Content Unit

[Cybercrime]

Project: B-SAFE
Number: 2018-1CZ01-KA204-048148
Name of author: bit cz training
Last processing date: 26.6.2020

Cybercrime

First introduction

Certainly you had already received the email which requires the change of your passwords to your bank accounts or requiring some arrears or debt. Those emails generally do not look credibly, there is no clear identification of the person, institution and the language formulation is very bad. But many people want to satisfy the requirement, they often fear that they are neglecting something. What a next surprise that their bank account is sourced and the debt was invalid. The last but not least example of cybercrime is software piracy, i.e. using of illegal copy of the software not respecting the copyrights and its price. Those are the examples of the cybercrime meetings almost every person who is online.

Cybercrime is a long-established phenomenon that is inseparably tied to global connectivity. Any criminal activity that involves a computer either as an instrument, target or a means for perpetuating further crimes comes within the ambit of cybercrime. A generalized definition of cybercrime is "unlawful acts wherein the computer is either a tool or target or both" (IT Act 2000).

Cybercrime has been used to describe a wide range of offences, including offences against computer data and systems, computer-related forgery and fraud, content offences, and copyright offences. Our increasing dependence on computers and digital networks makes the technology itself a tempting target; either for the gaining of information or as a means of causing disruption and damage.

Practical relevance – This is what you will need the knowledge and skills for

After working through this content unit, you will know the definitions of the main terms related to crime in cyberspace, you can recognize dofferent types and methods of cybercrime and how to protect yourself from crime coming from virtual space. You will also be familiar with the dangerous aspects not only for adults, but also for your children.

Overview of learning objectives and competences

In LO_ Cybercrime_01 you will know the definitions of main terms related to crime in cyberspace. Also, you will know the different types and methods of cybercrime and their local and international impact.

In LO_ Cybercrime_02 you will know what is the most often cybercrimes and how to protect yourself against them. Also, you will know the contribution of the EU in the fight against cybercrime. In LO_ Cybercrime_03 you will be familiarized what is the main dangerous aspects of cybercrime for children as well as for adults.	
Learning objectives	Fine objectives
LO_ Cybercrime_01: You know the role of cybercrime on the internet.	FO_ You know the role of cybercrime on the internet_01_01: You can recognize differences between the types of cybercrime. FO_ You know the role of cybercrime on the internet_01_02: You can name the methods to attack in cyberspace. FO_ You know the role of cybercrime on the internet_01_03: You can describe what is internal and external fraud FO_ You know the role of cybercrime on the internet_01_04: You can explain what is cybertheft. FO_ You know the role of cybercrime on the internet_01_05: You can name types of impact of cybercrime. FO_ You know the role of cybercrime on the internet_01_06: You can explain the impact of cybercrime internationally. FO_ You know the role of cybercrime on the internet_01_07: You can explain what is cyberwar.
LO_ Cybercrime_02: You know the possibilities of prevention, protection and legislative measures.	FO_ You know the possibilities of prevention, protection and legislative measures_02_01: You can illustrate the methods to help protect yourself against cybercrime. FO_ You know the possibilities of prevention, protection and legislative measures_02_02: You can recognize the safe websites FO_ You know the possibilities of prevention, protection and legislative measures_02_03: You can explain what is ethical hacking. FO_ You know the possibilities of prevention, protection and legislative measures_03_04: You can understand what is EU cybercrime prevention strategies.
LO_ Cybercrime_03: You know the impact of cybercrime on your life	FO_ You know the impact of cybercrime on your life_03_01: You can name some of the ways how cybercrime can put children and adults in danger.

	FO_ You know the impact of cybercrime on your life_03_02: You can realise how cybercrime can cause loss of identity or financial losses. FO_ You know the impact of cybercrime on your life_03_03: You know the impact of cybercrime to companies and society.

1.The role of cybercrime on the internet

Cyber crime is the flip side of cybersecurity — a huge spectrum of damaging and illegal activity carried out using computers and the Internet. This unit will help you understand cyber crime and how to defend you personally, your children and your organization against it.

Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers. Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

What does cybercrime mean? Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offence (child pornography, hate crimes).

Here are some specific examples of the different types of cybercrime:

- Email and internet fraud.
- Identity fraud (where personal information is stolen and used).
- Theft of financial or card payment data.
- Theft and sale of corporate data.
- Cyberextortion (demanding money to prevent a threatened attack).
- Ransomware attacks (a type of cyberextortion).
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- Cyberespionage (where hackers access government or company data).

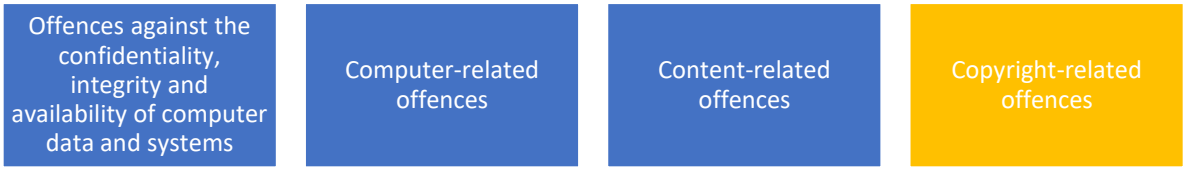
When speaking about cybercrime following the above mentioned examples, we usually speak about two major categories of offence:

1. a computer connected to a network is the target of the offence - this is the case of attacks on network confidentiality, integrity or availability.
2. an offence committed with the assistance of computers connected to a network and related information and communications technology - this is the case of the attacks such as theft, fraud, and forgery.

The following text is focused on offences committed with the assistance of computers.

The cybercrimes consist of various groups and categories. Types of cybercrime are used to describe criminal acts (such as phishing, etc.) and they are contained in the following categories.
This typology is focused on the object of legal protection: "offences against the confidentiality, integrity and availability of computer data and systems"; content-related offences; and copyright-related offences. The fourth category of "computer-related offences" does not focus on the object of legal protection, but on the method used to commit the crime. It can lead to some overlap between categories.

Categories of cybercrime



Let's now look at every single one of these categories:

Offences against the confidentiality, integrity and availability of computer data and systems

All offences in this category are directed against one of the three legal principles of confidentiality, integrity and availability.

- Illegal access (hacking, cracking)
- Illegal interception (the interception without right)
- Data interference (inputting of malicious codes, for example, viruses)
- System interference (inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data, for example, viruses that stop or slow computer systems)

Example
In 2017, the WannaCry attack, allegedly launched by North Korea, unleashed a type of ransomware which not only locks down content on user devices, but also rapidly spreads itself. WannaCry infected 300,000 computers around the world, and users were asked to pay hundreds of dollars to decrypt and restore their data.

Computer-related offences

This category covers many offences that need a computer system to be committed. Unlike previous categories, these broad offences are often not as stringent in the protection of legal principles.

- computer-related fraud
- computer-related forgery
- phishing
- identity theft

- misuse of devices

Example
In 2013-2016, Yahoo experienced a data breach which resulted in the theft of 3 billion user accounts. For some of these accounts, the attackers got hold of private information and passwords, which could be used to access user accounts in other online services. Much of this data is available today, either free or for a price, on the dark web.

Content-related offences

This category covers:

- Erotic or pornographic material
- child pornography
- xenophobic material - racism, hate speech, a glorification of violence
- insults related to religious symbols
- Illegal gambling and online games
- libel and false information
- spam and related threats

The development of legal instruments to deal with this category is far more influenced by national approaches, which can take into account fundamental cultural and legal principles. For illegal content, value systems and legal systems differ extensively between societies.

Example
A notorious paedophile (i.e., a person sexually aroused by a child), Matthew Falder, who was a UK academic with a PhD from Cambridge University, was charged in 2017 with over 137 offences committed against 46 individuals, which included intentionally encouraging rape and sexual activity with a child family member, inciting sexual exploitation of a child, and the possession and distribution of child pornography, among other offences (Dennison, 2018; Vernalls and McMenemy, 2018). He blackmailed his victims to commit humiliating, despicable, degrading and abusive acts against themselves (e.g., self-harming and licking a soiled toilet brush) and against others, and recorded these acts on images and videos (Davies, 2018; Dennison, 2018). He then shared the images and videos on hurt core sites (like Hurt 2 the Core, now defunct), which specialize in rape, murder, sadism, torture, and paedophilic content (McMenemy, 2018).

Copyright-related offences

Digitization has opened the door to new copyright violations. The most common copyright violations include the exchange of copyright-protected songs, files and software in file-sharing systems or through share hosting services and the circumvention of digital rights management (DRM) systems.This is the most often part of the cybercrime, generally tolerating by the whole society, but we should assume that this is the illeagal act with the possible consequence of incorrect behavior.

Example
The most often examples of Copyright-related offences is using the illegal copy of software on your home computer or downloading the music or films from online public stores (f.e. ShareRapid, MegaRapid)

1.Apply knowledge

Exercise TRUE/FALSE

Situation: If the music or film is published on Internet, I can legally download it.
Task: Pick the right options following the true/false principle:

a. true
b. false

Exercise SINGLE CHOICE

Task: Pick the right options following the single-choice principle: More answers could be true.
Mark the correct categories of cybercrime

a) Computer-related offences
b) Physical theft of a computer, tablet or phone
c) Content-related offences
d) Copyright-related offences

Exercise MATCH ANSWERS

Task: *Match answers – you can drug and drop the correct answers to the certain part of the text*
_____covers many offences that need a computer system to be committed. Unlike previous categories, these broad offences are often not as stringent in the protection of legal principles.
_____includes violations of legal instruments more influenced by national approaches, which can take into account fundamental cultural and legal principles. Value systems and legal systems differ extensively between societies.
_____ include the exchange of copyright-protected songs, files and software in file-sharing systems or through share hosting services and the circumvention of digital rights management (DRM) systems
Computer-related offences, Content-related offences, Copyright-related offences

2. The methods and examples of cybercrime

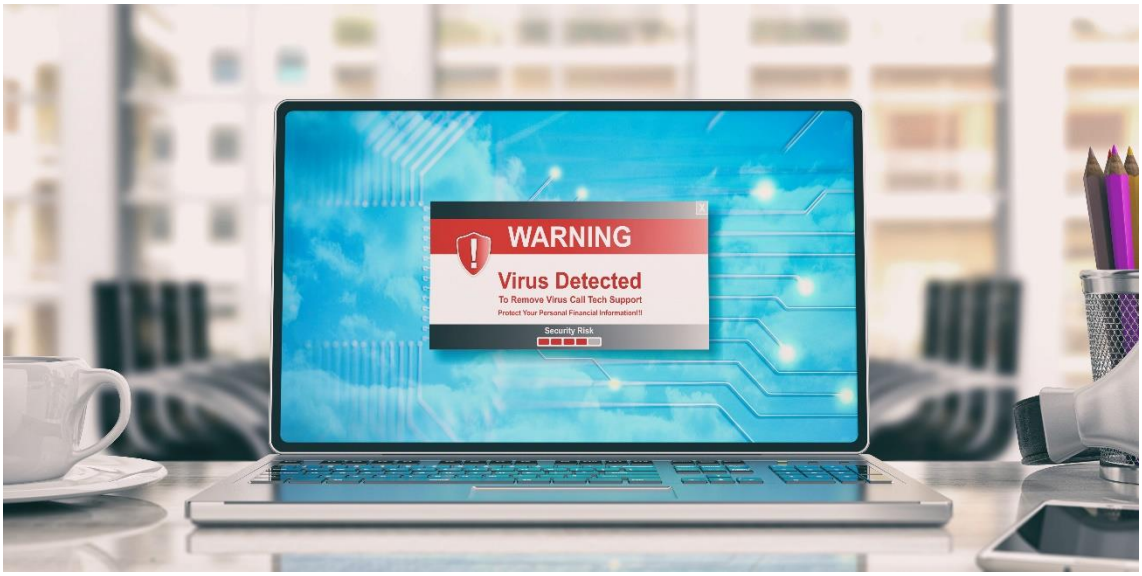
These were four categories that are distinguished when it comes to cybercrime. Now we want to have a closer look at **the roles of computers in cybercrime and the methods how to attack in cyberspace**:

Computers play four roles in crimes - they serve as **objects, subjects, tools, and symbols**. Computers are objects of crime when they are sabotaged or stolen. Computers play the role of subjects when they are the environment in which technologies commit crimes. Computer virus attacks fall into this category. When automated crimes take place, computers will be the subjects of attacks. The third role of computers in crime is as tools, enabling criminals to produce false information or plan and control crimes. Finally, computers are also used as symbols to deceive victims.
The most common is cybercrime serving as a subject. The main methods of using a computer, as a criminal subject, are:

- malware
- hacking
- spam

- phishing
- Distributed DoS attacks (DDoS)

The main methods to attack



Definition
Malware is a general label for malicious software that spreads between computers and interferes with computer operations. Malware may be destructive, for example, deleting files or causing system crashes, but may also be used to steal personal data.

There are many **forms of malware**. Some of them are the following:

- **Viruses** can cause mild computer dysfunction, but can also have more severe effects in terms of damaging or deleting hardware, software or files.
- **Worms** are self-replicating programs, but they can spread autonomously, within and between computers, without requiring a host or any human action. The impact of worms can, therefore, be more severe than viruses, destroying whole networks.
- **Trojans** are a form of malware that appear to be legitimate programs but facilitate illegal access to a computer. They can perform functions, such as stealing data, without the user's knowledge and may trick users by undertaking a routine task while undertaking hidden, unauthorised actions.
- **Spyware** is software that invades users' privacy by gathering sensitive or personal information from infected systems and monitoring the websites visited.

Definition
Hacking is a common process which results in the breaching of one's privacy and confidential information. The weaknesses of a system or loopholes in a network are identified and private details are accessed. Therefore, hacking is also known as an unauthorized intrusion.

However, hacking is not always perceived as theft and used for productive causes. Such type of hacking that involves good intentions is known as ethical hacking. This type of hacking is done to secure the operating system.

Hackers can be classified into different categories such as a white hat, black hat, and grey hat, based on their intent of hacking a system.

White Hat Hackers - Ethical Hackers
They never intended to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments. Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. Numerous companies hire ethical hackers for penetration testing and vulnerability assessments.

Grey Hat Hackers
They are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge. They intend to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

Black Hat Hackers – crackers
They hack to gain unauthorized access to a system and harm its operations or steal sensitive information. Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the operating system, blocking network communication, etc.

Definition
Spam is unsolicited or junk email typically sent in bulk to countless recipients around the world and is often related to pharmaceutical products or pornography. Spam email is also used to send phishing emails or malware and can help to maximise potential returns for criminals).

Crime moves away from traditional methods such as violence, drugs or burglary and internet-based crime is becoming more prevalent. This goes with the trend resulting from increased online business and communication. The victims of crime may lose anything that has value - safety, peace, money or property.

Excursus
The first study to examine the emotional impact of cybercrime, it shows that victims' strongest reactions are feeling angry (58 %), annoyed (51 %) and cheated (40 %), and in many cases, they blame themselves for being attacked. Only 3 % don't think it will happen to them, and nearly 80 % do not expect cybercriminals to be brought to justice— resulting in an ironic reluctance to take action and a sense of helplessness.

Definition

Phishing - A phishing campaign is when spam emails, or other forms of communication, are sent en masse, with the intention of tricking recipients into doing something that undermines their security or the security of the organization they work for. Phishing campaign messages may contain infected attachments or links to malicious sites. Or they may ask the receiver to respond with confidential information

Example
A famous example of a phishing scam from 2018 was one which took place over the World Cup. According to reports by Inc, the World Cup phishing scam involved emails that were sent to football fans. These spam emails tried to entice fans with fake free trips to Moscow, where the World Cup was being hosted. People who opened and clicked on the links contained in these emails had their personal data stolen.

Definition
Distributed DoS attacks (DDoS) are a type of cybercrime attack that cybercriminals use to bring down a system or network. Sometimes connected IoT (internet of things) devices are used to launch DDoS attacks. A DDoS attack overwhelms a system by using one of the standard communication protocols it uses to spam the system with connection requests.

Example
A famous example of this type of attack is the 2017 DDoS attack on the UK National Lottery website. This brought the lottery's website and mobile app offline, preventing UK citizens from playing.

The most frequently committed cybercrimes include:

Online impersonation

This crime is one of the most commonly committed cybercrimes in existence. For this criminal act it is typical to use another person's name, domain address, phone number or any other identifying information without consent and to cause harm or commit fraud, which is a crime.

Example
Claire began being harassed by strangers after someone made a post on the Internet offering sexual services in her name. The post included private information, including her phone number and home address.

Cyberstalking

Physical stalking can take forms of following in person, secretly watching, persistent calling and texting to manipulate, and different other means to approach the victim unexpectedly. The difference of cyberstalking is that it is committed on online technology such as email, social networks, instant messaging, personal data available online – everything on the Internet can be used by cyberstalkers to make inappropriate contact with their victims.

Example
After John and his girlfriend broke up, he began stalking her by planting a prepaid GPS-enabled cell phone under her car. John tracked his ex-girlfriend's movements, and followed her by logging into the cell phone account online. John also called his ex upwards of 200 times a day.

Cyberbullying

We can name this crime when people use social media or the internet to intimidate, harass, threaten or belittle others. In general, if a person uses the internet or any other form of electronic communication to threaten, harass or scare another person, this conduct may be a crime.

Examples
While traveling on the road with a junior team, one of the players takes an embarrassing photo of a girl that he met at the rink. He then posts the photo on Facebook and sends the photo to all of the other players on the team. The photo then gets distributed. Three of Paul's teammates send texts to him, blaming him for the team's loss and telling him that he does not know how to play the game. Paul is afraid to tell his coach and parents so tolerates the bullying for the entire hockey season. He does not return to hockey the next season.

What is the difference between cyberbullying and cyberstalking?

Cyberbullying	Cyberstalking
Cyberbullying is constant contact with the person; saying hurtful things to the person or telling others untrue information about the person. For instance, the offender creates the Facebook group entitled "I hate…" and invites all friends to join it.	Cyberstalking is an obsession with finding out as much you can about the person (without actually asking them). For instance, the offender finds out where the person was born, if the person is married, etc.

Identity theft and data theft

Identity theft is the act of stealing personal identification information to commit illegal acts, such as: opening a line of credit, renting a house, purchasing goods or services, auction- and wage-related fraud or extortion.
Data theft is the act of illegal possession of sensitive data, which includes unencrypted credit card information stored in businesses, trade secrets, intellectual property, source code, customers' information and employee records.

Example
The Marriott was hacked in 2018, where 383 million guest records and over 5 million passport numbers were stolen, data breaches have increased in frequency and severity. Those date could be sold on the dark market and anyone can abuse them and use the another identity.

Financial crimes

This variety includes activities that dishonestly generate wealth for those engaged in the conduct in question. It consists of exploitation of insider information or the acquisition of another person's property by deceit to secure a material benefit. Financial crime is commonly considered as covering the following: fraud, money laundering, bribery, bribery and corruption and many others.

Example
Some recent high-profile financial crimes include the Enron scandal, where the energy company committed widespread fraud and corruption, and the Bernie Madoff investment scandal, where Madoff pretended to have a successful investment firm, but he was really just stealing money from new clients and giving it to older clients (This is what is called a Ponzi scheme, and Madoff ran the largest one in history). Madoff was convicted of numerous crimes including money laundering and many different types of fraud..

Cybercrime is often committed by someone near you – for example in your company. This type of cybercrime is called internal fraud and refers to a type of fraud that is committed by an individual against an organization. In this type of fraud, a perpetrator of fraud engages in activities that are designed to defraud, misappropriate property, or circumvent the regulations, law, or policies of a company. For instance, internal fraud involves activities such as nonreporting of transactions intentionally, performing unauthorized transactions, and intentional mismarking of positions.
Internal fraud can be classified into two broad categories, embezzling and identity theft. In the case of embezzling, the cash is taken directly from the organizations and in the case of identity theft, a customer's personal information is misappropriated by the employee to make a profit. Examples of internal fraud include:

- The theft of a customer's money.
- Credit Abuse of a customer
- Money Laundering
- Procurement Fraud
- Data Theft

On the other hand, the fraudulent activities of persons external to the company are called external fraud. It involves the theft of money or stock by persons outside the business. Examples of external fraud include:

- Identity theft - taking control of a virtual identity of the person
- Falsifying invoice details (altering the payee's account number)
- Falsifying order details, so that goods are delivered to the wrong destination
- Impersonating a person's voice or forging their signature
- Falsification of emails

There are various **purposes of cyber-attacks** in cyberspace ranging from the moderate to the merciless ones, the 4 most typical purposes are:

- vandalism (common attacks on government web sites)
- propaganda (dissemination of political news mainly through the internet)
- access denial (attacks against e.g. armed forces which use computers and satellites for communication)
- network attacks against infrastructure (attacks on transmission systems of the companies in power engineering, gas industry, heating industry, oil industry and communication infrastructure, which are sensitive to cyber-attacks, etc.)

2.Apply knowledge

Exercise SINGLE CHOICE

Situation: What is Distributed DoS attacks **(DDoS)?**
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

a) when spam emails, or other forms of communication, are sent in masse
b) **a type of cybercrime attack that cybercriminals use to bring down a system or network**
c) unsolicited or junk email typically sent in bulk to countless recipients around the world
d) unauthorised use of, or access into, computers or network resources, which exploits identified security vulnerabilities in networks

Exercise SINGLE CHOICE

Task: Pick the right options following the single-choice principle: Only one answer is true.

e) What activities does the person call „grey hat hacker "?
f) a. It is the person that spread untrue information about someone else.
g) b. It is the person who tries to steal personal identification information.
h) **c. It is the person who gains access to a system of someone without permission, just for fun.**
i) d. It is the person who is responsible for many financial crimes through the internet.

Exercise SINGLE CHOICE

Situation: What does internal fraud mean?
Task: Pick the right options following the multiple-choice principle: Only one answer is true.

a. Internal fraud is committed by suppliers in case they do not supply the negotiated service or goods at time.
b. Internal fraud involves activities such as grooming or cyberbullying.
c. **Internal fraud is committed by employs in case of performing unauthorized financial transactions.**
d. Internal fraud is committed by customers of the company by submitting of an unjustified complaint.

3.Impact of the cybercrime

Computers can be also used to attack to commit real-world crimes (IPR violations, credit card frauds, EFT frauds, pornography, etc.) and even terrorism. Terrorists often use information technology to plan and execute their criminal activities. This then is referred to by the term cyberterrorism. The increase in international interaction and the widespread usage of IT has facilitated the growth of crime and terrorism. Because of the advanced communication technology people need not be in one country to organize such a crime. Hence terrorists and criminals can find security loopholes in the system and can function from unusual locales instead of their country of residence.

The majority of future international incidents, whether military or spy, will have a cyber dimension. Therefore, it is very timely to consider the evaluation of these attacks. At present, there are debates about the possibility of escalating incidents into an unsustainable war conflict, where death, destruction, personal injury or property damage may occur. The problem is that attributing actions to a particular state is almost impossible. It is difficult to recognize a particular attacker without precise cooperation of the state in whose territory the attacker is located.

The impact of cybercrime

The impacts of cybercrime can be devastating due to the high risk of data loss and financial impact.

For individuals

Data breaches, identity theft, problems with devices: cybercrime can have a big impact on individuals. You might find yourself dealing with suspicious charges on your credit card as a result of identity theft, a ransomware attack demanding hundreds or thousands in blackmail to release your files, or expensive fees in data or electricity from cryptojacking or botnets. The costs can be worse than monetary when cyberbullying, including sexual harassment, is plaguing you.

For businesses & governments

Businesses as well as healthcare organizations and governments can also suffer from sensitive data loss, huge financial burdens, and brand damage. The average ransomware attack against small and medium businesses in 2019 demanded $5,900 to unblock their files or systems. Far worse, the downtime during these attacks cost the affected businesses $141,000 on average. That's to say nothing of ransomware attacks on governments, such as the one that caused Jackson County, Georgia to pay $400,000 to restore their IT systems and infrastructure.

Another term used in this context is cyberwar. Let's look at these two terms in detail:

What is cyberterrorism?	What is cyberwar?
The concept of cybercrime is often confused with cyberterrorism. Cyberterrorism is always more severe than other behaviors that are carried out in or through cyberspace. NATO defines cyberterrorism as "cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal".	Cyberwar involves the use and targeting of computers and networks in war. It involves offensive and defensive operations about the threat of cyberattacks, espionage and sabotage. Cyberwar has been defined as "actions by a nation-state to penetrate another nation's computers or networks to cause damage or disruption".

Example
Cyberware, including network attack, has gained some additional importance since the 11th of September. This situation after the 11th of September attacks brought an intensive discussion about the use of information and communication technologies by terrorists. This discussion was facilitated by reports that the offenders used the Internet in their preparation of the attack. Although the attacks were not cyber-attacks, the Internet played a role in the preparation of the offence. In this context, different ways in which terrorist organizations use the Internet were discovered.

3.Apply knowledge

Exercise SINGLE CHOICE

Associated fine objective: FO_ You know the role of cybercrime on the internet_01_05: You can explain what is cyberwar.

Situation: What is the worst cyber-attack to commit real-world crimes?
Task: Pick the right options following the single-choice principle: Only one answer is true.

c. credit card frauds
d. pornography
e. cyberterrorism
f. identity theft

Exercise MULTI

CHOICE

Task: Pick the right options following the single-choice principle: More answers could be true.
What impact can have the cybercrime for individuals?

a) **identity theft**
b) losing of the job
c) healthy problems
d) **Data breaches**

Exercise FILL IN THE BLANK

Task: fill in the correct answer to the blank in the certain shape without any possibilities
_____ can also suffer from sensitive data loss, huge financial burdens, and brand damage.
companies, businesses, business, organizations, governments, institutes

4.Possibilities of prevention and protection

Everything from stolen money, theft of personal and financial data, loss of productivity and the damage and destruction of critical corporate or individual data is categorized as cybercrime. Unfortunately, the hackers and those that commit cybercrimes are becoming more and more sophisticated
What are the best ways to protect your computer and your personal data?
The best way how to protect yourself against cybercrime is prevention. For online security, five key points are good to keep in the mind: **Precaution, Prevention, Protection, Preservation and Perseverance.**

These points are included in the following steps:

1. Avoid disclosing personal information on Internet and emails
2. Carefully consider sending any photograph online, - anyone can use it anytime in the another context

3. Use strong passwords
4. Use and update antivirus software
5. Avoid sending credit card number and its passwords by email
6. Keep a watch on the sites that your children are accessing
7. Keep back up of your data to prevent loss of information due to virus attack
8. Use a security program that gives control over the cookies
9. Keep software and operating system updated
10. Never open attachments in spam emails
11. Do not click on links in spam emails or untrusted websites
12. Contact companies directly about suspicious request
13. Keep an eye on your bank statements
14. Be mindful of which websites you visit

How can I recognize the safe websites?

The 3 website safety tips below will clear away the uncertainty and teach you how to identify if a site is trustworthy or not. First, you'll learn a couple of simple visual checks that give you useful info at a glance. Then, we'll explain the website safety tools you should have in place to inform and guide you. Finally, we'll tell you how to research a little deeper should any questions still remain. Now let's get savvy and put the fun back into web surfing.

1 - Website safety visual checks

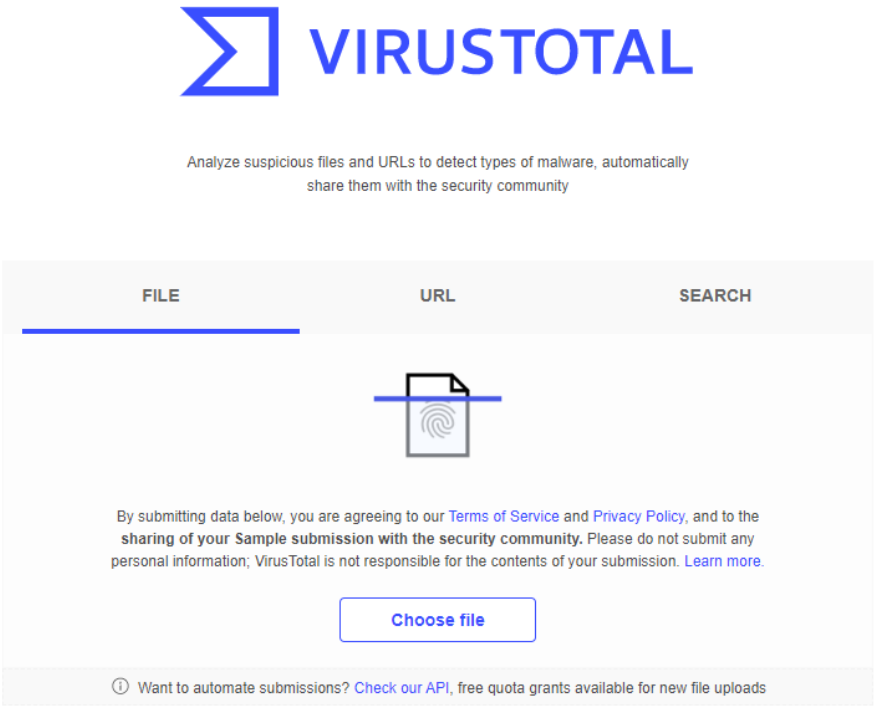
- Double-check those URLs — Let's start with the easiest tip. It's really no more difficult than making sure the URL looks legit. Before you click any link, hover your cursor over it and look at the bottom left corner of your screen where the URL is displayed. The first trick of phishing is to look as authentic as possible. At first sight, the URL might look like the real McCoy, but closer inspection may reveal a 1 instead of an l, or .net instead of .com. Train yourself to sanity check each and every URL before you click or before you enter any personal information like a username and password.
- Check for https — Those letters you see at the start of every URL stand for Hypertext Transfer Protocol (http). It's the foundation for how data is communicated on the web. And while it's eminently useful, it's also easily hackable. The addition of an "S" as in "https" (and the lock icon), however, tells you that the site is secure. Websites with a padlock icon in the address bar and an https prefix are encrypted and have a trusted SSL certificate, basically guaranteeing a secure connection between website and browser. If you cannot verify that a website or link is safe with https, be on your guard and do not enter any personal information.

And, do note: cybercriminals do everything in their power to present themselves as legit, so while https: websites are more secure, you could be on to one that is run by a crook. So, if you are still suspicious about an https: site, use the other safety tools below to check if a website is safe.

2 - Website safety tools

- Use your built-in browser tools — The first tools you should familiarize yourself with are the security measures already in your browser. Look at your privacy and security settings. Chances are, you'll find the default settings are more lax than you like. Manually adjust the rules and settings in the way that makes you comfortable. Block popups, prevent automatic downloads, don't allow tracking. Your options will vary depending on your browser of choice.

- Run an online website safety check — There are several from which you can choose, but we recommend VirusTotal for its unbiased position. These online tools use antivirus scanners and other security solutions to check a website for any threats. Simply enter the URL you want scanned into the search bar on the site, and get instant results. Enter a URL, and VirusTotal will tell you if the site is suspicious.



- Install web security tools — For total website safety confidence, protect yourself with top-of-the-line cybersecurity suites, (f.e. Avast Free Antivirus, McAfee, AVG, Windows Defender). You can also add the benefit of privacy to website safety if you go with a virtual private network.

3 - Website safety quick research

- Check contact details for the website — If you've done all of the above and you're still not quite sure, then march on up to the front door and knock. That is to say, find the "Contact Us" info on the site and give them a call. Depending on how (and if) they answer will clue you as to whether or not it's a legitimate operation.
- Check if your antivirus has an Anti-Phishing Certificate — Not all do. Look for 3rd-party labs who test for anti-phishing, such as AV-Comparatives. They test antivirus products against phishing URLs (which attempt to get your personal information) and they check for false

positives when it comes to legitimate banking websites, to make sure the security product knows the difference.

- Check to see if the URL has a privacy policy — this is a no-brainer. If a website doesn't have a privacy policy, that is a red flag as to whether the company is legit or not.
- Look up the domain owner of the website using WHOIS — You can also research who owns a particular domain by checking the public records available through a WHOIS search. Learn everything about the domain, including who registered it and when.

A Business Response to Cyber Crime

As a business, your best bet against cyber crime is to prepare a solid incident response plan. Often planning is not enough — you should have the security staff and tools in place to execute it. An incident response plan, according to the SANS framework, includes:

- Preparation—codifying your security policy, identify types of critical security incidents, prepare a communication plan and document roles, responsibilities and processes for each one. Recruit members to your computer security incident response team (CSIRT) and train them.
- Identification—use security tools to accurately detect anomalous behavior in network traffic, endpoints, applications or user accounts, and rapidly collect evidence to decide what to do about the incident.
- Containment—isola
- te the affected systems, clean them and gradually bring them back online.
- Eradication—identify the root cause of the incident, and do everything to ensure the issue does not repeat itself. Fix broken security measures that let in the attackers, patch vulnerabilities, and ensure you clean malware from all endpoints.
- Recovery—bring production systems back up, taking care to prevent another similar attack. Test to ensure that systems are back up and working as usual.
- Lessons Learned—up to two weeks after the incident, review it with the team to understand what went well and what didn't, and improve your incident response plan.

The EU tries to combat cybercrime by a wide range of means. In 2005, the Council adopted the EU counter-terrorism strategy to fight terrorism and make Europe safer. The strategy includes four pillars: prevent, protect, pursue, respond.

To fight and pursue cybercrime on different levels, EU has implementedthe following legislative actions:

- 2001 – **Framework Decision on combating fraud and counterfeiting,** which defines the fraudulent behaviours that the EU States need to consider as punishable criminal offences.
- 2002 – **ePrivacy Directive**, which defines regulations of electronic communications within the EU, to increase privacy for individuals and entities.
- 2011 – **A Directive on combating the sexual exploitation of children online and child pornography**, which addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for sexual abuse)
- 2013 – **A Directive on attacks against information systems**, which aims to tackle large-scale cyber-attacks to strengthen national cyber-crime laws and introduce tougher criminal sanctions

Internationally active organizations seek to contribute to the fight against cybercrime. There are two major organizations operating in the EU:

European Cybercrime Centre - EC3 assists member states in their efforts to dismantle and disrupt cybercrime networks and developing tools and providing training.

The European Union Agency for Cybersecurity (ENISA) works to deliver advice and solutions and improving cybersecurity capabilities. A centre of expertise for member states and EU Institutions seek advice on matters related to network and information security.

4.Apply knowledge

Exercise SINGLE CHOICE

Task: Pick the right options following the single-choice principle: Only one answer is true.

What is Anti-Phishing Certificate?

a) **check for false positives when it comes to legitimate banking websites, to make sure the security product knows the difference**
b) check if a website doesn't have a privacy policy
c) verify that a website or link is safe with https
d) verify the real owner of the website

Exercise TRUE/FALSE

Task: Pick the right options following the true/false principle: Only one answer is true.

The addition of an "S" as in "https" (and the lock icon) is more safety website.

a) **True**
b) False

Exercise SINGLE CHOICE

Task: Pick the right options following the single-choice principle: One answer is true.
What is VirusTotal?

a) Antivirus program with installation to your computer
b) Web browser
c) **Tool for online check of web safety**
d) Hypertext Transfer Protocol

5. The impact of cybercrime on life

The Internet can be a **dangerous environment for children and also for adults.** Especially, in this digital period where social media such as Facebook, Instagram or the Internet in general play an inseparable role. Protecting especially children on the Internet requires high awareness about the risks and advanced IT skills — as a parent you have to know what dangers lurk and how to safeguard against them.

Here are the six greatest risks that kids face online:

- Cyberbullying
- Accidentally Downloading Malware
- Grooming
- Phishing
- Posting Private Information
- Chat room "friends"

However, not only children are confronted with virtual threats. The cybercrime landscape is enormous, and there are varieties of ways in which cybercrimes can catch up directly with you. Cybercriminals attack human ignorance, nescience and comfort, which can cause a loss of identity and finances. What should people be aware about? Criminals consciously design their traps by taking advantage of human weaknesses or human behavior, such as:

- individual's willingness to trust others
- suggested urgency or importance of a message
- signs of legitimacy or authority in a message or individual (branding identical to the official branding of an individual or organization to cultivate trust)

- fear of situations that are high stress or where individuals can be highly anxious
- convenience (the easier decision may not be the most secure)
- individuals' tendency to overshare personal identity details online (especially on forms of social media, including Facebook, Twitter, LinkedIn)
- unfamiliarity with new forms of technology which open individuals to risk
- individual's underestimation of the situation

If a person remains in the behaviour shown above, he or she will face a higher risk to become a victim of cybertheft. Cybertheft is a type of crime when financial or personal information is stolen through the use of computers. Cyber thieves are sophisticated and can breach security measures data.
In the first phase, the offender must first acquire a foreign computer identity. This is most often done by stealing electronic data (passwords, access data, etc.), usually by unauthorized copying (skimming), deceitful phishing or hacking. This is called identity theft. In the second phase, the perpetrator misuses the identity. The aim is generally property benefit. In some cases, the aim may be simply to harm the victim, for example by acting under his name in social networks such as Facebook.

The defence is not complicated - it is important to follow a few simple rules:

1. monitor the account
2. buy on secure websites - if there is a green padlock icon before the "https," you know off the bat you're on a secure website
3. be careful about opening untrustful emails

Cyber theft is when your financial or personal information is stolen through the use of computers. Cyber thieves can target banks, corporations and individuals.
In the first phase, the offender must first acquire a foreign computer identity. This is most often done by stealing electronic data (passwords, access data, etc.), usually by unauthorized copying (skimming), deceitful phishing or hacking. This is called identity theft.

In the second phase, the perpetrator misuses the identity. The aim is generally property benefit. In some cases, the aim may be simply to harm the victim, for example by acting under his name in social networks such as Facebook.

Impact on individuals, companies and society

Cybercrime has a direct and significant **impact on jobs, innovation, economic growth, and investment**. Additionally, IP theft makes up at least 25% of cybercrime costs, and has an especially high threat to military technology. Two areas of cybercrime that are difficult to measure are IP (IP address) theft and loss of opportunity.

Individuals and businesses can suffer **significant financial loss** because of cyber crime with the most obvious impact being theft. Loss of business can also be significant in the instance of a denial of service attacks for large corporations

It may make life easier, but it also leaves us vulnerable to risk. Because of this, cyber security is top priority and affects our daily/working lives greatly. Breaches in cyber security can be catastrophic for organisations and their employees or client base.

Damages from cyberattacks and cyber theft may spill over from the initial target to economically linked firms, thereby magnifying the damage to the economy. Firms share common cyber vulnerabilities, causing cyber threats to be correlated across firms.

Crime affects everyone and in future cybercrime (and cyber security) is going to affect people more and more. No one is safe – it impacts the rich and the poor:

- Anyone with a mobile phone in their pocket.
- Anyone who has a bank account.
- Anyone who stores important files on their computer.
- Anyone whose name is in a direct marketing database.

Cyber crime is not some futuristic possibility. It is being committed every day right now. Thieves commit cyber crimes to steal people's money and their identity. With your identity, the thief can take out loans, incur credit, accumulate debt and, then flee without a trace. It can take years to rehabilitate your identity. A virus can destroy someone's files and a lost database can result in receiving unwanted sales calls.

Cyber security is important for national security – securing this beautiful country of ours.

- There are some state secrets that must remain secret.
- The personal safety of our leaders is very important.
- The fingerprint database and Home Affairs database must be secure.
- Terrorists must not be able to halt trading on the important national and world database with sensitive data.

But national security cannot override our personal freedom we fought so hard to achieve:

- Our freedom of speech is crucial.
- A free press holds people to account.
- Personal privacy ensures democracy.
- Freedom to do things online without surveillance.

5.Apply knowledge

Exercise SINGLE CHOICE

Task: Pick the right options following the single-choice principle: Only one answer is true.

Who can be affected by cybercrime?

a. anybody dealing with mobile, online accounts or bank accounts.
b. only children.
c. only companies
d. only public institutions.

Exercise SINGLE CHOICE

Task: Pick the right options following the single-choice principle: Only one answer is true.

What is cyber theft?

a. obsession with finding out as much you can about the person
b. using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goa.
c. saying hurtful things to the person or telling others untrue information about the person
d. when your financial or personal information is stolen through the use of computers

Exercise TRUE/FALSE

Task: Pick the right options following the true/false principle: Only one answer is true.

Cyber security is not important for national security.

a) True
b) False

Sources

Source: http://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf
Source: https://study.com/academy/lesson/finance-crime-definition-comparisons-examples.html
Source: https://www.avast.com/c-cybercrime
Source: NATO science for peace and security series, 2008
Source: CLARKE, Richard A. Cyber War, HarperCollins (2010) ISBN 9780061962233
Source: CNN, News, 04.08.2004, available at: www.cnn.com/2004/US/08/03/terror.threat/index.html. For an overview, see: Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; Gercke, Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007
Source: EU counter-terrorism strategy
Source: https://www.avast.com/c-website-safety-check-guide
Source: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
Source: https://www.enisa.europa.eu/
Source: https://arxiv.org/pdf/1811.06624.pdf

1.Save knowledge

Summary

Using computer technology, information systems and information technology and their integration into almost all sectors of human activity is a phenomenon of nowadays. There is almost no area of human activity, where information or communication technology is not used.

Unfortunately, as technological progress is on the rise, there is a bigger possibility of crime. Crime can be committed in many ways, the most commonly committed cybercrimes include:

- Malware - general label for malicious software that spreads between computers and interferes with computer operations
- Hacking - common process which results in the breaching of one's privacy and confidential information
- Spam - unsolicited or junk email typically sent in bulk to countless recipients around the world
- Phishing - spam emails, or other forms of communication, are sent en masse, with the intention of tricking recipients into doing something that undermines their security or the security of the organization they work for
- Distributed DoS attacks (DDoS) - attack overwhelms a system by using one of the standard communication protocols it uses to spam the system with connection requests

However, hacking is not always perceived as theft and used for productive causes. Such type of hacking that involves good intentions is known as ethical hacking. This type of hacking is done to secure the operating system.
The most frequently committed cybercrimes include:

- Online impersonation - use another person's name, domain address, phone number or any other identifying information without consent
- Cyberstalking - obsession with finding out as much you can about the person
- Cyberbullying - saying hurtful things to the person or telling others untrue information about the person
- Identity theft - stealing personal identification information to commit illegal acts
- Data theft - illegal possession of sensitive data, which includes unencrypted credit card information stored in businesses
- Financial crimes - covering the following: fraud, money laundering, bribery, bribery and corruption and many others

The impacts of cybercrime can be devastating due to the damage to reputation, high risk of data loss and financial impact for:

- Children
- Adults
- Companies
- States/governments

The cybercrime can have not only financial, but also dishonest impact on individuals or companies. Businesses as well as healthcare organizations and governments can also suffer from sensitive data loss, huge financial burdens, and brand damage.
The huge planned actions of cybercrime should be named as cyberterrorism or even cyberwar. Cyberterrorism is always more severe than other behaviors that are carried out in or through

cyberspace. Cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal.
Cyberwar involves the use and targeting of computers and networks in war. It involves offensive and defensive operations about the threat of cyberattacks, espionage and sabotage.

An important tool in the fight against cybercrimes is prevention and enlightenment. Finally, computer literacy is important as an essential element in preventing the use of information and communication technologies. We should prepare not only children, but also adults and companies for the dangers of cyberspace and try to provide them with the required knowledge to safely use information technologies.

For online security, five key points are good to keep in the mind: **Precaution, Prevention, Protection, Preservation and Perseverance**.

These points are included in the following steps:

1. Avoid disclosing personal information on Internet and emails
2. Carefully consider sending any photograph online, - anyone can use it anytime in the another context
3. Use strong passwords
4. Use and update antivirus software
5. Avoid sending credit card number and its passwords by email
6. Keep a watch on the sites that your children are accessing and use the parental control tools
7. Keep back up of your data to prevent loss of information due to virus attack
8. Use a security program that gives control over the cookies
9. Keep software and operating system updated
10. Never open attachments in spam emails
11. Do not click on links in spam emails or untrusted websites
12. Contact companies directly about suspicious request
13. Keep an eye on your bank statements
14. Be mindful of which websites you visit

How can I recognize the safe websites?

1 - Website safety visual checks
2 - Website safety tools
3 - Website safety quick research

The internet is teeming with phishing scams. No brand is safe from being falsified, and no user is safe from being targeted. More than ever before, we need to take responsibility for our own online safety. Follow the tips above and stay smart. You have received all the info you need, but your greatest defender is you.