b) looks for drawbacks in the system;
c) reboots the system;
d) is a useful utility.
10. What is the best way to translate this sentence into Ukrainian?
Customers can also keep tabs on the account balance from the comfort of their home.
a) Клієнти також можуть зберігати вкладки на баланс облікового запису з комфорту свого будинку.
b) Клієнти також можуть стежити за балансом рахунку, зручно влаштувавшись вдома.
c) Клієнту комфортно користуватись онлайн банкінгом з дому.
d) Клієнт слідкує за змінами на рахунку з комфорту свого дому.

7. a) Render the following text in Ukrainian.

With technology getting more and more advanced, banks are outdoing each other in adding banking services that can be accessed across various platforms and applications. Unfortunately, with the tough economic times, cyber crooks and fraudsters are also growing

more tech-savvy nowadays and this has led to the rise of scams victimizing hapless online banking customers. Although many online banking consumers are now aware of what phishing is, a lot of them still fall victim to it. In electronic frauds, phishing is perhaps the oldest form of identity theft where scammers send out an authentic-looking email that purportedly comes from the victim's bank, requesting him or her to update his or her account information for various official-sounding reasons. The client will then be asked to click on a link that is supposed to direct him to the bank's website but instead takes him to a site that looks exactly like the bank site but is actually a fraudulent one, where the scammers can record whatever pertinent data the client enters. To avoid being conned into a phishing scam, never click on links for bank account updates.

Stealing, cracking, or guessing passwords is another method widely-used by hackers to gain access to bank accounts or financial transactions. Studies have shown that the more experienced and technologically advanced of these hackers can make about one billion guessing attempts in one second. The best prevention bank customers have against these attacks is to use more secure passwords. A 5-character password can be cracked in 10 seconds, while an 8-character can only be correctly guessed in 115 days.

b) Think of the possible title for the text.
c) Formulate the main idea and a topic sentence of the text.*

8. a) Render the text in English:

Шахраї надсилають потенційній жертві лист з банку або платіжної системи, наприклад, PayPal. У листі написано, що з рахунком жертви є якісь проблеми, для вирішення яких необхідно пройти по посиланню з листа. Найчастіше ця вимога супроводжується загрозою блокування банківського рахунку. Посилання, як правило, веде на фальшивий сайт банку — як правило, він виглядає в точності, як справжній сайт, та і адреса відрізняється лише однією літерою. Довірлива жертва вводить справжні логін та пароль, тим самим повідомляючи їх шахраям. Мільйони людей попадаються на цю вудку щорічно. Фішингом цей метод називається від англійського fishing (рибалка), тому що шахраї розсилають такі листи сотнями тисяч з надією, що знайдуться довірливі користувачі, які клюнуть на них. Популярний у США і Канаді метод мережевого шахрайства. Жертва отримує електронний лист з пропозицією отримати кредитну картку з великим лімітом і надзвичайно низькою процентною ставкою. Як тільки жертва перераховує шахраям пару десятків доларів, вони тут же зникають.

b) Browse the Internet in search for some more information concerning security measures to prevent phishing. Present the result of your search in class.

*9. * Internet Research*

- Browse the free web resources to search for 'Online Banking Scams'.

- Be ready to present the results of your research in class in the form of PowerPoint Presentation / written (oral) report / 200-250-word essay (choose the form that suits you best).

10. *Write a short summary of the text 'How secure are mobile banking apps?', p. 99 (see the scheme in ex.10, Unit 1).*

Extended Reading

(1) Designing Fraud-Detection Architecture That Works Like Your Brain Does

At its core, fraud detection is whether people are behaving "as they should," otherwise known as catching anomalies in a stream of events. This goal is reflected in diverse applications such as detecting credit-card fraud, flagging patients who are doctor shopping to obtain a supply of prescription drugs, or identifying bullies in online gaming communities.

To understand how to design effective fraud-detection architecture, one needs to examine how the human brain learns to detect anomalies and react to them. As it turns out, our brains have multiple systems for analyzing information. (If you are interested in how humans process information, we recommend the book *Thinking Fast and Slow*, by Daniel Kahneman).

Consider a game of tennis, where the players have to detect the arriving ball and react to it appropriately. During the game, players have to perform this detection-reaction loop incredibly fast; there is no time to think, and reactions are based on instinct and very fast pattern detection. Between sets, a player may have a moment or two to reflect upon the game's progress, identify tactics or strategies the other player is using, and make adjustments accordingly. Between games, the players have much time for reflection: they may notice that a particular aspect of their game is consistently weak and work on improving it, so during the next game they can instinctively perform better. (Note that this reflection can be conscious or unconscious. We have all occasionally spent hours trying to solve a challenging problem, only for the solution to materialize during the morning shower while we are thinking of nothing in particular.)

In a similar fashion, effective fraud-detection architecture emulates the human brain by having three subsystems work together to detect anomalies in streams of events:

Near real-time system: the job of this system is to receive events and reply as fast as possible, usually in less than 100ms. This system typically does very little processing and depends mostly on pattern matching and applying predefined rules. Architectural design should focus on achieving very high throughput with very low latency, and to this end, use patterns such as caching of user profiles in local memory.

Stream-processing systems: this system can take a little longer to process the incoming data, but should still process each even within few seconds to few minutes of its arrival. The goal of this system is to adjust parameters of the fraud-detection models in near real-time, using data aggregated across all user activity (for example, flagging vendors or regions that are currently more suspicious).

Offline-processing system: this system can run in anything from hours to months of latency and focuse on improving the models themselves. This process includes training the models on new data, exploring new features in the data, and developing new models. It also requires that human data analysts explore the data using BI tools.

(http://blog.cloudera.com)

(2) How secure are mobile banking apps?

Do banking institutions have a good handle on the things they need to remediate and new control layers they need to adopt to keep users secure?

To answer those questions, Accenture and NowSecure have performed vulnerability assessments of customer-facing mobile banking apps of 15 banking institutions in the North American market.

They have tested the iOS and Android app versions of each of these banks, and found that every app they tested had at least one security issue.

"Of the 465 tests completed for banking apps running on Android, 44 or nine percent had low security issues; 48 or 10 percent had medium security issues; and 10 or two percent had high level security issues. For banking apps running on iOS, a total of 315 tests indicated 24 or eight percent low level security issues; 13 or four percent with medium level issues; and none with high level issues," they noted.

Security risks

Among the security risks identified were:

- World-writable files (i.e. other apps can have write access to the files)
- Broken SSL check / sensitive data in transit (i.e. unencrypted communications). Curiously enough, none of the tested iOS apps had this problem
- Writable executables – a failing that can be combined with other issues and lead to additional app vulnerabilities, including remote code execution ones.
- Lack of obfuscation of the app source code, allowing for easy reverse-engineering (some 60% of the tested Android banking apps are guilty of this)
- Weak SecureRandom implementation
- Dynamic code loading
- Inappropriately set "HttpOnly" flag (to prevent XSS attacks)
- Inappropriately set "Secure" flag (to prevent the sending of cookies over insecure channels)
- TLS traffic with sensitive data (80% of tested iOS banking apps had sensitive values intercepted while proxying SSL and Transport Layer Security (TLS) app communications (i.e. username, password, GPS coordinates, etc.)
- Lack of app transport security (60% of tested iOS banking apps had ATS globally disabled, which allows a connection regardless of HTTP or HTTPS configuration, connection to servers with lower TLS versions and a connection using cipher suites that do not support forward secrecy).

Based on this and other historical app security assessments, the researchers have concluded that banking institutions have been proactive when it came to remediating well-known critical security issues such as Heartbleed, MITM exposure and others, but less so in regards to the above noted security risks.

Many of the institutions have also introduced multi-factor authentication for online banking (a good step), but chose to leverage SMS technology to deliver authentication codes.

(https://www.helpnetsecurity.com/2017/04/27/mobile-banking-security/)

(3) Is Online Banking Safe?

by Wesley Fenlon

Online banking is simple and convenient, but is it really as safe as banking in person with a teller. It's easy to be wary of online banking; the process involves transferring large quantities of our sensitive information over the Internet, after all. With credit card fraud as common as it is, how could banking online be safe?

While it's true that online transactions can lead to credit card fraud and stolen information, most banks do their best to make transmissions secure. Online retailers with poor security and millions of customers are juicy targets for hackers, who can theoretically obtain huge lists of usernames, passwords and corresponding financial information. Thanks to the encryption online banks use, you can mostly rest easy while paying bills online. Keep reading to find out why you should be using online banking -- and what you should watch out for, just in case.

Online Banking Sites

Online banking is an appealing concept: It's accessible anywhere, anytime and using e-billing eliminates the pounds of paper bills mailed to your house every year. That last advantage can actually make online banking more secure than traditional paper banking. Bills frequently list your account number, credit card number or other financial information that would be dangerous in the wrong hands. Without paper statements, only someone with access to your online bank account can access your personal information.

Many Web sites – banks included – use a transfer protocol called Hypertext Transfer Protocol Secure, or HTTPS. While we use HTTP on a daily basis to browse the World Wide Web, HTTPS adds a form of security that encrypts data. This security is typically depicted in your Web browser by a lock or key, and any secured URL should begin with "https://" instead of "http://". Next time you log into your online banking account, pay attention to your URL bar. Is the page encrypted? If so, it will be very difficult for anyone to eavesdrop on the connection and hijack your financial data.

Popular online commerce sites like *Amazon* go to great lengths to secure their information, too, so you should see the same comforting HTTPS protocol while carrying out transactions. But that doesn't mean all online retailers are equally secure.

Online Shopping

Don't use a debit card when making online purchases because if the number is stolen, thieves will have access to your entire bank account.

Banks obviously have to closely safeguard their money; keeping those dollars secure is the only reason they exist. Retailers, though, make a profit by selling products. Whether it's the fault of shoddy security or tenacious hackers, some Web sites have a history of being hacked, resulting in fraudulent transactions for customers. Even major outlets are susceptible: In 2007, TJX, which owns discount retail giants T.J. Maxx and Marshalls, among others, was hacked to the tune of 45.7 million credit card numbers [source: Jewell]. Avoid making purchases on sites that look sketchy, and never fall for e-mail phishing schemes that try to get hold of your personal information.

There's one last precaution you should take when shopping online: Avoid using a debit card whenever possible. It's bad enough when identity thieves obtain your credit card information and make fraudulent purchases. But if they gain access to your debit card number, they could tap directly into your bank account and potentially clear it out. Whether you're using a debit card or credit card on the Internet, take advantage of your bank's online services and account management to monitor your balance. Carefully watching for fraudulent charges will help keep your finances safe, whether you're shopping or managing your money with online banking.

https://money.howstuffworks.com/personal-finance/online-banking/online-banking-safe2.htm

Contents