Content Unit

Check Unit

Project: B-SAFE
Number: 2018-1CZ01-KA204-048148
Name of author: UDIMA
Last processing date: 24.8.2020

Funded by the
Erasmus+ Programme
of the European Union

"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

1. The ten the biggest Internet threats for users

It is easy to access the internet in this digital era and it offers many ways to explore the virtual world where, unlike the real world, everything is easily accessible. It opens a new world and is coming along with lots of advantages but also many risks.

1. Inappropriate content

There are tons of contents on the internet and not all of this contents are socially acceptable nor are they classified by age or area. Some content may be illegal, inappropriate, offensive, or unsuitable for some age groups. Anyone can find inappropriate, disturbing, or explicit content, even small children without supervision.

Many disturbing websites are not ‘illegal’ which means that no one monitors and manages their content. Some of these contents are pornography, violence, dangerous products (such as weapons), racism or hate, pro-ana sites (promote anorexia), or other sites with extremist content.

2. Data theft

Financial or personal information is stolen through the use of computers, server and other electronic devices in order to obtain some benefit or harm the victim. Cyber thieves can target banks, corporations, and individuals. It is an illegal act of obtaining sensitive data, which includes unencrypted also credit card numbers, bank account details of individuals, passwords, information stored in businesses, trade secrets, intellectual property, source code, customers’ information, or employee records.

The cybercriminal can access these users’ computers through spyware, which is a software that enables a user to obtain information about another’s computer activities.

3. Identity theft

Identity theft is the act of stealing personal identification information to commit illegal acts.
In the first phase, the offender acquires a foreign computer identity. This is most often done by stealing electronic data (passwords, access data, etc.), usually by unauthorised copying (skimming), deceitful phishing, or hacking.

In the second phase, the perpetrator misuses the identity for own benefit to harm the victim. For example by acting under its name in social networks such as Facebook. It is the act of stealing personal identification information to commit illegal acts, such as: opening a credit line, renting a house, purchasing goods or services, auction- and wage-related fraud or extortion.

4. Unwanted attention

This kind of attention could come from someone who is simply obsessed with the victim (cyberstalking) or someone whose intention is to harm the victim (cyberbullying).

On the one hand, Cyberstalking is unwanted obsessive attention to a specific person through the internet. It is committed via online technology such as e-mail, social networks, instant messaging, personal data available online – everything on the Internet can be used by cyberstalkers to make inappropriate contact with their victims. Some ways are following the person online, looking for personal information in an obssesive way, secretly watching online , persistent calling and texting to manipulate, and different other means to approach the victim unexpectedly.

On the other hand, cyberbullying is a crime that occurs when people use social media or the internet to intimidate, harass, threaten, or belittle others.

5. Scams and tricks

One type of scam or trick would be phishing. It is a practice of sending fraudulent communications that appear to come from a trustable source, usually through e-mail.

These communications can include malware (spyware, ransomware, viruses and worms), which usually happens due to dangerous clicks or email attachment that then installs risky software.

6. Unwanted information

Using the Internet we can end up finding information that we weren't looking for or false information or profiles. You can find misleading information either instead of what you were looking for or without requesting.

The most popular online communication medium is e-mail. It is very common to use it in our daily routine and that is why this is one of the favourite mediums for spam. Fake e-mails are a common threat, but you can also reaceive these kind of misleading informartion through social networks messages or different websites.

Moreover, fake news can be found everywhere, not only when using ~~the~~ e-mail. On social media it is very common to find not only fake news but also fake identities.

7. Easy spreading and long staying

Information such as photos, news, etc., can be uploaded anytime, anywhere and by anyone. Once, the information is online, it remains there forever so you must be very careful with the information that you share online.

It is also very easy to spread it all around the world and in a short period of time.

8. Destruction or modification of data

Important data can be destroyed or modified in the user's computer in order to harm.

One way could be through viruses, which are computer programs designed to infect other computer programs, destroying essential system data and making networks inoperable. Another example could be trojans, which are computer programs that get access to a computer or system that is camouflaged in the form of regular software in order to cause damage to system processes, hard drive data, etc.

9. Disabling the device

The computer's operating system device can be attacked by a trojan. It is a computer program that gets access to a computer or system.

Trojans are camouflaged in the form of regular software in order to cause damage to system processes, hard drive data, etc. Mostly introduced via e-mail attachments.

10. Cyberterrorism

Cyberterrorism is always more severe than other behaviors that are carried out in or through cyberspace.

This kind of crime is a cyberattack that aims to generate fear or intimidate society with an ideological goal. For this purpose, the terrorist uses computers or communication networks to cause enough destruction or disruption.

2. The top ten most important rules for internet safety behaviour"

1. Passwords

Many services on the Internet are protected with an access code, in order to protect the privacy of the information. If this password is simple or common (very easy among users) it could be easily guessed improperlyaccessing the account as if it were the real user. For this reason, the use of strong passwords is recommended, with more than 8 characters in combination with letters (upper and lower case), digits and special characters; avoid personal information such as the national identity number, names of relatives or acquaintances and never use very simple patterns, or dictionary words. For greater security, it is recommended to periodically modify passwords. Passwords should never be recorded in notebooks or unencrypted files.

2. Security technologies

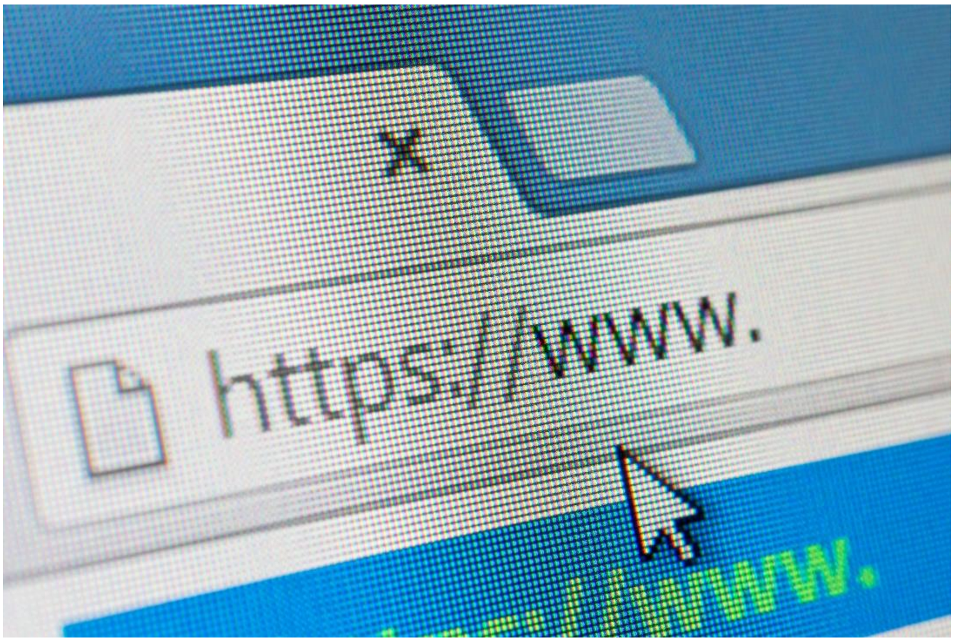
Create several backups of all your important data and make sure that they aren't all stored in the same place. Always keep your software up to date. Install a phishing filter/software on your email application and also on your web browser.

Antivirus, firewall and antispam solutions represent the most important applications for protecting the computer against the main threats that spread over the Internet. Using these technologies reduces risk and exposure to threats. To protect against viruses run regularly scheduled scans with your anti-virus software and make sure your anti-virus and anti-spyware software are compatible.

3. Trusted pages

Through Social Engineering techniques, many websites are often promoted with data that can attract the user's attention - such as discounts on the purchase of products (or even free offers), scoops or exclusive materials for current news, multimedia material, etc. . For safe browsing, it is recommended that the user is aware of these messages and avoid accessing webpages with these characteristics.

Verify the SSL credentials of the website and never use personal/sensitive information on sites that do not have a valid SSL certificate installed.



Through Black Hat SEO techniques, attackers often place their websites among the first places in search engine results, especially in cases of searches for keywords widely used by the public, such as current affairs, extravagant news or popular themes (such as sports and sex). In the event of any of these searches, the user must be attentive to the results and verify which websites are being linked.

If we do not want to leave our mark on the Internet, one of the safest ways is through a private virtual network or through a proxy server that acts as an intermediary in communication with the website we visit.

4. Share information

All the information we upload to the internet about ourselves, the images we share on social networks leave a digital trail that make up what is known as our 'digital identity'. For this reason, it is necessary to be aware especially with the digital l identity that we create and only upload information about ourselves that we consider one hundred percent public.

Do not give access to your location, camera or microphone to avoid giving extra information. Don't use the GPS to show on your publications where you are.

In both instant messaging clients and social networks, it is recommended to accept and interact only with known contacts. This avoids accessing the profiles created by attackers to communicate with victims and expose them to various threats such as malware, phishing, cyberbullying, or others.

5. Free WiFi networks

If you use a free Wifi network to browse public pages, the risk is minimal. However, we must avoid browsing web pages that allow us to enter personal data, such as passwords or users' names, since the Wifi could be compromised and therefore someone could intercept our personal data. We must pay the same attention when we connect to known Wifis..

6. Suspicious links

One of the most widely used means of directing victims to malicious sites is hyperlinks or links. Avoiding clicking on these prevents access to webpages that have threats capable of infecting the user. Links can be present in an email, a chat window or a message on a social network: the key is to analyse whether they are offered in any suspicious situation that make you doubt (an invitation to see a photo in a language other than your own, for example), come from an unknown sender or refer to an unreliable website.

7. File download

One of the biggest security breaches comes from downloading files. If you are not completely sure of the origin of what you are downloading, avoid it or check it before downloading. Many sites pretend to offer popular programs that are altered, modified or supplanted by versions that contain some type of malware and download the malicious code at the moment the user installs it on the system. Therefore, it is recommended that when downloading applications always do so from the official web pages.

On the other hand, malware propagation is usually done through executable files. It is recommended to avoid running files unless the security of the files is known and their provenance is reliable (whether it comes from an Instant Messaging contact, an email or a website).

8. Updating the operating system and applications

Having the operating system (Windows, Linux, Apple ...) and all the installed applications correctly updated is one of the main guarantees for not leaving open doors to your computer that cyber criminals can exploit. Although updating computers takes time, and sometimes requires a reboot, it is essential to fix security vulnerabilities in installed software.

If you are already taking the precautions of the case when browsing from your desktop or laptop PC, do not forget your mobile, it is very important that you take into account the same rules for this case. Through devices such as smartphones, the owners of others are more likely to violate security elements that your operating system may offer you.

9. Avoid entering personal information in dubious forms

When the user is faced with a webform that contains fields with sensitive information (for example, username and password), it is recommended to verify the legitimacy of the site. A good strategy is to check the domain and the use of the HTTPS protocol to guarantee the confidentiality of the information. In this way, phishing attacks that try to obtain sensitive information can be prevented by simulating a trusted entity.

10. Cookies

A cookie is a file created by a website that contains small amounts of data -that is sent between a sender and a receiver, in order to know the preferences of the user and to make their experience on the site easier. However, the information that is shared is likely to reach third parties, so it is convenient to assess the traffic of this data and in any case, from the browser we can decide to delete these cookies to avoid unnecessary scares.

Apply knowledge

Cybercrime

1. What is the definition of the cybercrime?

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) Cybercrime is watching the inappropriate content on internet.
b) Cybercrime is unlawful act wherein the computer is either a tool or target or both.
c) Cybercrime is monitoring of the work emails of employees by employers.
d) Cybercrime is obtaining the public information on Internet.

2. Which of the following examples is phishing?

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) You received a celebrating e-mail that you won the i-Phone and you should send some personal information to receive the prize.
b) You received an e-mail with some goods offer to buy it
c) You received an e-mail with the requirements of change the password to your bank account with the direct link to do it
d) You received an information e-mail about some cultural event in your city

3. True or False?
Hacking can also be perceived as the productive and useful act.

T □ **F** □

4. Match answers – you can drag and drop the correct answers to the certain part of the text

____________________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.

____________________ 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.

_____________________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
___________________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.
Cyberbullying, Cyberstalking, Identity theft, Financial crimes,

5. Complete the sentence with the correct word – fill in the blank.

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 is called (___________________).

Protection against inappropriate content

1. Match answers – you can drag and drop the correct answers to the certain part of the text

____________________ is described as an explicit description or image intended to stimulate sexual feelings.
_____________________ is the promotion or incitation of hatred against individuals or groups based on ethnic origin, religion, disability, age, nationality, veteran status, sexual orientation, gender, gender identity, or any other characteristic
______________________are the websites that understands anorexia as a lifestyle, not as a disease.

______________________ provide attractive information such as historical events, but facts are distorted and refer to other sources of information already manipulated by a shifted perception of the world.

Racism or hate, Pornography, Pro-ana websites, Sites with extremist content

2. Which rating can help me to recognize the websites with inappropriate content?

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) Motions picture Association rating (f.e. PG)
b) LT Int. Scale (f.e. LT Corporate Family ratings)
c) National Scale (f.e. NSR)
d) Online PEGI rating (f.e. PEGI 7)

3. Which of the following tools is the useful parental control for online content?

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) Protection online app
b) iWebfilter
c) K10 Web Protection
d) Anti-game

4. *Which skills are necessary to teach children to minimize the risks of the inappropriate content?*

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) IT skills
b) Critical thinking and resilience
c) Digital skills
d) Positive ways how to use tech

5. Complete the sentence with the correct word – fill in the blank
We can have the helpful tools for protection as the laws, parental controls, software settings, supporting institutions, but the key is the (_____________) between you and the child.
speech, trust, discussion, talk, communication,

Personal Data Protection

1. Complete the text with the correct words – fill in the blank

_________________, also known as information privacy, is an aspect of data security that deals with the proper handling of _________________. It mainly protects individual's personal data from _________________. The _________________ of personal data has been a _________________ right in Europe for years. Data protection has become more increasingly important in recent years due to _________________ and _________________ that facilitate the collection, processing, storage, dissemination and analysis of data. The _________________ is a legally binding regulation on the protection of individuals regarding the processing of personal data.

Misuse, technical developments, GDPR, fundamental, data privacy, personal data, protection, global networking,

2. True or False?

The GDPR only applies to the automatic processing of personal data

T □ F □

Personal data refers to sensitive data about an individual

T □ F □

Sensitive data must be increasingly protected

T □ F □

Personal data includes for example name, date of birth, age or home address, account number

T □ F □

Sensitive date includes for example credit card number, religious belief, union membership, racial and ethnic origin

T □ F □

3. Complete the text with the correct words – fill in the blank

The GDPR defines _________________ key principles that must be strictly complied within _________________. Violations of these principles can result in _________________. For _________________ personal data the GDPR has _________________ available lawful basics for processing as the processing of _________________ is prohibited in general unless specific conditions are met. Special requirements apply to the processing of _________________. Data processing is only permitted in specific _________________.

data processing, seven, non-sensitive, six, maximum penalties, personal data, sensitive data, exceptional cases

4. What is right regarding data breaches?

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) It is the duty of a data controller to inform the data processor immediately of any data breach.

b) If a data breach occurs, data controller must fulfil a reporting and notification obligation

c) If a data breach occurs, data processor must fulfil a reporting and notification obligation

d) The data protection authority must be informed within 24 hours

e) The data protection authority must be informed within 72 hours

f) The data protection authority must be informed if the violation is likely to pose a risk to the rights and freedoms of the data subjects

g) The additional notification of the data subject is not always necessary if there is likely to be a high risk for the rights and freedoms of the data subjects

5. Complete the text with the correct words – fill in the blank

In order to ensure the protection of _________________, the issue of _________________ is a central issue. In this context _________________ and _________________ are important keywords. _________________ refers to data protection through _________________. This means that when developing new technologies, appropriate solutions conforming to data protection must be ensured. _________________ signifies privacy through _________________. The person responsible must ensure by appropriate default settings that only those _________________ are processed, which are absolutely necessary.

personal data, data security, personal data, privacy by design, privacy by design, privacy by default, technological design, privacy by default, default settings

Smartphone Protection

1. What precautionary measure should you take to protect your smartphone and the private data stored on it in case of loss or theft?

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) Use a personal identification number and a screen lock
b) Use a Pin with a common number combination so that is easy to remember for you
c) Note the serial number of your smartphone
d) Do not install an anti-theft application

2. What is correct about IM?

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) IM (instant messaging) is an offline chat to exchange messages.
b) Instant messaging is an internet-based communication via mobile apps
c) The message transmission takes place in the so-called pull procedure
d) IM is only for the transmission of texts.
e) Examples of IM are WhatsApp, Skype or Facebook Messenger

3. Most IM apps are for free. What risks are coming along?

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) The app has to be paid later on, coming along with high costs
b) The individual's data is usually the product
c) Communication is mostly encrypted
d) Malware of all kinds is hidden in the apps

4. True or False?

There is no problem with unrestricted app permission
T □ F □

App producers are interested in your personal data
T □ F □

All access to personal data is obvious via the permission forms of an app
T □ F □

Data protection is an increasingly important issue regarding IM and apps
T □ F □

There is a risk of phishing
T □ F □

There is no problem with unencrypted communication
T □ F □

5. Complete the sentence with the correct word – fill in the blank

Given the potential _________________ of using apps on your smartphone, you're probably wondering how you can better protect yourself and your privacy. Here are some tips on what to consider when using apps on your smartphone: always use the _________________ version of the app, _________________ from using

images that you do not own as profile images, read the _________________ carefully before installing an app, enter only the _________________ data, use an _________________ that doesn't reveal much about you and doesn't bother you when it comes to spam, check the _________________ rights of the app and adjust them if necessary, adjust the _________________ of apps (e.g. visibility of profile pictures) and _________________ unwanted contacts.
block, security risks, refrain, latest, access, privacy policy, privacy setting of apps, most necessary, extra e-mail address

Information Stream/Online Communication

1. The most common online communication medium is

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) Instant messaging
b) E-Mail
c) Websites

2. Complete the sentence with the correct word – fill in the blank
_________________ are undesirable e-mails that mislead you in bad faith with deceptive information or lead you to perform harmful acts. Malicious programs are for example often transferred to fake e-mails via _________________. It is therefore important to be aware of the typical characteristics of malicious e-mails. Thus take care of the following: something is promised that seems _________________ (too good to be true), the content of the email somehow does not fit with the (supposed) trusted _________________, the e-mail contains certain _________________ words as the subject-matter (e.g. "last reminder" or "account blocked"), you are asked to disclose _________________, the _________________ seems strange, the e-mail contains a lot of _________________ (spelling or grammar), the e-mail is automatically moved to the _________________ or you are prompted to run programs with strange _________________ (e.g. jpg.vbs" or "gif.exe").
Fake e-mails, mistakes, attachments, spam folder, irritating, unrealistic, e-mail sender, confidential information, sender, file names.

3. Forums and chat rooms are both well-known and popular media for online communication and information exchange. Which statements are correct?

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) Forums are suitable for real time communication
b) Chats are suitable for real time communication
c) Forums are suitable for discussions where not all participants need to be online at the same time
d) Chats are suitable for discussions where not all participants need to be online at the same time
e) Forums are better organised
f) Chats are better organised
g) Only forums require a registration with a valid e-mail address
h) Chats and forums allow the exchange of text messages, but can usually also be used to exchange images, videos, links or files

4. What are the main risks of using forums and chats?

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) False identities
b) Malware
c) High costs
d) Links to phishing sites

e) Unencrypted communication
f) Encrypted communication

5. Complete the text with the correct words – fill in the blank

In social networks, the assumption of presumed anonymity can lead to thoughtless behaviour in dealing with _________________ and _________________. As a result, social networks are increasingly being targeted for _________________ activities. There is a danger of being misled by _________________ or by the conscious or unconscious dissemination of _________________. Thus, you should always consider the following aspects when dealing with _________________: never publish and discuss _________________ and _________________information in a public virtual space, use the _________________ provided to make information only accessible to a certain group of people, be critical when _________________ friends, check social networking settings for _________________ and be aware of _________________ information. If you detect misuse or misconduct on social networks, you should _________________ it to the service provider and appropriate _________________ and organizations.

false information, social media, confidential, data, fraudulent, misleading, report, false identities, information, authorities, privacy protection, accepting, personal, filters

Parental Control

1. The consequences for the victim of sexting are:

Task: Pick the right options following the multiple-choice principle: There could be more than one correct answer

a) Humiliation and social lynching for the protagonist of the images.
b) The minor faces public insult, affecting first of all his self-esteem, at an age in which their personality is being formed and largely depends on the image that others perveive as the opinion of others is important..
c) There are also feelings of helplessness, mainly when the case is told to parents, or educators, or guilt for being in that situation.
d) There are no consequences

2. Complete the text with the correct words – fill in the blank

Grooming is defined as _____________ deliberately carried out by an ________ to establish a relationship and emotional control over a minor in order to prepare the ground for sexual _____. In some cases, it is performed between minors, but usually with an age difference, where the eldest is usually the __________. The objective of grooming is to gain the trust of the _______, to obtain images or videos of ________ content, and even to meet in person.

Adult, cyberbullying, sexual, abuse, minor, harasser

3. Complete the text with the correct word – fill in the blank

One of the first steps of the ____________ used to be a bully who insults or threats the _________ by saying he or she will leak information that will __________ his/her _____________. The information sent by the stalker about the harassed may be true, but in this case, it will be leaked on purpose due to the fact of being _____________- or harmful for the interest of the harassed or it might be directly false. If so, it becomes ________________.

Cyberbullying, reputation, misinformation, negative, victim, damage

4. Complete the text with the correct word – fill in the blank

A way of finding out if the ______ is suffering __________ is to analyse the amount of time spent using the ______ devices, the frequency and the _______________ manifestations about not staying tuned. If the minor appears to be ______, anxious or agitated when he/she is not connected, or if he/she experiments frequent _________ swings, netholism could be the reason why.

Minor, emotional, mood, digital, netholism

5. Complete the sentence with the correct word – fill in the blank

Several techniques can be used to secretly data ____ from a digital device. Sometimes the _____________ hide their intentions by looking as something different than they are. For instance, in the ads, requiring information to visualize the content or asking the____________ to enjoy an ________ service. But, more often ___________ share their data because they are not aware of the danger, so a more responsible way of acting on the ________ is vitally needed.

Passwords, online, minors, leak, perpetrators, internet

Hardware and software

1. *Complete the following text.*

Hardware refers to the ___________ elements of a computer. Examples of hardware in a computer are ________________. Software, commonly know as ______________________ consists of all the instructions that tell the hardware how to perform a certain function. Software is capable of performing _____________ different tasks with the same basic hardware.

monitor and mouse, keyboard, physical, programs or apps, many

2. *What tips/tricks can you do regarding software protection? (multiple choice – one answer is not correct)*

a) Regular updates to software
b) Create several backups
c) Don't install software firewalls
d) Encrypt information

3. *One example of hardware protection is to avoid buying hardware components from risky sources/countries (True/false choice).*

a) True
b) False

4. *What measures can you implement to have a better software protection? (multiple choice – one answer is not correct)*

a) Install an antivirus and keep it updated
b) Explore the security tools you install
c) Install operating system updates once in a while
d) Disable file and media sharing if you don't need it

5. *What are the most common attacks to hardware? (multiple choice – two answers are not correct)*

a) Physical accidents
b) Modding
c) Trojan
d) Phishing

Personal data in social media

1. What security issues you should be careful when you use social media? (multiple choice - Pick the right options following the multiple-choice principle. None, one, more than one or all options can be true)

a) If a link re-directs you to a website you should pay attention to see if there is a physical address and contacts
b) See if a website have a return policy as well as their shipping policy
c) When you receive a friend request from a someone that you don't recognize you can try a reverse image search
d) To avoid a phishing attack you should see the full URL which will help to show whether it leads to a legitimate website.

2. Match answers – you can drug and drop the correct answers to the certain part of the text.

Most of the websites allow the setting of information which is being posted as public or private information by using the control option "_____________".

How personal data is presented or stored on a particular social network is the responsibility of the ____________.

The most common attack in social media use a strategic to lure the user namely through a ____________________.

Social media owner/provider; Phishing attack; Privacy settings

3. What characteristics are related to social media networks? (multiple choice – one answer is not correct)

a) Interactive
b) Facilitate the creation or sharing of information, ideas, career interest and others forms of expression
c) Connection between two or more people
d) More than 4 billion active social media users

4. *What are the most common risks in social media? (multiple choice – one answer is not correct)*

a) Software that uses encryption to disable a target's access to its data, like photographs or documents, until a ransom is paid
b) Type of malicious code or software that looks legitimate but can take control of your computer
c) Form of malware that is capable of copying itself and spreading to other computer
d) Form of malware that do physical damage to your computer.

5. What tips can you apply to always be one step ahead from a potential cybercrime in social media? (multiple choice – one answer is not correct)

a) Don't save your credentials access in your devices/browser/applications
b) Avoid sharing personal information online
c) Have the latest security software
d) Check your privacy setting

Cybersecurity

1. *What is Cybersecurity? (multiple choice – one answer is not correct)*

a) Preventing and detecting digital attacks, protecting systems, hardware and software
b) Practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks
c) Cybersecurity only applies to software and hardware
d) Techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation

2. *In order to improve your cybersecurity online what measures from above can you apply? (multiple choice – one answer is not correct)*

a) Create different passwords to different accounts and profiles
b) Change your passwords once in a while and use a combination of uppercases and lowercases letters, symbols and numbers
c) Save your passwords in a spreadsheet in your computer
d) Use a multi-factor authentication factor (if possible) for different online accounts

3. *What precautions you should apply when you buy online? (multiple choice – one answer is not correct)*

a) Read reviews and see if other consumers have had a positive or negative experience in that specific website
b) Create virtual credit cards
c) Keep you anti-virus and anti-spyware software updated along with your firewall
d) **Don’t read the terms and conditions of different websites because they are all very similar**

4. *From the list, please select the right sentences concerning the definition and application of cloud computing. (multiple choice – one answer is not correct)*
a) Practice of using a network of remote servers hosted on the Internet to store, manage and process data rather than a local server or a personal computer
b) Delivery of different services through the Internet including servers, storage, databases, networking, software and analytics
c) **There is only one type of cloud computing solutions**
d) Cloud computing can be provisioned without human interaction

5. *What measures can you use in order to improve cloud computing? (multiple choice – one answer is not correct)*
a) Use a multi-factor authentication
b) Setting different levels of authorization to information according to what people needs
c) Ensure training concerning the protection of data and private information
d) **Do backups to your data/information once in a while**

Internet of things – 5 quiz questions

1. What IoT sentences are correct? (multiple choice - Pick the right options following the multiple-choice principle. None, one, more than one or all options can be true)
a) The IoT will improve public transportation
b) IoT is turning physical objects into an ecosystem of information shared between devices that are wearable, portable, even implantable, making our lives technology and data rich
c) IoT business applications are numerous
d) Smart cars, wearable fitness and trackers, voice assistants and smart cars are all examples of IoT technologies

2. From the list, please select the right options regarding Internet of Things? (multiple choice – one answer is not correct)
a) The IoT can only be applied to people and homes and to the car industry
b) System of interrelated computing devices, mechanical and digital machines
c) Convergence of multiple technologies, real-time analytics, machine learning, commodity sensor and embedded systems
d) The term IoT encompasses everything connected to the internet

3. What are the most common applications of Internet of Things? (multiple choice - Pick the right options following the multiple-choice principle. None, one, more than one or all options can be true)
a) Wearable device that monitors blood glucose
b) A fridge that automatically creates shopping lists
c) Smart cities and smart homes
d) Retail and connected cards

4. In order to protect yourself from cyberattacks in all the layers that composes IoT devices what measures, from the list above, can you apply? (multiple choice - Pick the right options following the multiple-choice principle. None, one, more than one or all options can be true)

a) Device authentication
b) Install reputable internet security softwares on your computers, tables and smartphones
c) Use a VPN solutions because it helps to secure the data transmitted on your home or public Wi-Fi
d) Check the device manufacturer’s website regularly for firmware updates

5. What are the most important steps to prevent a cybersecurity breach? (multiple choice - Pick the right options following the multiple-choice principle. None, one, more than one or all options can be true)

a) Identify threats and vulnerabilities
b) Asset risk exposure through different types of analyses
c) Develop protection and contingency plans
d) Determine when to alert emergency response team, cybersecurity professionals, service providers and/or insurance providers

Answer Key

Cybercrime

1b, 2ac, 3T
4: Identify theft, Cyberbullying, Financial crimes, Cyberstalking
5: Cyberterrorism

Protection against inappropriate content

1: Pornography, Racism or hate, Pro-ana websites, Sites with extremist content

2ad, 3b, 4bd

5: trust, discussion, talk, communication, speech

Personal Data Protection

1: data privacy, personal data, misuse, protection, fundamental, technical developments, global networking, GDPR
2: aF, bF, cT, dT, eF
3: seven, data processing, maximum penalties, non-sensitive, six, personal data, sensitive data, exceptional cases
4: b e f
5: personal data, data security, privacy by design, privacy by default, privacy by design, technological design, privacy by default, default settings, personal data

Smartphone Protection

1ac 2be 3bd
4: aF, bT, cF, dT, eT, fF
5: security risks, latest, refrain, privacy policy, most necessary, extra e-mail address, access, privacy settings of apps, block

Information Stream/Online Communication

1b
2: Fake e-mails, attachments, unrealistic, e-mail sender, irritating, confidential information, sender, mistakes, spam folder, file names.
3: b c e h
4: a b d e
5: data, information, fraudulent, false identities, false information, social media, personal, confidential, filters, accepting, privacy protection, misleading, report, authorities

Parental Control

1 a b c
2: Cyberbullying, adult, sexual, minor, abuse, harasser
3: Cyberbullying, victim, damage, reputation, negative, misinformation
4: Minor, digital, digital, netholism, mood, emotional
5: Leak, perpetrators, passwords, online, minors, internet

Hardware and software

1: keyboard, monitor and mouse; programs or apps; physical; many
2: g
3: True
4: g
5: g,h

Personal data in social media

1: a, b, c, d
2: Social media owner/provider; Phishing attack; Privacy settings
3: d
4: d
5: a

Cybersecurity

1: c
2: c
3: d
4: c
5: d

Internet of Things

1: a, b, c, d
2: a
3: b
4: a, b, c, d
5: a, b, c, d