DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Let's get started!

Be safe online and secure your PC

Project number: 2017-1-PL01-KA2014-038433

Co-funded by the Erasmus+ Programme of the European Union

Ask yourself:

1. Have you ever heard about cybersecurity?
2. Do you secure your pc? How?
3. Has your computer ever been infected by a virus?

Let's start!

What is cyber security and why it matters

Cybersecurity is becoming increasingly relevant in today's world, with more than 230,000 new malware samples launched every day. Security threats are not just faced by large corporations conducting operations online. Anyone who browses the net is a potential victim of cyber-criminals.

The biggest cybersecurity threats to people include:

- links to malicious websites,
- malware,
- drive-by downloads and
- viruses.

Let's start!

A Few Hints

- The Internet is not a safe place because any computer can be an easy target for cybercriminals.
- Unsafe websites that do not have a security certificate should be avoided. Look for HTTPS at the start of the URL.
- An email from an unknown source should not be opened.
- An anti-virus software needs to be installed to help prevent threats.

Let's start!

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security comprises cybersecurity and physical security -both are used by enterprises to protect against unauthorised access to data centers and other computerised systems. Information security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cybersecurity.

Let's start!

Have you ever had a virus?

PC viruses are like a flu, designed to spread from host to host and has the ability to replicate itself. Similarly, in the same way that flu viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming such as a file or document. In a constantly connected world, viruses can be spread through:

- email and text message attachments,
- Internet file downloads,
- and social media scam links.

Your mobile devices and smartphones can become infected with mobile viruses through unsecure app downloads. Viruses can hide, disguised as attachments of socially shareable content such as funny images, greeting cards, or audio and video files.

Let's start!

SPAM!

- Nobody wants it or ever asks for it.
- No one ever find it useful.
- Sometimes it is actually interesting, like 1% of junk mail that is really useful to some people.

Spam is electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email.

Watch this video:
https://www.youtube.com/watch?v=_QdPW8JrYzQ

Let’s start!

Why SPAM emails exist!

Spam is an email sent to thousands, and sometimes millions, of people without prior approval, promoting a particular product, service, or a scam to get other people's money.

- *replying to that email indicates that your e-mail address is valid and your e-mail address may be sent to other spam lists.*
- *Never do that when receiving any e-mail that is spam; it is usually best to delete the email.*
- *Be careful where you post your e-mail address. Never post in chat rooms, news groups, or other public places.*
- *When filling out any form on the Internet, watch carefully for any check box that by default may be checked for you to receive a newsletter or share your e-mail with a third-party.*

Let's start!

Hacking

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose.

Who is he?

An hacker is not always someone doing illegal things!
White hat professionals hack to check their own security systems to make it more hack-proof. **Black hat** hackers hack to take control over the system for personal gains. They can destroy, steal or even prevent authorized users from accessing the system. **Grey hat** hackers comprise curious people who have just about enough computer language skills to enable them to hack a system to locate potential loopholes in the network security system.

Let's start!

The art of manipulating people: Social Engineering

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Watch this video:
https://www.youtube.com/watch?v=lc7scxvKQOo

Let's start!

What Does a Social Engineering Attack Look Like?

Email from a friend

- If a criminal manages to hack or socially engineer one person's email password, they have access to that person's contact list. Once the criminal has that email account under their control, they send emails to all the person's contacts or leave messages on all their friend's social pages, and possibly on the pages of the person's friend's friends.

Taking advantage of your trust and curiosity

- Contain a link that you just have to check out–and because the link comes from a friend and you're curious, you'll trust the link and click–and be infected with malware so the criminal can take over your machine and collect your contacts info and deceive them just like you were deceived

Let's start!

What Does a Social Engineering Attack Look Like?

Email from another trusted source

- Phishing attacks are a subset of social engineering strategy that imitate a trusted source and concoct a seemingly logical scenario for handing over login credentials or other sensitive personal data. According to Webroot data, financial institutions represent the vast majority of impersonated companies and, according to Verizon's annual Data Breach Investigations Report, social engineering attacks including phishing and pretexting (see below) are responsible for 93% of successful data breaches.

Using a compelling story or pretext

- Urgently ask for your help. Your 'friend' is stuck in country X, has been robbed, beaten, and is in the hospital. They need you to send money so they can get home and they tell you how to send the money to the criminal.
- Present a problem that requires you to "verify" your information by clicking on the displayed link and providing information in their form. The link location may look very legitimate with all the right logos, and content (in fact, the criminals may have copied the exact format and content of the legitimate site).

Thank you for your attention!

DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Project number: 2017-1-PL01-KA2014-038433

Co-funded by the
Erasmus+ Programme
of the European Union

DIGIT

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Dive in!

Be safe online and secure your PC

Project number: 2017-1-PL01-KA2014-038433

Co-funded by the Erasmus+ Programme of the European Union

Dive in!

How to prevent risks: start simple

The Internet is not a safe place because any computer can be an easy target for cybercriminals.

- Unsafe websites that do not have a security certificate should be avoided. Look for HTTPS at the start of the URL.
- An email from an unknown source should not be opened.
- An anti-virus software needs to be installed to help prevent threats.

Dive in!

Create strong passwords

- A good, strong password should be long and complex, with lower-case letters, capital letters, symbols, and numbers.

Use security software

- Your device – computer, laptop, tablet, or smartphone – should be equipped with a reliable anti-virus software. Update it regularly.

Adjust browser security settings

- Most popular browsers such as Google Chrome, Firefox, and Opera have special settings that allow you to block potentially harmful resources, such as pop-up windows.

Dive in!

Remember to log out

- When you're done using a website or an app, make sure you logged out of them because leaving them open make your data more vulnerable.

Think twice before clicking on links in emails

- Chances are you'll receive messages from cyber-criminals that design them to be very convincing.

Be careful what you download

- There are so many resources available out there so sometimes we don't give a second thought about what we download. Of course, the Internet has tons of legitimate sites with safe content, but the ones that offer harmful content filled with malware are also out there.

Dive in!

The symptoms of a virus!

Frequent pop-up windows.

Pop-ups might encourage you to visit unusual sites. Or they might prod you to download antivirus or other software programs.

Changes to your homepage.

Your usual homepage may change to another website, for instance. Plus, you may be unable to reset it.

Mass emails being sent from your email account.

A criminal may take control of your account or send emails in your name from another infected computer.

Dive in!

The symptoms of a virus!

Frequent crashes.

A virus can inflict major damage on your hard drive. This may cause your device to freeze or crash. It may also prevent your device from coming back on.

Unusually slow computer performance

A sudden change of processing speed could signal that your computer has a virus.

Unknown programs that start when you turn on your pc

You may become aware of the unfamiliar program when you start your computer. Or you might notice it by checking your computer's list of active applications.

Unusual activities like password changes

This could prevent you from logging into your computer.

Dive in!

It's time to act!

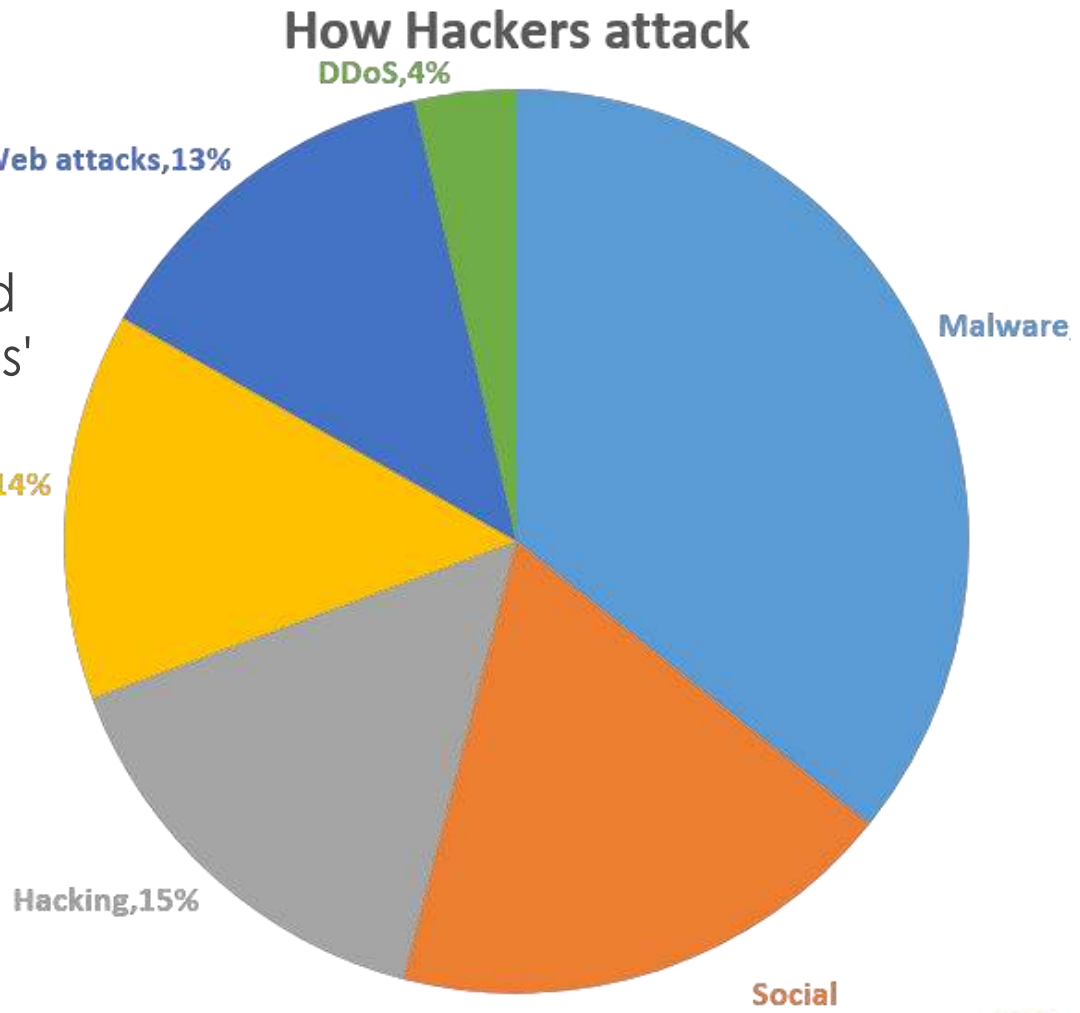
Protect yourself from viruses and malware

1. Keep your software up to date
2. Don't click on links within emails
3. Use free antivirus software
4. Back up your computer
5. Use a strong password
6. Use a firewall
7. Minimise downloads
8. Use a pop-up blocker

Dive in!

Cyber attacks and viruses: who's behind them?

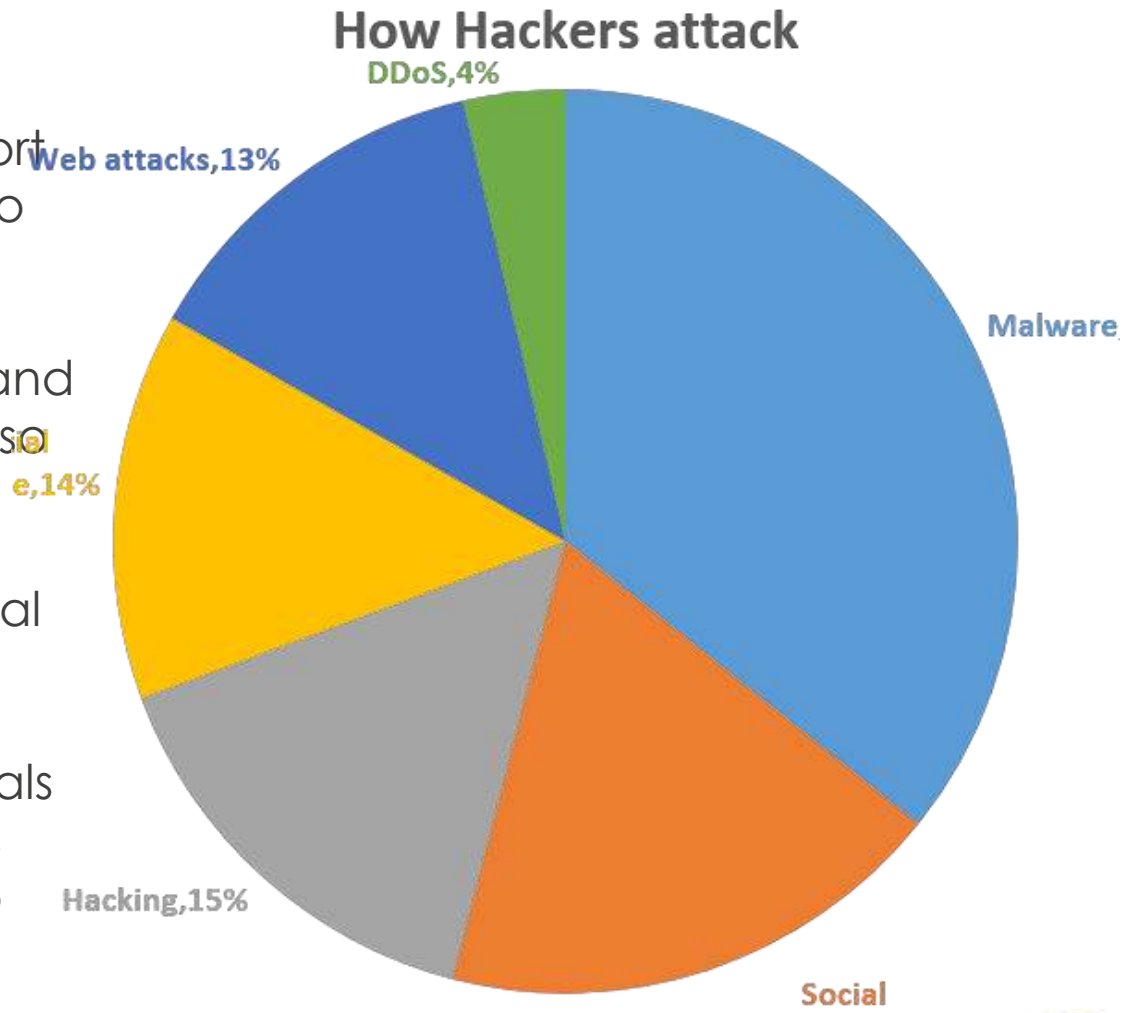
1. Malware: Cybercriminals continue to steal data from victims' computers, most commonly using spyware or remote administration malware using vulnerabilities, social engineering, or brute forced passwords, planting malicious software on victims' devices via infected websites, and sending malicious attachments or links by email.
2. Social engineering: Cybercriminals continue to innovate in the social engineering space, developing new methods to manipulate users into believing a message, link, or attachment is from a trusted source, and then infecting targeted systems with malware, stealing money, or accessing confidential information.



Dive in!

Cyber attacks and viruses: who's behind them?

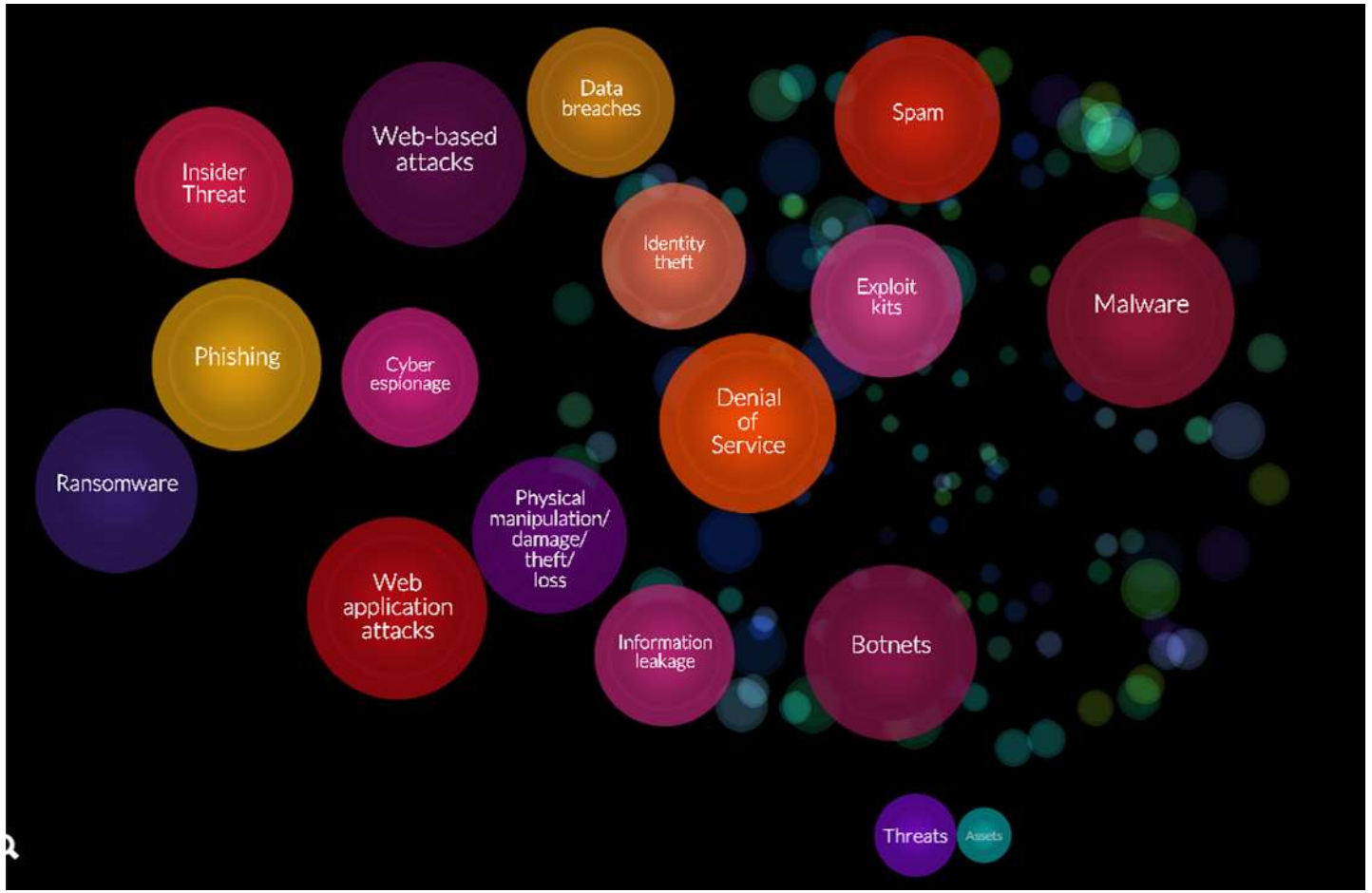
3. Hacking: exploiting vulnerabilities in software and hardware is often the first step in an attack, the report stated. Hackers currently cause the most damage to governments, banks, and cryptocurrency platforms.
4. Credential compromise: While enterprise users increasingly look to password managers for storing and keeping track of passwords, these managers can also be vulnerable to attack, the report noted.
5. Web attacks: Cybercriminals can extort website operators for profit, sometimes by threatening to steal client databases or shut down the website.
6. DDoS: Denial of Service attacks typically hit government institutions, and political events. Criminals also perform DDoS attacks for profit, taking websites offline and demanding payment from the victims to stop the attack



Dive in!

Check here to know the major threats in Europe:

https://etl.enisa.europa.eu/#/



Dive in!

Some tips for you

Slow down. Spammers want you to act first and think later. If the message conveys a sense of urgency or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.

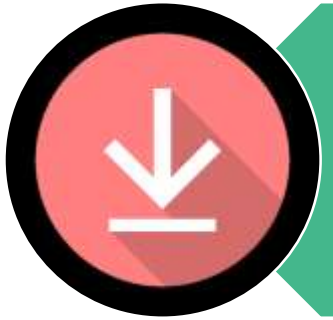
Research the facts. Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company's site, or a phone directory to find their phone number.

Don't let a link be in control of where you land. Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.

Dive in!

Some tips for you

Email hijacking is rampant. Hackers, spammers, and social engineers taking over control of people's email accounts (and other communication accounts) has become very common. Once they control an email account, they prey on the trust of the person's contacts. Even when the sender appears to be someone you know, if you aren't expecting an email with a link or attachment check with your friend before opening links or downloading.



Beware of any download. If you don't know the sender personally AND expect a file from them, downloading anything is a mistake.

Foreign offers are fake. If you receive an email from a foreign lottery or sweepstakes, money from an unknown relative, or requests to transfer funds from a foreign country for a share of the money it is guaranteed to be a scam.

Dive in!

Know who is in charge to protect you!

European Union Agency for Network and information Security: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering

EUROPOL: https://www.europol.europa.eu/newsroom/news/15-ways-you-could-be-next-victim-of-cybercrime

Thank you for your attention!

DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Project number: 2017-1-PL01-KA2014-038433

Co-funded by the
Erasmus+ Programme
of the European Union

DIGIT

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Wrap-up!

Be safe online and secure your PC

Project number: 2017-1-PL01-KA2014-038433

Co-funded by the Erasmus+ Programme of the European Union

Dive in!

Lesson learned?

Check what you do right now to protect your PC from viruses or to navigate safely.

Are there any changes you would make after this session?

Wrap-up!

How to Protect Your Computer From Viruses and Hackers

Wrap-up!

Social Engineering - How to Scam Your Way into Anything

Assessment questionnaire

External resources

Thank you for your attention!

DIGITO

BOOST COMPETENCES FOR RESPONSIBLE ONLINE IDENTITY

Project number: 2017-1-PL01-KA2014-038433

Co-funded by the
Erasmus+ Programme
of the European Union