LESSON 1.1 - PROTECTING DIGITAL DEVICES

INTRODUCTION

We live in a world immersed in technological change, and it happens constantly, on a daily basis. The rules that run the necessary and logical behaviour are constantly in a “Beta” state since the changes happen at an incredible speed.

When it comes to new challenges, we need to face them with a positive and responsible attitude that we must obtain through necessary formation in the related areas.

We need to be conscious of how neglecting our personal data can affect us. Just like we keep some details of our life away from the internet, we must keep that habit in our digital lives. We should not spread our information in an irresponsible way without knowing where it can end up since information is always susceptible to interpretations and possible misuse by third-parties (blackmail, fraud…).

We’ll start by focusing on the information that we have in our devices and how it can be exposed accidentally and be stolen by third-parties. Although it is a complex matter to deal with, we have to know the essentials to protect our data and be sure that we have taken all the required steps to ensure our information and our devices are as secure as possible.

PROTECT YOUR DATA - OPERATING SYSTEMS

When you buy a digital device, whether it is a computer or a Smartphone, it usually comes with an Operating System (OS) installed.

Most of the infections, attacks, security breaches etc. are usually only possible because of the connection between the digital device and the internet.

What can we do?

From our side, the best we can do is to keep our Operating System updated as often as possible. Companies release their own updates frequently. If the OS provides Automatic Updates, the updates will download and install automatically. If the automatic update feature is not activated or configured correctly, visit the

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

This project has been funded with support from the European Commission.
This publication reflects the views of its authors only, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

OS developer page for the latest updates or how to activate it. Do not update your OS though unknown or unreliable sources, because it might expose the OS to malware.

Where?

- Windows: In Windows updating the Operating System is really simple:
  We go to the start menu and type in “update”, this will show the “Windows Update” option. From there it’s as easy as clicking “Search for updates” button. From the same window, we can activate the Automatic Updates.

- MacOS: As a general rule, Mac informs users about available new updates through a pop-up window in the 'Notification tab' taking us to its download and installation.
- Linux: Updating Linux to its latest version sometimes implies reinstalling the entire distribution you are using. Although, we can just update the Linux packages manually to its most recent version.
  The command sequence is:

1. Open the terminal (**Control + Alt + T**)
2. Write **sudo apt-get update** and press **enter**.
3. Now repeat with **sudo apt-get upgrade**
4. When the installation is done, restart your PC

- Android: With Android, at the start of every month Google posts a security log on all the registered vulnerabilities and security losses. With this post, the monthly update is released. The Android Over the Air or OTA update is the easiest way to update your Android device. These updates pop up in the device as a notification and all that is required is to accept the installation. You can manually install it from “**Settings/System/About this device**”.

- IOS: In the case of IOS it manages automatic updates really well. We can also force them in “**Settings/General/Update Software”.**

There can be some variations on what has been mentioned above, depending on the OS you are using, but generally is the same for most of the devices.

PROTECT YOUR DATA - WEB BROWSERS

In the case of Web Browsers, the risk of exposure to threats is higher. We use browsers to explore the web and to use a lot of resources (like applications) online. Each of these has its vulnerabilities, just like operating systems receive more attacks the more they are used among users.

What can we do?

Web browsers have extensions called, "Add-Ons", and “Plugins”, we need to know which security-related utilities we have for our web browsers and apply them so we can assure that we move through the net the safest we can.

Where?

In the configuration menu of our browsers, we have the possibility to reinforce our security with the use of “Extensions”. Below, you can find a table we have created to help you with this task.

Table 1: extensions related to security

		e	O	
No-Script Suite Lite	NoScript		NoScript Suite Lite	Disconnect
Tunnelbear	BetterPrivacy		Privacy Badger	
Ghostery	Ghostery	Ghostery	Ghostery	Ghostery
HTTPS Everywhere	HTTPS Everywhere		HTTPS Everywhere	TrafficLight
Web Of Trust	Web of Trust	Web of Trust	Web of Trust	Web of Trust

Each browser has its own security extensions and it is our duty to inform ourselves about the ones that can protect our system and apply the ones we think are most convenient depending on how we are going to use our devices.

PROTECT YOUR DATA - APPLICATIONS (SOFTWARE)

During the installation of any application of any type, we find ourselves with two options: 1). Download and install them from trusted websites assuring that they are the safest download, or 2). download them from a third-party website without the security given by the original developer.
Even if computers come with a good variety of the safest and most renowned applications available the user may want to download third-party applications.
In the case of mobile devices, the most popular stores like Google Play and Apple Store are where we can download most of the applications for Android and IOS. In these places, they periodically check all the available apps to make sure they are safe.
Google uses Google Play protect to find malware, spyware, or any type of harm. Apple has a revision team that analyzes the apps that get uploaded to their store. The System only allows apps from the official store reducing the risk of infection notoriously.

What can we do?

- Do not install applications from places that are not official. Only use trusted stores, or developer websites and trusted site.

- Do not install applications that offer functionalities that are not ethically correct. (Example: Apps that promise to allow us spying, hacking… functionalities).
    - Illegal software or games that allow us to obtain free services, items, etc… that should be purchased.
    - Apps that promise to win easy money.

Another important point is the allowance of permissions that we usually skip or accept. It is very usual that free apps ask for permission for specific aspects of our device (usually more than needed) such as: **Storing data, Camera, Contacts, Microphone, SMS, Telephone, Localization…** Allowance to give your GPS position to the app.
All these allowance result in danger that we can detect with one single read to allowance pop-ups.

Where?

Before installing any app, we can see every permission the app asks for:

- From our own phone, we can access permission configuration given to the apps from the settings menu in the Application section, and if we do not think that the app needs those permissions we can turn them off in there.
- We can uninstall any application that we consider suspicious of many malfunctions (the device heats quickly, the battery life is shorter than usual, something is generating unknown charges in my account, etc…).

BASIC AUTHENTICATION METHODS

When we think about accessing a service or our data, we think about secure access. Usually, this access concession comes with an authentication process. Anyone who manages or uses passwords must take into account certain good practices when generating passwords.

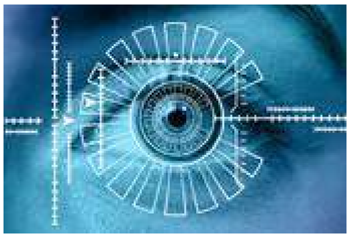
- We should not use default passwords. (widely used in electronic devices)
- Passwords must be robust, impersonal safe and we do not have to reuse them.
- Passwords must be changed periodically.
- Do not use the same password for different service.
- Do not use a password reminder.
- Hints for secure password creation:
    - Include numbers.
    - Use a combination of uppercase and lowercase letters.
    - Include special characters. What are special characters? See Examples: - * ? ! @ # $ / ( ) { } = . , ; :

Once connected to our host, we must know that we can endanger our information if we do not take the necessary measures. Let’s check the following cases about ending our session in a definitive or temporary way:

- Closing session or changing user (in case the host has more than one account or is used by more than one user, browsers, web services, etc ...)
- Lock the screen in case of being absent from your computer for a short period of time, to prevent others from accessing your files or running applications
- We must configure applications, browsers, and services to prevent our connection data from the different applications from being automatically stored locally once we stop using them (normally from the privacy settings area) or if it is not possible to delete them manually.

Other alternatives to using passwords in a traditional way can be:

- Verification in two steps: it is not a complete alternative to the password, but a reinforcement that increases your security. It is based on a double verification: "something we know" (the password) together with "something we are" or "something we have". Most of the time, this second factor is usually a code sent by text (SMS) or mail.
- The fingerprint as an alternative to the password has advanced dramatically in recent years thanks to smartphone development.
- Other biometric data such as iris recognition, facial recognition, heart rate...
- Use of unique and temporary password. The system would generate a random and temporary code that is sent to us by text (SMS) every time we try to log in.



Source of images: https://pixabay.com

MULTIPLE-FACTOR AUTHENTICATION - WHAT IS IT?

Secure access has become an obligation for accessing our devices, everyone understands that access without a supervised control it is not the safest way to keep our data. That is why the Operating Systems, Applications, Cloud Storage, etc. security keeps getting more efficient assuring that everything is as secure as it can be. It's recommended to have a tough and secure password, and for the system to control access to verify the user and give them access to their data.
Access control has undergone various changes over time forcing the user to create new, more secure passwords and use multiple-factor authentication which consists of:

The Multiple-Factor Authentication (MFA) is an authentication method based on more than one factor such as something the user **knows** (pin, password), something the user **possesses** (USB token or a coordinate card) and something the user **is** (behaviour or physical trait: fingertips, iris, voice, or face) or a combination of some of those factors.

We must not mistake it with the Two-Steps verification. In the Two-Steps verification, the first step usually involves a password and a second factor such as a random code made by a token (external or internal device). For example, a password + a code sent by email or SMS. The token-based hardware can be compared to a key or a card with a display where the necessary key is generated for that specific occasion (these keys are called One-Time Passwords (OTP)). Software-based tokens create a One-Time Password similar to those used in a mobile app or desktop application.
The authentication of two or more factors increases the difficulty of any attempt of identity theft or password-stealing since the authentication only becomes effective if every verification required is fulfilled.
Example: authentication using a coordinate card does not need any physical token.

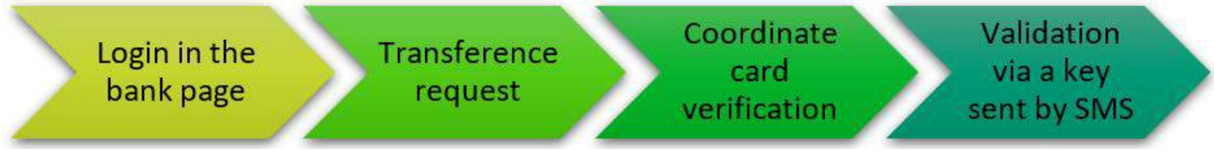
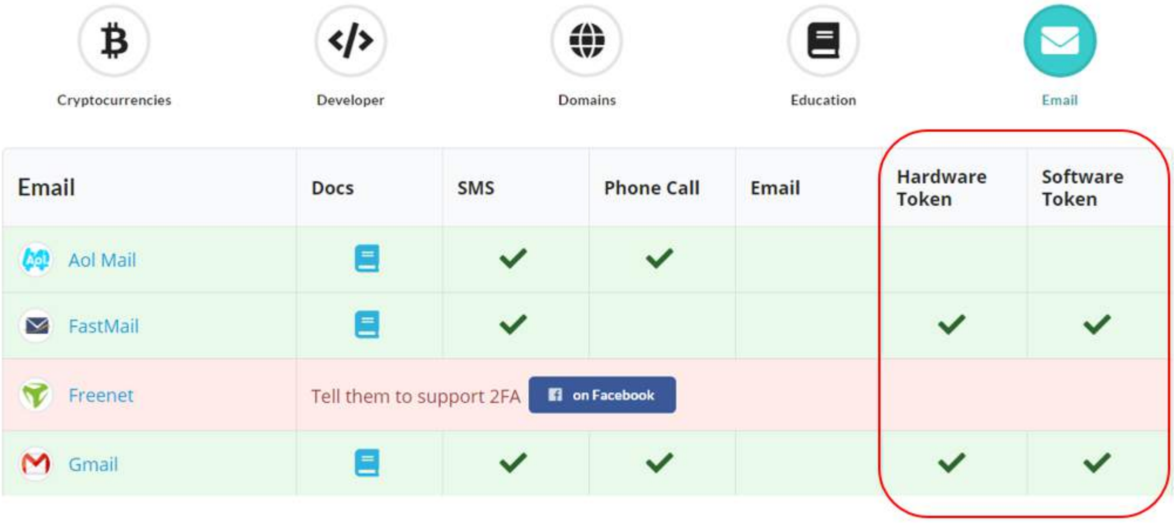

Login in the bank page
Transference request
Coordinate card verification
Validation via a key sent by SMS

Figure 1: Bank Operation (Multiple Factor Authentication)

MULTIPLE FACTOR AUTHENTICATION - WHAT CAN WE DO?

On the websiteTwoFactorAuth.org you can check which services use the double-factor or Multiple-Factor Authentication, as well as the procedures they use. It allows you to filter through a wide variety of services: email, e-banking, Cloud Computing, Communication, backup and sync, VPN Provider, and other services. Below you can see an example of two-factor authentication for an e-mail service.



Email	Docs	SMS	Phone Call	Email	Hardware Token	Software Token
Aol Mail	📘	✓	✓			
FastMail	📘	✓			✓	✓
Freenet	Tell them to support 2FA on Facebook					
Gmail	📘	✓	✓		✓	✓

Figure 2: Two factor authorisation example. Source: TwoFactorAuth.org

Now we can choose the services that use Two Factor Authenticator, it will be a safer procedure than the two-step verification which has become a vulnerable and unsafe procedure.
We can use a token-based in software, some examples are:

- Google Authenticator
- Amazon AWS MFA
- Microsoft
- Facebook
- Authy
- Duo Mobile

Services that manage sensitive information such as e-banking or e-commerce should use MFA. In your work environment it’s always recommended to use the multiple authenticator factor, we as teachers handling student data -in many cases underage-, we should use MFA whenever possible to prevent sensitive information from being exposed. Remember that the loss of our data can create legal problems for our school, college or institution.
When it comes to social media we must always try to configure the highest level of security as possible. We can tune it down for convenience but that means we can risk leaving our personal data exposed or having our identity supplanted.

If the services that we use do not allow these security methods, you can always use, as an intermediate, a password manager (free or paid), that allows double factor.

FIREWALLS, BUILDING WALLS

A **firewall** is a system (it can be hardware or software or both at the same time) that allows us to protect our device or a group of devices from possible hazards that come from the internet. It blocks unauthorized access and allows authorized outputs.

A firewall works like a barrier between our computer and outside networks. It can be configured from a list of options allowing us to accept certain transmissions from a specified port or to disable the reception of the same. This also applies to the transmissions we send.
Even if it looks easy to use we must not forget about the points where the firewall can not help us. The most common firewall limitations are:

- Attacks from outside its operational point, for example, those that come from within our organisation.
- Users from the organisation with access to our computers who have malicious intentions (copying sensitive data, infection, malware installation, etc.).
- "Social Engineering" attacks.
- Security breaches produced by services and protocols allowed by the firewall. Such is the case of services published on the Internet, we need to pay attention to their configuration.

It is important to correctly configure the firewall rules to allow the traffic of applications, services, etc. that we know are trustworthy and block the suspicious ones.
As far as we, as teachers, are concerned, both individually in our work and in what we teach our students about device protection, we are interested in personal firewalls:

- Windows: Comes with one already installed, where it lets us allow or block Applications, Protocols, and/or ports in a basic way.
- MacOS: Very similar to Windows. https://support.apple.com/es-es/HT201642
- **Linux**: Linux has a firewall called IPtables, which comes with the OS. With it, we can configure the default rules, filter by traffic through specific ports, and block the traffic from a specific IP or MAC, on both incoming and outgoing connections.
- IOS: By default, there's no firewall in IOS. To have one you have to install an external application that requires a JailBreak installation (an application that allows us to get administration control over our phone).
- Android: There is no default application or configuration and it comes with all the ports open. Like with IOS, to change the firewall you have to install an App with root settings. There are a few exceptions like the app *"Firewall without root"* that, as the name implies, it does not need root permissions.

PHYSICAL SECURITY (EXTERNAL STORAGE DEVICES)

External devices are always a threat source for our data. Infection through Universal Serial Bus (USB) devices occurs mainly when we are copying infected files from a USB to our computer. The firewall has no impact on them and a few manage to avoid antivirus software by simulating legitimate hardware. For example, the well-known 'badUSb' that passes itself off as a keyboard, mouse, etc. There are some cases where antivirus software is not capable of detecting those threats. Sometimes they become mini-hosts and are able to remove all content from the device. Everything mentioned above can apply to other external devices such as hard drives, memory cards, etc.

What can we do?

An important measure is not to install found or un-checked devices. We run the risk of background installation from internal programs that can damage or steal our data (usbHacking). Most of them are self-executing so, when they are plugged in, an automatic execution of instructions -previously programmed by the attacker- gets unleashed.

When using a suspicious device –maybe previously infected - before putting it into operation run a secure erase tool, like Eraser. This tool completely removes confidential data from your device by overwriting it several times with carefully selected patterns.

Disabling "autoplay" from USB disks can stop the execution of some of these threats, although this does not always work for all of them.

Protecting hard disk data, USB devices, memory cards, etc. using encryption (all the operating systems usually give you the option of applying encryption) and protect them with a password of your choice. It will be a good action in case there is a loss or theft of the physical device.

Where?

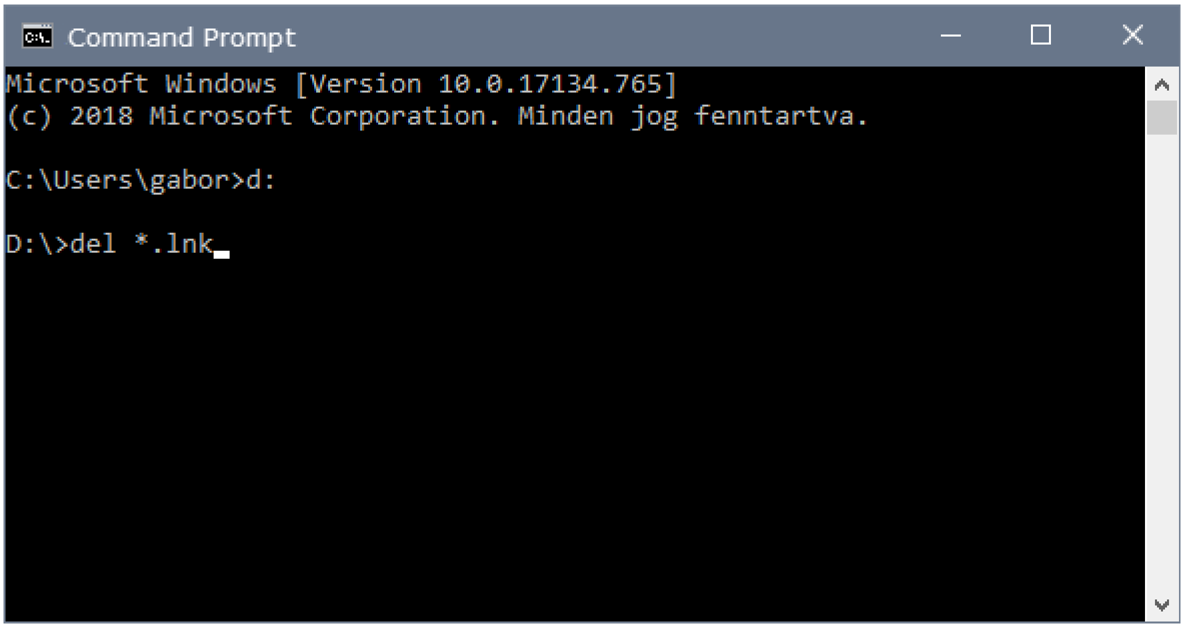
You can protect from data threats via external devices using **Windows GPO policies**.

Nevertheless, keep in mind that if the user who clicks to run a USB drive is an administrator, he could change the policy removing this protection, but this measure would make it difficult.

If the device is infected and the antivirus has real-time scanning, disinfection, and boot checking, it will always be more efficient because it will eliminate the infection before it is loaded from the service or program, preventing damage and making its elimination easier.

In case of removable device applications (i.e. **USB Disk Security**). This application can block USB access to our device, USB connection control, USB scanning, safe URL verification, and quarantine for insecure files.

There are manual solutions to solve popular cases like "Shortcut virus” in USB drives. You can run from the Command Prompt (CMD) the following lines in Windows:



```
Microsoft Windows [Version 10.0.17134.765]
(c) 2018 Microsoft Corporation. Minden jog fenntartva.

C:\Users\gabor>d:

D:\>del *.lnk
```

PHYSICAL PROTECTION OF OUR DEVICES

Last but not least, let us talk about the protection of our digital devices. For example, overconfidence in setting an unlock pattern can lead us to believe that leaving our mobile phone within reach of other people does not pose any danger. However, someone could obtain it, being able to access it if they have physical access to it.

According to a study by the United States Naval Academy and the University of Maryland, two out of three people are able to reproduce the pattern just by looking at it once at a distance of 1.8 meters, and if they could see it a second time, this figure would go up to 80%. In addition, the trace we leave on the screen when passing our finger, constantly drawing the same pattern, can also help another malicious person to obtain our pattern.

Although all the measures discussed in this topic are advancing more and more with the new implementations, carelessness can make these measures inefficient and therefore we should not overlook them.

What can we do?

Of course not showing anyone any of our security systems, or patterns or passwords. This is mandatory. In the same way, avoid leaving our devices within the reach of third parties in the same way that we would not leave our purse or personal documentation.

On mobile devices, it is possible to use simple routines in order to prevent anyone seeing our pattern being drawn or using a privacy filter like a thin plastic sheet that prevents the content of the screen from being seen from lateral angles.

Where?

In the case of Android devices, in settings/security you can configure the pattern so it is not drawn which protects us from malicious observers.

Each device will offer different access guarantees, knowing our devices and their benefits about security should be part of mandatory reading when acquiring any device.
The basic rule, in any case, is, not to leave devices without blocking when we cannot take them with us and not sharing their use with third parties. It is not about the trust we have for somebody, it is about security education.

Practical tips

Learning activity to be used in the classroom with our students:
We can use our mobile devices and enter the application settings and analyze if the permissions that we have granted to certain applications make sense, and then remove the permissions that we consider unnecessary from the application that compromises our data and then check whether the device's functionality has been affected

SUMMARY

The security of our data depends on many factors. Having updated software at all levels: operating system, browsers, application software, etc. and install add-ons and dedicated software will always be a guarantee of protection. In the same way, to provide security to our access methods, connection data will make it more difficult for us to suffer loss, theft, or deterioration/destruction of our data. The use of a good Firewall will prevent as far as possible the access of annoying guests as well as the information output from our team to the network. Special mention deserves common sense and information when it comes to protecting our connection data with the highest degree of authentication available and the necessary privacy. Regarding external devices encrypt the data, thought of accidental losses or theft will be more than interesting, taking again to common sense, don't use promotional devices or devices of unknown origin. Our devices may be vulnerable, let's use our knowledge to protect them as much as possible.

BIBLIOGRAPHY

1. Defensa Frente a las Ciberamenazas <https://www.ccn-cert.cni.es/> Retrieved on March 2019
2. Instituto Nacional de Ciberseguridad <https://www.incibe.es/> Retrieved on March 2019
3. Oficina de Seguridad del Internauta <https://www.osi.es/es/contra-virus> Retrieved on April 2019

LESSON 1.2 - RISKS AND THREATS IN DIGITAL ENVIRONMENTS

INTRODUCTION

This lesson introduces the advanced risks and threats existent in digital environments from a practical and useful view. The objective is to provide you with the knowledge to develop your skills in differentiate a wide variety of risks and threats, and know how to apply security and protection measures to protect you against them and be able to teach them to your students.

Along the lesson, you will be introduced to the most common threats and the guidelines to detect them, protect you and remove them if needed. Scams emails, threats on the websites and how detect and prevent malware will be the focus of this lesson. Although there are measurements our schools need to apply to the networks and systems we are using in the school, in this course, we will focus on the measures that we, as teachers, can apply and teach our students to avoid these threats.

Such as the European Union has defined, future European citizens need to be able to identify and protect themselves from these threats. We, as teachers, need to know how to apply these guidelines and the best practices to teach them in our classes. At the end of the lesson, you will be able to teach your students on how to detect, protect and remove the most common threats existent today in digital environments.

Source: https://picserver.org

INTRODUCTION TO DIGITAL RISKS AND THREATS

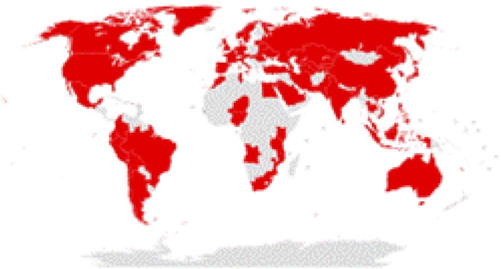
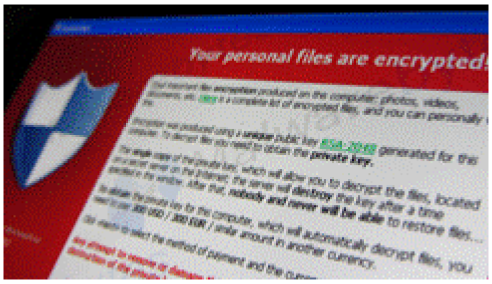
Today there is a wide variety of risks and threats in digital environments. New threats are constantly emerging that we have to face. Here is a list of the best known today:

- Malware:
    - Viruses: malicious executable code that is attached to other executable files and normally replaces them. It requires someone to run the program to infect the device
    - Worms: replicate themselves without human intervention by exploiting vulnerabilities. They do not alter programs, but are in the RAM memory and are quickly replicated from one computer to another slowing down the network and the connected devices.
    - Trojan horses: carry out malicious action disguised as legitimate software to give an attacker remote access to the infected computer.
    - Ransomware: program that blocks the access to a computer until a ransom is paid. It usually propagates as a worm (exploiting a vulnerability) or a Trojan horse (a downloaded file).
    - Rootkits: Software that modify the operating system to create a backdoor to allow access with admin privileges to the device continuously hiding its presence to the user.
    - Bot: software that automatically perform repetitive actions and it can be used to execute malicious actions, for example, denial-of-service attacks
- Email threats:
    - Spam: unsolicited messages over the internet sent with purposes of advertising, phishing, spreading malware, etc.
    - Phishing: fraudulent email disguised as being legitimate
- Browser threats:
- Spyware: spy on the user.
- Adware: deliver advertisements (usually with spyware).
- Scareware: persuade the user to take a specific action based in fear.

Practical tips

An example that can help you to show your students how an attack of ransomware can affect a company, it is the one shows in the next episode of the Good Wife series:

https://youtu.be/lrXXzWtYkOw

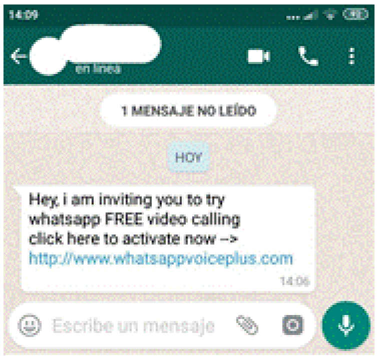
 Map of countries initially affected by the Wanna Cry ransomware attack in May 2017. Source: Wikipedia Commons	 Your personal files are encrypted! Example of message received when a ransomware attack is performed. Source: Flickr

SCAMS EMAIL: SPAM

Scams and scammers have always existed, but the Internet makes it easier for any of us to be the target of a crime of this kind and for more people to be reached in less time. It also makes it easier for others to access important information about our lives that will enable them to commit their crimes. So, it is important to be aware that we can become an easy target for attackers who want to make a profit through deception, and to know the most used scams to stay away from them. The techniques scammers use are known as social engineering techniques. The most useful strategy to avoid them is security awareness, although there exists tools and services schools should apply to reduce the number of messages of this type that they receive. In this lesson, we will focus on the measures that we as teachers can do and teach our students to avoid these threats.

Spams are unsolicited messages over the internet sent with purposes of advertising, phishing, spreading malware, etc. Studies show that at least 80% of the emails we receive is spam. That is a serious difficulty for Internet providers, and for us as users since we waste a lot of time on checking the emails. But, moreover, spam can cause more serious problems. Spam emails can be used as a medium to collect legitimate email addresses as a first step to perform subsequent and more dangerous attacks (phishing, malware, etc.).

Other medium to spreading the spam are instant messaging apps such as WhatsApp or Telegram. Spammers have found another easy way to spread the spam among young through WhatsApp. Some with the only objective of bother the communications, another with more harmful reasons, such as calling or video calling through WhatsApp (with the consequent loss of money) or giving a URL of a malicious website.



1 MENSAJE NO LEÍDO

HOY

Hey, i am inviting you to try
whatsapp FREE video calling
click here to activate now -->
http://www.whatsappvoiceplus.com
14:06

The popularity of social networking, it is making harder to distinguish between legitimate and fraudulent email. Spammers can extract private details from social networks of their targets and cause greater harm to them. Therefore, spams are becoming more and more sophisticated.

PROTECTING YOURSELF AGAINST SPAM

Let’s see some basic hygiene measures to protect ourselves against spam, and also teach our students how to keep protected:

1. Be discreet. One of the basic rules of security and privacy is not give more information than it is strictly necessary, this also applies to email:
    - Do not disclose your email in social networks, websites/blogs, registration forms, surveys, chat rooms, forums, etc. If needed, use the practice known as **address munging**: transform your email address so that it cannot be recognized by bots. For example, from example@domain.com to: example at domain dot com. Another option is to replace the text by an image of your email, but it is less useful for others, since they cannot copy-paste your email. Of course, this apply to your phone number too.
    - When subscribing to free services, check the privacy policy to know what they claim they can do with your personal data.
    - And when sending an email to a number of recipient who do not know each other, use the field “bcc:” to keep the emails account privates.
2. Use separate email accounts for different purposes. For example, do not give your main email account when registering in free services or forums, instead use a separate email account. Many email providers allow to create **disposable email addresses** which you can manually disable or that expire after a time interval.

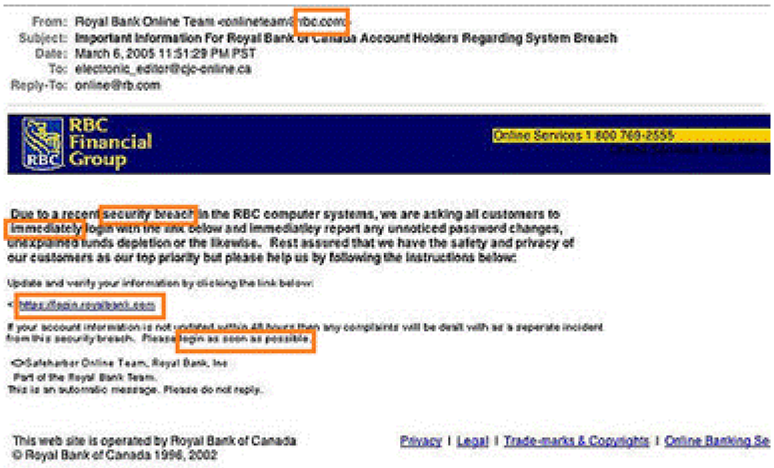
3. Disable HTML email, or configure your email to avoid automatically display HTML or download images and attachments.
4. Do not open attachments from unknown senders, and be aware that spammer usually try to attract your attention with incredible offers or even miracles. Remember do not click the links because they are trying to confirm your email account or trick you.
5. Configure the **anti-spam filters** of your email software, and keep update your antivirus, installed the latest security patches of your system and applications, and activate your personal firewall. When identifying a spam email, block it as spam, so it is added to your blacklist. The same applies for your instant message services (both WhatsApp and Telegram include way to block contacts identified as spammers).

Source: Flickr

SCAMS EMAIL: PHISHING

Phishing emails is one of the most used by scammers, and although they are older than others, phishing scams continue to evolve and are increasingly sophisticated and difficult to detect. The main objective of phishing the email is to get money from the victim by deceiving them through an email in which they usually impersonate a third party (bank, insurance company, betting house, social network representatives, work departments, etc.) requesting sensitive personal information (bank accounts, users and passwords, etc.). They can't only withdraw money, but also steal your identity, make purchases, even trade the steal information to others.

Let's see an example of phishing email that can be used to teach our students to be careful with these types of attacks. Look the pictures below. Figure 1 shows an example of phishing email. We have framed in orange the important data to observe. Note the sender mail domain (what appears after the @) is rbc.com. A quick search in one of the Internet search engines (Google, Bing, etc.) will show that the domain of the Royal bank is rbcroyalbank.com (https://www.rbcroyalbank.com). That's a first warning signal. In addition, we are urged to do something through different messages: “security breach”, “immediately login”, “login as soon as possible”. In this way, they want us to worry and do what they ask us to do without thinking too much. Finally, they give us a website access. If we access using the URL given in the email, a web page will be opened whose address (in the address bar of the browser) does not match the one that appears in the email. What is more, if we try to access it without using the link given in the email (this is an important tip), we will see that the URL does not exist.



From: Royal Bank Online Team <onlineteam@rbc.com>
Subject: Important Information For Royal Bank of Canada Account Holders Regarding System Breach
Date: March 6, 2005 11:51:29 PM PST
To: electronic_editor@cjc-online.ca
Reply-To: online@rb.com

Due to a recent security breach in the RBC computer systems, we are asking all customers to immediately login with the link below and immediatley report any unnoticed password changes, unexplained funds depletion or the likewise. Rest assured that we have the safety and privacy of our customers as our top priority but please help us by following the instructions below:

Update and verify your information by clicking the link below:

<https://login.royalbank.com

If your account information is not updated within 48 hours then any complaints will be dealt with as a seperate incident from this security breach. Please login as soon as possible.

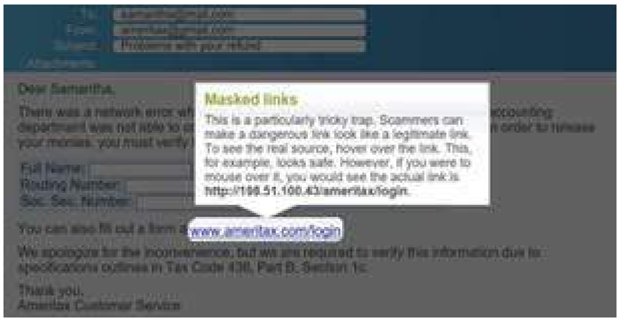
©Safeharbor Online Team, Royal Bank, Inc
Part of the Royal Bank Team.
This is an automatic message. Please do not reply.

This web site is operated by Royal Bank of Canada
© Royal Bank of Canada 1996, 2002

Privacy | Legal | Trade-marks & Copyrights | Online Banking Se

Figure 1. Example of phishing scam by email. Source: Flickr.com

Be careful because sometimes scammers mask a malicious URL into another that looks legitimate:



To: samantha@mail.com
From: ameritax@mail.com
Subject: Problems with your refund
Attachments:

Dear Samantha,

There was a network error wh [illegible] accounting department was not able to [illegible] in order to release your monies, you must verify [illegible]

Full Name:
Routing Number:
Soc. Sec. Number:

You can also fill out a form at www.ameritax.com/login

We apologize for the inconvenience, but we are required to verify this information due to specifications outlined in Tax Code 436, Part B, Section 1c.

Thank you,
Ameritax Customer Service

Masked links

This is a particularly tricky trap. Scammers can make a dangerous link look like a legitimate link. To see the real source, hover over the link. This, for example, looks safe. However, if you were to mouse over it, you would see the actual link is http://198.51.100.43/ameritax/login.

Figure 2. Masked links

DETECTING AND AVOIDING PHISHING

It is very important to teach our students how to protect themselves against scams email. Apart from the measures to avoid spams, let see some characteristics more specific of phishing emails:

1. Sender’s email address unknown
2. They ask for sending or verifying personal information via email.
3. They urged you to do something or send offers that expire immediately, gift deals or coupons, etc., or claim that they are from a law enforcement agency or that there was some kind of problem with your bank account, or a recent purchase or delivery, etc., and ask you to resend or call to a number and give personal information. Remember that neither your bank, nor any reliable service, will ask for personal information such as passwords through email.
4. Beware of misleading links. Sometimes the URL looks invalid at first glance, but others not. Hover your mouse over the links in the email to check them, before access to the link. Some phishing scams use Java to change the link when you hover over it with your mouse. So, you will need to access to the service through their website without using the link of the email (type the address into a separate browser window, never use the link provided in the email). Another option is to configure e-mail as plain text to prevent code from being executed (recommended for security reasons).
5. Let’s assume that you clicked on a link from a suspicious email, check carefully the domain in the web address bar of the browser. Note that this action is dangerous since the website can be malicious and infect you with malware.
6. Check if the mail has attachments. Phishing scams many times hide malware. Never open any attachment, it could be malware.

There are tools to help us protect ourselves from phishing. One of them are browsers that include phishing protection. There are also browser add-ons and extensions to block phishing attempts. In addition, most of antivirus include protection against phishing too.

CONGRATUALTIONS!!!!
According to our raffle, you have been
Caribbean!
All we need from you is your name,
congrats and thank you for your

Source: U.S. Air Force photo by Senior Airman William Tracy (https://www.schriever.af.mil)

Practical tips

Learning activity to use in the classroom with our students:

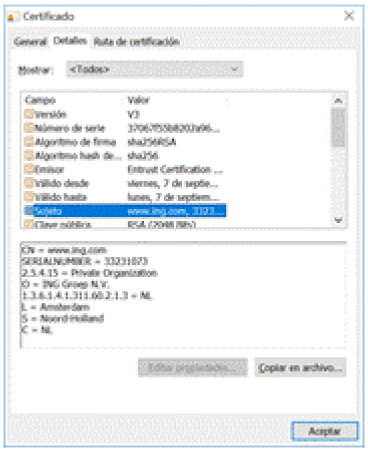
Learning by doing is one of the best methods to teach your students these concepts. You can build your own emails (some fraudulent, some not) and send them to your students. Then, you can propose an activity to them consisting of finding out which of them are fraudulent and which not and why. After a while and without notice, you can send messages from time to time, challenging your students. You can create a file containing something like "I got you!" on Google drive (or any other cloud provider) by shortening the link and using it as a hidden link in your fraudulent emails. To hide the sender field of the email you can create aliases in your email account (most providers like Gmail or Yahoo allow it) and send it from them.

SECURE ACCESS TO WEBSITES

It is increasingly common to make arrangements through the Internet: online purchases, travel bookings, banking, working from home, etc. so it is important to protect our personal information against cybercriminals. In addition to phishing, online shoppers are vulnerable to other attacks such as fraudulent websites or Man-in-the-Middle attacks.

You have to be careful with who you trust your personal data, but how do you know if a website is legitimate before deliver them your data? Let’s see some tips to find out if a site is legitimate:

1. **SSL certificate**: If a website is asking you for some personal data, the URL should start by https (instead of HTTP) and, therefore, the site is secured by using a SSL certificate. That means that your data will travel encrypted and protected against Man-in-the-Middle attacks, for example. To get a SSL certificate the company must pass a validation process, but there are different levels of validation:
    - Domain Validated certificates (DV). DV are validated against domain registry only, so no identifying organizational information is validated. You cannot trust this kind of certificate because it is not possible to know if the business is legitimate. In the details of the certificate (click on the padlock to know the value of each field of the certificate) the field subject will only show the domain (CN = www.domain.com), no data about the organization will appear that enable you to identify the business
    - Organization Validated certificate (OV). OV are trusted because organizations are identified by real agents against business registry databases property of the governments. Details of the certificate will show the name of the organization and other details as address, city and country.
    - Extended Validation certificates (EV).EV are the maximum level of authentication. The details of the certificate show more data such as the serial number and type of organization.



Campo	Valor
Versión	V3
Número de serie	37067f55b8202a96...
Algoritmo de firma	sha256RSA
Algoritmo hash de...	sha256
Emisor	Entrust Certification ...
Válido desde	viernes, 7 de septie...
Válido hasta	lunes, 7 de septiem...
Sujeto	www.ing.com, 3323...
Clave pública	RSA (2048 Bits)

```
CN = www.ing.com
SERIALNUMBER = 33231073
2.5.4.15 = Private Organization
O = ING Groep N.V.
1.3.6.1.4.1.311.60.2.1.3 = NL
L = Amsterdam
S = Noord-Holland
C = NL
```

It is important that our students can identify the level of security that a SSL certificate can provide when they make online transaction sending sensitive information through Internet.

2. Check for a **website privacy policy** and contact information. Privacy laws in EU (and also in countries as Canada and Australia) require to clearly communicate how user data are collected, used and protected. Any legitimate site will have one, but that is not enough, you need to read the policy carefully before giving your information away. Many websites publishes in their policies that they deliver your data to third parties, and they are legitimate websites and from popular providers. And keep in mind that having a privacy policy and contact information does not mean it is legitimate.
3. Search for a **trust seal**. These badges are obtained from trusted certifying entities (CA) after passing multiple administrative checks with the organization.
4. Even so always be careful with pop-ups, phishing kits that imitate commonly visited sites, malicious ads and search engine warnings. Do not let that keep you from going online! Just have a safe behaviour when you are connected to Internet (see lesson 4 for responsible use of Internet).

PREVENTING MALWARE

Malware comes from “MALicious softWARE” which is software program designed to harm a digital device without the consent of the owner. Among malware we can find viruses, worms, Trojan horses, spyware, botnets, keystroke loggers, dialers, ransomware, …

The best protection is YOU. The antivirus programs, although necessary, are not infallible. They can help you with the malware already identified, but new malware is constantly being developed. The measures to avoid these infections are similar to other risks and threats, i.e. having a safe behaviour of technology. Let us see a Decalogue of best practices to prevent them:

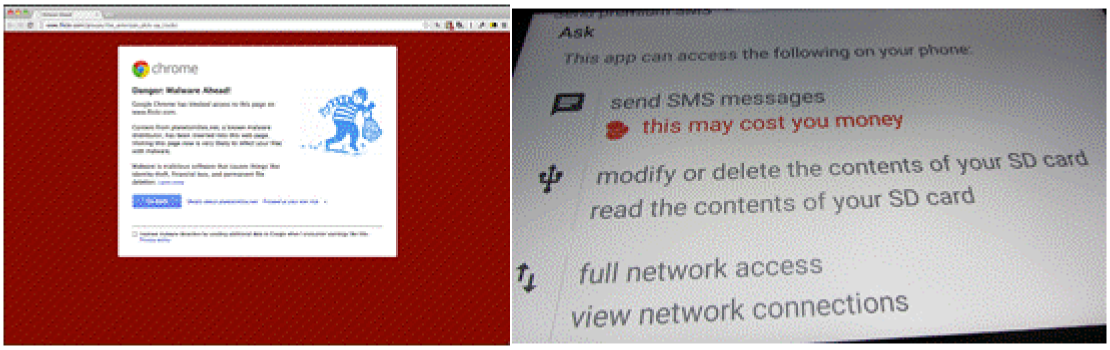
1. Update your software by installing the patches as soon as they are available. Malware, as the worms, exploits software vulnerabilities to infect your data and devices.
2. Use security software such as antivirus and firewalls and keep them active and updated.
3. Do not keep services or apps you do not use in your device, uninstall or shutdown them. Less is more in cybersecurity,
4. Be aware of physical access to your devices: avoid other people to access (physically) to them and use access control measures such as passwords, patterns, fingerprints…Use strong passwords and multi-factor authentication when possible.
5. Do not use an administrator user for performing your regular tasks; malware can take advantage of full access to your digital device.
6. Encrypt and protect with password your sensitive data
7. Perform backups regularly.
8. Be careful with pop-ups and use a pop-up blocker, and above all, be careful to not tell yes when asks you to install unknown software. Also be aware that social network games and applications are another means of malware entry and data theft (they usually ask for more information than required).
9. Do not download and install illegal software, neither software from untrusted websites and be sure that the software you are downloading has been not modified by third parties (a checksum should be provided in the website, so you can calculate the checksum once download the software- there are free programs to do it- and check if it matches.
10. Check that your browser security settings are high enough to detect malicious software.

Source: flickr.com

DETECTING MALWARE

Although there are a lot of different types of malware, they have some common symptoms:

1. Your digital device and/or the Internet connection are slower than usual
2. The operating system or apps crashes regularly. Same with your web browser.
3. Hard disk seems to have a lot of activity when you do not have so many programs (neither an resource-intensive program) running
4. Non-authorized changes in your web browser: homepage, new toolbars, redirection to different websites than the required, usual messages appear,…
5. Strange behaviour of your system: programs that start automatically, antivirus turned off or unable to update, you are blocked when trying to admin your computer (access to Control Panel or Registry Editor, for example), unknown icons on your desktop or unknown files in your computer, unexpected reboots,…



chrome

Danger: Malware Ahead!

Ask

This app can access the following on your phone:

send SMS messages

this may cost you money

modify or delete the contents of your SD card

read the contents of your SD card

full network access

view network connections

Source: Flickr

REMOVING MALWARE

And, what happens if still you are infected? The best is reinstall your operating system and recover the last backup. Since that is not always possible, here you have some recommendations:

1. Create a system restore point just in case you need to roll back.
2. Delete temporary files. Both Windows (cleanmgr.exe) and Linux (systemd)
3. Execute a full system scan with your antivirus software (make sure it is updated).
4. If that is not enough, you will need to scan for rootkits using antimalware software. Maybe you will need to scan with several programs. If your antivirus or any of the antimalware programs has identified the name of the malware, you can search in the Internet for specific virus vaccines, i.e., very

small free programs, usually developed by antivirus providers, to remove a specific malware.

5. If you are experiencing problems to install new software, start Windows in "Safe Mode with networking" and try again.

Some malware is very difficult to definitely clean, do you understand now the importance of backup all your important files regularly?

Source: Flickr

SUMMARY

In this lesson, we have learn how to differentiate among the most common threats in digital environments. In addition, we have learnt how to identify a scam email and know what type of scam is through examples. Then, we have reviewed the most important protection measures to avoid spam and phishing.

Later, we have learnt about how to identify a legitimate website from other fraudulent, and how to know if the website is secure before giving our data or buying products.

Finally, we have learnt how to prevent malware, and techniques on detecting and removing if needed.

The most important measure to teach our students here, is that YOU are the most important measure to avoid the risks on digital environments. A safe behaviour in the internet can avoid most of the risks. So we need to be conscious of our decisions when using digital tools, as well as we are when using other type of tools.

BIBLIOGRAPHY

1. The ABCs of detecting and preventing Phishing. Heimdal security. July 25, 2018. https://heimdalsecurity.com/blog/abcs-detecting-preventing-phishing. Retrieved on March, 2019.

2. Security guidelines of CIS <https://www.cisecurity.org/> (Retrieved on March, 2019)

3. General Tips & Advice. Practice good online safety habits with these tips and advice <https://www.stopthinkconnect.org/tips-advice/general-tips-and-advice> (Retrieved on March, 2019)

4. National Cybersecurity Alliance. Stay Safe Online: Spam and Phishing < https://staysafeonline.org/stay-safe-online/online-safety-basics/spam-and-phishing/> (Retrieved on March, 2019)

5. Graham, J., Howard, R., Olson, R. Cyber Security Essentials. CRC Press, Taylor & Francis Group. New York. 2011.

LESSON 1.3 - PROTECTING DIGITAL CONTENT

PRESENTATION

In our learning to protect our digital assets, we have identified and studied the different threats that we can find in the different “daily use services”. For example: public WiFi hotspots, mail, chats…

In this lesson it’s time to protect digital content from direct intrusions, destruction and theft of physical media that store it.

First, we will begin remembering the most usual storage spaces of the information, understanding what differences exist saving the information in one place or another, and maintaining the integrity of our data.

SAFELY STORING OUR DIGITAL CONTENT

We are going to list a series of supports for our data:

- Notebook
- Optical discs (CD, DVD, BluRay, HD-DVD, ...)
- Flash Memories (Pendrives, SD cards, ...)
- Magnetic hard drives
- Solid-state hard drives
- Remote servers
- Space in cloud

Supports of data

Most will sound familiar to us. Very often we are saving, moving and transferring information with these supports. We do it daily, but without being fully aware of the limitations of them.

Given the following question: “Would we leave our information located in a single and unique support (for example: a pendrive)?”

It seems reasonable to answer NO. This is because we know that something as practical as a pendrive can be lost, broken, corrupted, stolen or become obsolete. Nevertheless, many times we do not have the habit of keeping the information in several places or having a way to recover it in case of losing it.

Then,

“What is the best data storage strategy?”

ENCRYPTION OF DATA ON DEVICES AND PASSWORD PROTECTION

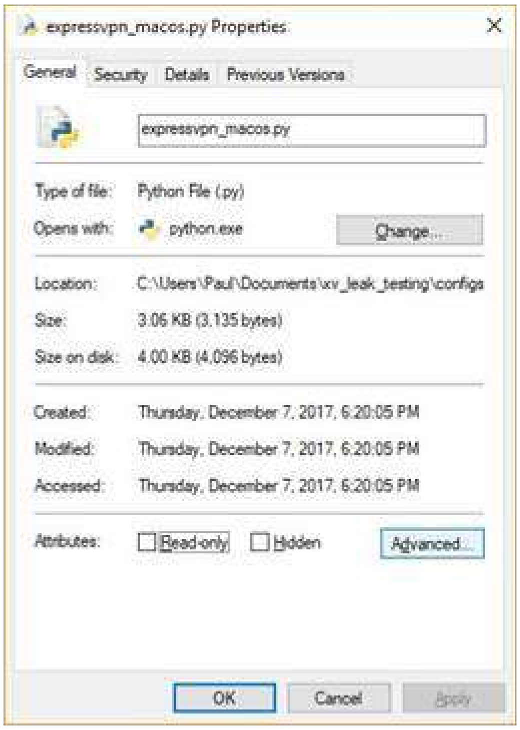
As a first level of security, many discs and flash memories incorporate a small software that allows the user to **encrypt** the content of the hardware and make it accessible through an **internal file manager.** We can protect this file manager by password too.
We can see the usefulness of encryption easily. If our device is stolen, the information can not be accessed. That is because the disposition of the physical information can not be interpreted by the operating system, unless it has not been decrypted before by the internal manager of our device.
Even so, the security of our information can not depend solely on this.

In addition to file managers, we have tools of the operating system that can act on files and folders to encrypt them.

The main procedure to encrypt files and folders by OS:

WINDOWS

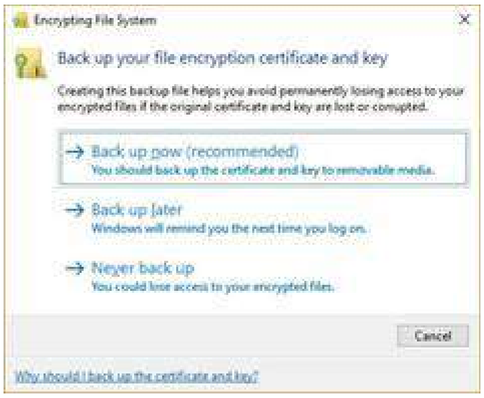
1. In Windows Explorer, right-click on the file or folder you wish to encrypt.
2. From the context-menu, select Properties.



expressvpn_macos.py

Type of file: Python File (.py)
Opens with: python.exe
Location: C:\Users\Paul\Documents\xv_leak_testing\configs
Size: 3.06 KB (3,135 bytes)
Size on disk: 4.00 KB (4,096 bytes)
Created: Thursday, December 7, 2017, 6:20:05 PM
Modified: Thursday, December 7, 2017, 6:20:05 PM
Accessed: Thursday, December 7, 2017, 6:20:05 PM
Attributes: □ Read-only □ Hidden

3. Click on the Advanced button at the bottom of the dialogue box.
4. In the Advanced Attributes dialogue box, under Compress or Encrypt Attributes, check Encrypt contents to secure data.
5. Click OK.
6. Click Apply.
7. If you selected a folder to encrypt, a Confirm Attribute Change dialogue box will be displayed asking if you want to encrypt everything in the folder. Select Apply change to this folder only or Apply changes to this folder, subfolders and files, and click OK.
8. Click on the Back up your file encryption key pop-up message. If the message disappears before you can click it, you can find it in the Notification Area for your OS.
9. Ensure you have a USB flash drive plugged into your PC.
10. Click Back up now (recommended).



Encrypting File System

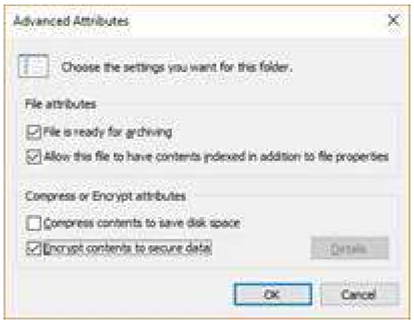
Back up your file encryption certificate and key

Creating this backup file helps you avoid permanently losing access to your encrypted files if the original certificate and key are lost or corrupted.

→ Back up now (recommended)
You should back up the certificate and key to removable media.

→ Back up later
Windows will remind you the next time you log on.

→ Never back up
You could lose access to your encrypted files.



Advanced Attributes

Choose the settings you want for this folder.

File attributes

☑ File is ready for archiving

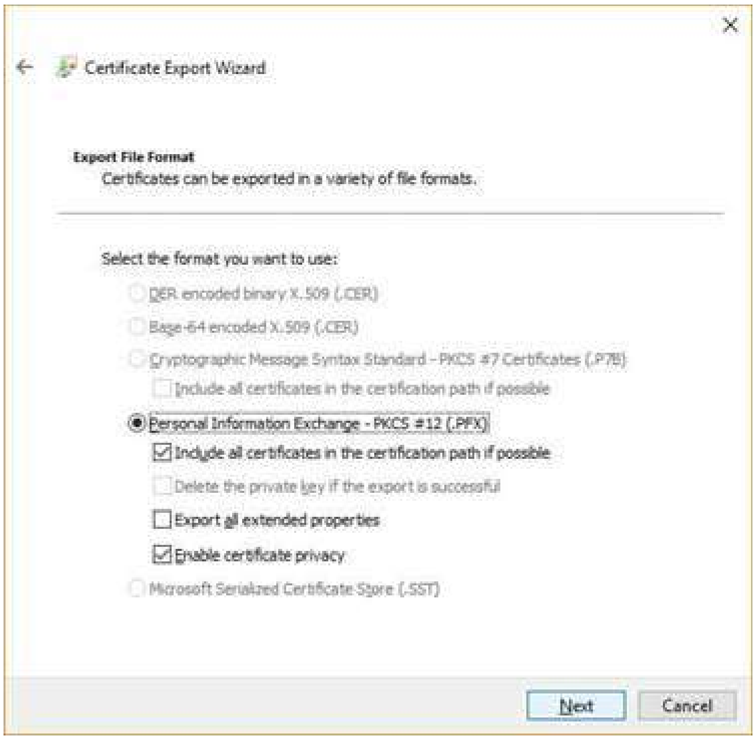
☑ Allow this file to have contents indexed in addition to file properties

Compress or Encrypt attributes

☐ Compress contents to save disk space

☑ Encrypt contents to secure data

11. Click Next to continue.
12. Click Next to create your certificate.
13. Accept the default file format to export and click Next.



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

☐ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

☐ Delete the private key if the export is successful

☐ Export all extended properties

☑ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

14. Check the Password: box, enter your password twice, and click Next.
15. Navigate to your USB drive, type a name for the certificate and key you want to export, and click Save. The file will be saved with a .pfx extension.
16. Click Next, Finish, and then OK.
17. Eject your USB drive and put it somewhere safe.

To decrypt a file or folder, follow the first six steps above, but uncheck the Encrypt contents to secure data box in Step 4.

MAC/OS-X

1. Open Disk Utility (go to Finder > Applications > Utilities folder).
2. Once there, go to the File and choose New > "Disk Image from Folder..." (or type shift-command-N).
3. Select the folder you want to encrypt, and then click Image.
4. Now, pick your encryption method and click Save.
5. You'll be prompted to enter a password for your new encrypted disk image, type in any password you want (just make sure it's secure!).

Should we add anything else?

We have seen that we have remote servers and free space in the cloud to also store the information. Places where our data can also rest and be encrypted, but its use also requires a series of habits so that our information remains safe.
Let us first explain the difference between **local storage** and **cloud storage**.

DIFFERENCE BETWEEN LOCAL STORAGE AND CLOUD STORAGE

We refer to **local storage** when *the hardware where our information is stored is accessible by us directly*.
Cloud storage occurs when *we send our data to a physical medium outside of our direct reach*, but accessible by programs, apps or web clients.

Managed physical place where our data can be stored in the cloud. Source: PIXNIO

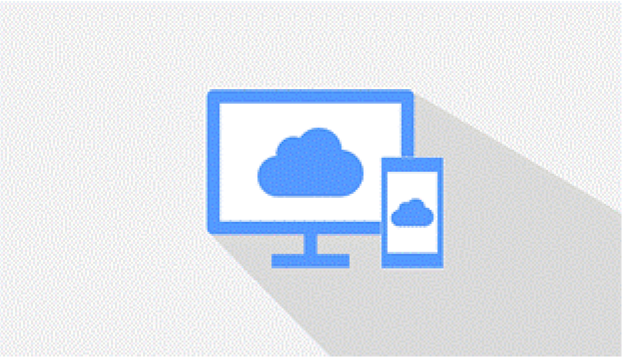
So, the cloud is actually a collection of real storage spaces well organized (remote hard drives, servers ...) and managed by an entity outside of us. For the user, it is a virtual space that is accessed through the internet in which documents and computer programs are stored so that other users connected to the same network can access them and use them.

In these spaces (server farms, set of disks ...) our information is physically present, and even we have full access to the management of it, we do not have to worry about the state or the management of that physical space where it is located.
Now we ask, are all the companies that offer cloud spaces equally safe and reliable?
Obviously, this will interest us a lot. At least they are expected to guarantee the integrity and access to the data we upload there.

WHAT DOES IT MEAN TO BE SYNCHRONIZED?

This expression is heard and read a lot. Our tablets, smartphones and devices often ask questions of the same kind:

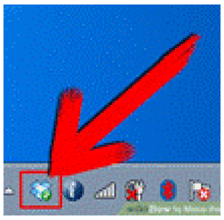
"Do you want to synchronize your files?"
"Do you want to synchronize your work with our servers?"



The act of **being synchronized** means that *the files we manipulate in our local devices keep the same status and versions as the one found in the cloud storage space*. Synchronization gives us the advantage offered by having data at the local level (quick access, no lag…) with the security of having a backup in the cloud. Usually, cloud service providers usually have a catalog full of applications that help keep our data synchronized.

What we need to be synchronized?

Every local environment involved in synchronization has an app -or desktop app- to keep this state between files in local and cloud levels. Those apps must be installed in our OS in order to keep synchronization. Nevertheless, It is necessary to check by ourselves that the files are correctly synchronized paying attention to its icons below (arrows, checks…) and the application is in a stable state.



Desktop apps like One Drive and Google Drive or Dropbox can show us those states. We only need to check the icons in our taskbars where these services are running, and specifically those most valued files in our system.

Source: TICbeat

Now is time to ask ourselves where are the limits of all these services. Generally, providers don't asure a copy of your data in cloud storages because those services are usually paid. If our centers have a contract with a cloud storage provider, we can be assured.

They use data mirroring methods and redundant hosts along geographically separated storages. When some of these nodes gets down, providers can resorte our data from other nodes.

If we have not ordered any of these services, we may use a local backup system.

BACKUP POLICY

Every center needs a system to keep data safe, but also needs to have some method in case there is a serious loss of data.

There are different types of backups and it is convenient to know which kind of them is the best for us.

In general, there are 4 different types of backups:

- **Full backup**: as the name suggests, this type of backup makes a full backup of all files of our unit/drive.
  The backup covers 100% of the information, which usually requires more time to complete and takes up more space.
  If you are sure you want to protect everything, it is the best solution.
- **Differential backup**: only contains the files that have changed since the last time the copy was made. Therefore, only new and / or modified files are included.
- **Incremental backup**: a copy is made of all the files that have been modified since the last complete, differential or incremental backup was executed.
  It is the fastest method to make backup copies.

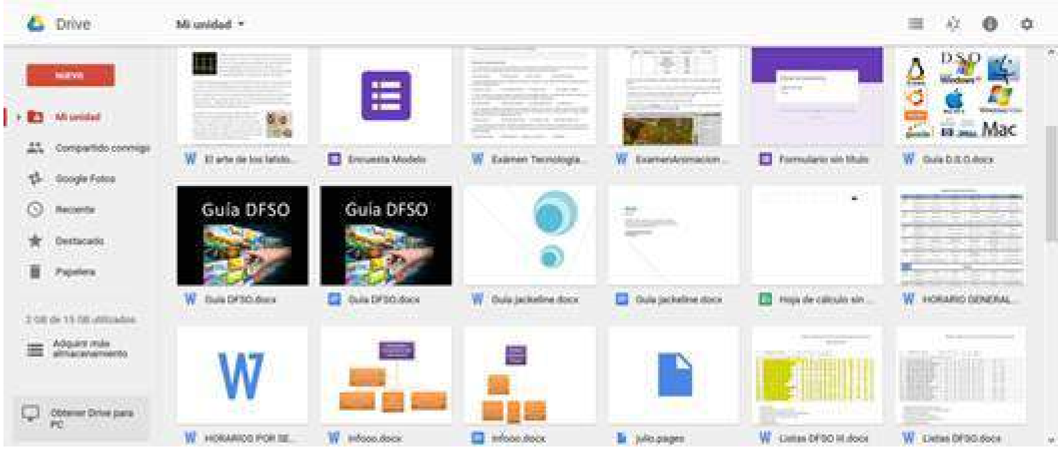
- **Mirror backup**: similar to the full copy.
  The difference is that the files are not compressed and can not be protected using a password.
  Therefore it occupies more space and is less secure.

Source: FLICKR

USING AND CONFIGURING CLOUD

Regardless of the cloud service that we use (Google Drive, One Drive, DropBox, iCloud, Amazon Home Drive, ...), they all start from the same list of options for management and configuration.

First, we may **bind a mail account** to the desired cloud service. From there, we will have password-protected access to the cloud or a two-step challenge to access. This space is equivalent to a root folder where we can build our directory tree and store the files we want within the space limits offered by the service provider. In general, a free initial amount is available, which can be extended depending on the provider and his ordered service pack.



Google Drive user interface to manage files and folders in the cloud.

The main options are usually similar to those on a File Manager for desktop computers, mobile devices or tablets:

- Creation of online collaboration files (Documents, Spreadsheets, Presentations, Drawings, Forms ...)
- Creating folders
- Upload of existing files or folders from local storages
- Copy and move files and / or folders
- Deleting files and / or folders
- Managing the folder tree and its organization
- Querying information about files and / or folders
- File version management

They also include options related to file sharing and real-time working on them, and information of users who have interacted with each item saved:

- Management of file and / or folder permissions
- Privilege configuration and users interaction on files and / or folders (visualization, comment and creation).

We also have the security management of the account, where we can set individual login options and choose the challenge option to authenticate.

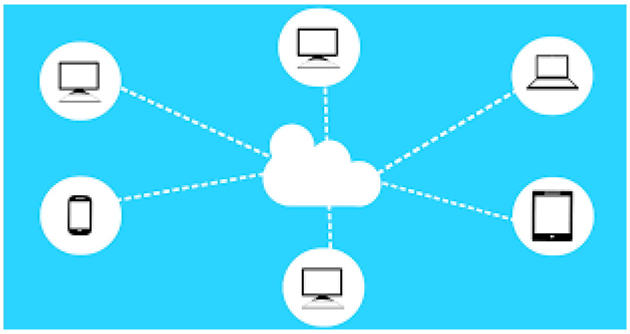
And do not forget: **in case of logging in with an account that provides access to a space in the cloud, we must always close the session when we finish using it** , especially if we have made such a session in a device or equipment for public use. <u>Our students need to know this, not only in order to prevent information theft but also to prevent any type of cyberbullying by identity theft.</u>

CLOUD COMPUTING: USE OF THIRD-PARTY SERVICES

When you store your data in an external provider either because you use cloud services, rent servers or external services (hosting, housing, Software as a Service -

SaaS. etc.) you are exposed to different risks such as: lack of control over your data, data breaches, lost or theft of intellectual property, compromised credentials or account hijacking, compliance violation or social engineering attacks. In short, greater risks because the data are stored in a third-party and probably accessed through to a public network which makes them more susceptible to attacks.

However, the use of cloud computing provides many advantages. It allows us to access our data from different devices, for example, and that organizations can hire services (SaaS) without having their own datacenter with all that this entails.



Source: Pixabay

So, how can we protect ourselves from these risks? You should carefully read the privacy policies of the providers. For example, we must pay attention to whether we are giving our consent for our information (or part of it) to be disclosed to third parties (data leakage). Furthermore, in order not to depend on the security policies of third parties, it is advisable to have the data stored in the cloud encrypted and, above all, not to store confidential or sensitive information on the network. Confidential information such as banking, health, etc. should be stored on external disks that are not normally connected to the network. In addition, multifactor authentication and implement one-time passwords is recommendable. Compliance violations and loss or theft of intellectual property should be minimized by due diligence, policies and agreement responsibilities with the provider.

You will be exposed to similar risks when you connect to public or open Wi-Fi networks where information is transmitted over the network without being encrypted and can therefore be captured and read, even modified, by a third party. **Public Wi-Fi** although convenient, often are not secure (not require WPA2 password). When using wireless hotspots, avoid use apps or websites requesting personal or financial data, and send data only when the websites are fully encrypted (https). If you often use unsecured Wi-Fi, use VPN (Virtual Private Networks) to connect them. And turn off Bluetooth when not in use!

© flick.com

SUMMARY

We should remember the following points in this lesson:

- We may know about every data storage device available, including: average life span expectancy, strength and size.
- Offers and differences between local storage and cloud storage.
- How to use encryption manager software to protect our data.
- Synchronization and what it takes.
- Use and configuration of cloud environments.

REFERENCES

- COMPARITECH - How to encrypt files in Windows 10, 8 and 7 https://www.comparitech.com/blog/vpn-privacy/encrypt-windows-files/
- INTEGO - How to encrypt files https://www.intego.com/mac-security-blog/how-to-use-apples-built-in-features-to-encrypt-files-and-folders/
- Internet Lab - Tipos de copia de seguridad https://www.internetlab.es/post/2104/tipos-de-copias-de-seguridad/
- ¿Qué es la informática en la nube? - https://azure.microsoft.com/es-es/overview/what-is-cloud-computing/
- Los soportes de información (INCIBE) - https://www.incibe.es/extfrontinteco/img/File/empresas/kit_concienciacion/Pildoras_informativas/incibepresentacin_2__los_soportes__texto.pdf
- Diccionario de la Real Academia Española

LESSON 1.4 - RESPONSIBLE USE OF TECHNOLOGY

INTRODUCTION

Source: https://www.publicdomainpictures.ne

It is just as important to know how to use technology responsibly as it is to encourage our students to develop healthy and responsible habits in the face of mass media.

In this lesson we will review some of the risks associated with the use of technological resources that we face as teachers but which our students also face. We will also get to know some didactic guidelines and we will be able to review useful materials to integrate into the classroom.

The learning goals to be developed in this lesson are:

- To list some positive uses of technology and how it affects our daily lives
- To prevent risks and to promote the responsible use of technologies among young people
- To help students' parents to encourage the responsible use of technology
- To Identify incident reporting mechanisms
- To Know how to create an "Acceptable Use Policy" (AUP) and how to guide others to apply it.

THE IMPACT OF TECHNOLOGY ON OUR LIVES

The technology has undergone rapid worldwide extension in a totalizing manner covering all aspects of everyday life. It has even become an element that serves social integration while generating just the opposite, since those who do not have access or knowledge to make use of technologies not only stay away from the flows of information and participation, but also become invisible to those who are integrated into the new technological order of reality. This is the origin of the so-called "digital divide", a term coined by Morrisett (Hoffman et al, 2001).

Source: www.Pixabay.com

Technologies have profoundly transformed economies, markets, jobs and their impact is greater, according to Druker (1969), in society and politics, as well as the way we see the world and ourselves. This is because the use of digital technologies has been progressively integrated into all sectors of society, transforming the way we trade, learn, teach and communicate. As Marí (1999, p.14) said, "the novelty lies in the totalizing character of the technological revolution: it reaches all dimensions of life and global society".

However, for Lévy and Medina (2011) society and technology cannot be understood as differentiated entities since technology is a social and cultural product. According to this conception, technology does not generate an effect or impact on society, but develops indissolubly together. If we start from the premise that technology is a human creation and one of the essences of our nature is the need to establish links and form part of social groups, what else could the Internet be used for?

But the truth is that technological development, especially in the field of the Internet, has been developing hand in hand with a social and cultural transformation that has led to the so-called "cyberculture" (Lévy, 2011). Cyberculture is defined by the interconnection between people, the creation of communities and the development of distributed collective intelligence:

- Interconnectedness favours the sense of living in the "global village" Marshall Mac Luhan spoke of in the 1960s.

- The second principle, the creation of communities, is a natural extension of interconnectedness. "A virtual community is built on the affinities of interests, of knowledge, by sharing projects, in a process of communication or exchange" (Lévy, 2011, p. 100). These communities make possible new forms of participation in public life and learning.
- Finally, so-called collective intelligence can be understood as the ultimate goal of cyberculture. We can define it as that which arises from the collaboration between many people and which is possible thanks to the advantages of the social Internet or 2.0 which allows the users of the Internet to be in turn those who feed it with content.

Technology is an engine of change, and has made it possible for us to live in the so-called "global village" (MacLuhan, 1968), where physical limits have been reduced, favouring greater mobility of products, services and people. On the other hand, however, it has also made possible the manipulation of information that favours the creation of a conditioned public opinion and generates a unitary consciousness in the countries that have the information monopoly, at the same time as transforming the way people conceive the world and themselves.

In this context defined by network society and cyberculture, technological development and social development interact with each other and revert to a continuous cycle of change and constant development.

RISK PREVENTION AND PROMOTION OF RESPONSIBLE USE OF TECHNOLOGIES AMONG YOUNG PEOPLE

Today's digital society in which virtual and face-to-face environments coexist, it is necessary for citizens to be properly integrated in a responsible and civic way, becoming aware of the opportunities and risks that technology offers. For this reason, the directives at European level (Vuorikari et al. 2016) (European Commission, 2012) emphasise the development of digital competence of citizens and the promotion of responsible use of digital resources.

Source: www.Pixabay.com

But in order to conceive of a competent and responsible digital citizenship it is necessary to start training, as well as the integration of measures to prevent risks arising from the misuse of technology at an early age.

It does not make sense to avoid risks to young people from prohibition or control but from accompaniment and training to promote their autonomy. Adults must accompany and guide children and young people in their digital life, in the education for an adequate use of technologies that goes beyond the knowledge of purely technical aspects and the prevention of online dangers. Therefore, training should not be limited to knowledge of technologies and techniques of online protection, but should extend to the rules of civility and good treatment in the virtual world and emotional education aimed at working assertiveness, empathy and critical thinking.

This is Save the Children's position (2017) on the promotion of responsible digital citizenship, the commitment to prevention and the promotion of responsible use with the necessary advice and guidance from educators and families. Only in this way is it possible to take advantage of the opportunities offered by technology to reduce gaps and offer equal opportunities.

We have already seen in the section dedicated to addiction to technology the description of the levels of prevention that in general could be summarized in two; firstly, the universal level that takes place when minors begin to use technology in primary education, which has as an essential objective the initial training of adults in charge of supervising and accompanying minors in their technological initiation.

Secondly, we are talking about a selective level of prevention aimed at minors already initiated in technologies that begin to make habitual use of them and need to acquire specific strategies that promote responsible use. With this age group and in this type of prevention actions, you are currently working as a teacher. Your students are teenagers who already have mobile devices that are or are beginning to be active on social networks and who are probably beginning to have doubts and some conflicts arising from the use of technologies. Your work as a guide in the development of their competences as responsible and civic digital citizens is essential. That's why you need to keep up to date with the preventive strategies and programs at your fingertips. As well as the resources and materials you can access to work in your school.

More information

Internet Segura for Kids (IS4K) is the Internet Safety Centre for minors in Spain and aims to promote the safe and responsible use of the Internet and new technologies among children and teenagers. IS4K is led and coordinated by SEAD (State Secretariat for Digital Advancement), with the support of Red.es, and executes its services through INCIBE (National Institute of Cybersecurity), in collaboration with other reference entities. In line with the European strategy BIK (Better Internet for Kids), it is part of the pan-European network INSAFE of Internet Security Centres and is co-financed by the European Commission.

THE POLICY OF RESPONSIBLE USE OF TECHNOLOGIES IN AN EDUCATIONAL CENTRE

Educational centres, like any other organisation, are not oblivious to the risks arising from the use of technology. In school contexts, a large amount of personal information is managed and the work is essentially focused on minors, so it is necessary to have a policy of responsible use of technologies at school level. In this policy it is necessary to establish strategies for the prevention and promotion of responsible use but also protocols for action in the event of conflict or improper use by any of the members of the educational community.

This is the equivalent to the security master plan of any company.

Source: www.Pixabay.com

In order to be able to establish the centre's policy, it is necessary:

- Start by defining the current level of information and setting strategic objectives
- Analyse the potential risks to which the school is regularly exposed
- Identify good cybersecurity practices to follow
- Specify the measures to be taken at both the preventive and reactive level in the face of a problem arising from

It is important to bear in mind that the elaboration and application of these regulations must be the result of a coordinated and consensual work among all members of the educational community in order for it to be effectively applied.

In addition to the centre's policy, it is necessary to establish preventive measures of a technical nature, such as:the use of technologies.

- Configuration of the archive of documentation and personal information in compliance with current data protection regulations
- Configuration of the computer equipment that will be used by teachers and students to guarantee its security, using filters and antivirus to avoid information leaks.
- Configuration of the internet connection that can guarantee secure access via wifi network

Practical tips

- Establish a realistic centre policy, agreed by consensus and to which all the agents involved commit themselves.
- Review the centre’s policy on a regular basis to promote its improvement

HOW TO DEVELOP ACTIVITIES WITH STUDENTS TO PROMOTE THE RESPONSIBLE USE OF TECHNOLOGIES?

Whether you like it or not, your students live in a digital society and make daily use of technological resources, share personal information, access another, are active in social networks and make use of different devices for academic and recreational purposes. this is a situation that offers advantages but also risks. Therefore, you have a responsibility as a teacher to encourage responsible use of technologies. Regardless of whether or not you are a technology teacher or the head of technology at the school, it is necessary that you integrate the technologies in your classes following basic pedagogical and technical principles that favour the development of students' digital competence. This necessarily includes the integration of cybersecurity and responsible use strategies.

Source: www.Pixabay.com

At the technical level, throughout this course they are acquiring essential clues about strategies to follow referred to:

- The choice of technological resources and materials to be used
- Data protection
- Information management

At a pedagogical level, specific activities can be developed aimed at understanding the risks and benefits of technologies and how to use them responsibly, but if you do not have time set aside for this purpose, you can integrate responsible use strategies across all activities involving the use of technological resources.

In the didactic resources that you can review below you can see examples of specific activities to be integrated in the secondary classroom to incorporate effective security strategies. You must bear in mind that it is necessary to include in these activities concepts, procedures and attitudes to make it easier for students to act in front of technologies, providing possibilities to create, invent and share in a reflexive way, overcoming the role of mere consumer user. For this purpose, it is recommended to include didactic methodologies based on experiential situations, connected with real life, which, in turn, promote the active construction of knowledge and, therefore, of responses based on the personal and collective analysis and reflection of the students. Let us remember that our intervention takes place in secondary and high school with students who already have a technological background. Taking advantage of it and starting from their experiences will be essential. Some didactic methodologies that can be useful to you are:

- Project-based learning: It is a teaching model based on the use of realistic projects, based on a highly motivating question, task or problem, directly related to a known context, through which students develop competences in a collaborative approach in search of solutions (Bender, 2014).
- Case studies: It consists precisely of providing a series of cases representing various real-life problem situations for study and analysis. The difference with project-based learning is that it provides complete information about the case and guidelines for its solution as opposed to a much more open project-based approach that requires more autonomy on the part of the student body.
- Cooperative learning: The students work together for the fulfilment of a common objective, in a coordinated way based on a distribution of responsibilities and clearly defined interaction guidelines.
- Gamification: It consist of integrating techniques, elements and dynamics of games in non-recreational activities in order to enhance motivation and reinforce behaviour to solve a problem.

Practical tips

- incorporates regularly activities in which students must search for and filter information
- Develops students' critical thinking through activities that encourage reflection and dialogue about the digital content they access.

HOW CAN WE HELP STUDENTS' PARENTS TO ENCOURAGE THE RESPONSIBLE USE OF TECHNOLOGY?

The role of families is essential in introducing digital society and promoting responsible use of technology. From a very early age, children coexist with different technological resources, but they need the support and accompaniment of their families in order to develop their autonomy and critical thinking. Because of their characteristics; their curiosity, excessive confidence and desire to experiment often underestimate the risks they may also face. That is why some of the aspects that most concern parents are:

- The age of access to different resources such as mobile phones, internet browsing or social networks.
- The necessary guidelines to offer their children to make good use of the resources at their disposal...
- A healthy balance between technological and analogical activities to avoid possible addiction problems.
- The effects that the use of technology can have on their academic performance or cognitive functions, such as concentration, decision-making or psychomotor skills.

As teachers, our role in supporting families can be very valuable and, as in any educational act, coordinated action between school and family is a guarantee of success. To this end, different ways of coordination between teachers and families are offered to promote the responsible and ethical use of children's technology:

- Keep a fluid and reciprocal communication between the teaching team and the families in order to be able to monitor the modification of behaviours that could be a sign of a problem due to a misuse of technology. This communication can be promoted through technological resources such as mobile applications. In any case this communication should not be understood as a control over the student, communication with the students is also essential but must be complemented with coordination with families.
- The development of informative and/or formative activities in the educational centre about the promotion of the responsible use of technology outside the school, aimed both at minors and their parents, who should serve as a reference figure.
- Provide guidance information to parents that can help them make decisions and establish guidelines for good technological use at home as guides, infographics, Decalogue or models of family contracts such as the one shown in the image above. It is important to consider the format of these documents so that they are easy to read and useful, trying to favour conciliation as far as possible. If we provide documents that are too broad or with very technical language, we will not promote their reading.
- Acting in a coordinated way when faced with a problem of misuse by their children, acting individually with a conciliatory and resolving attitude.

Practical tips

- **Talk to parents to reinforce behaviours.** Do not limit communications with the family to problematic or negative situations; it is recommended that you also highlight the positive aspects or improvements that the student has experienced.

- **Listen to the parents.** They know their son, his particularities and his reactions when he arrives home after school. Advise them tactfully, but always listen first. Consider them your allies and make them see that they are an essential part of your child's education.
- **Personalize meetings and communications.** Be concrete and be prepared before meeting or sending an information note to give parents as much information as possible about their child, their difficulties and personal strengths.
- **Give clear directions with simplicity and closeness.** Heed all their questions and try to make the talk as didactic as possible so that parents know how to act to solve the problems their child may face.

POSITIVE USES OF TECHNOLOGY I

Returning to the beginning of the lesson, and after knowing some risks of an irresponsible use of technologies, it is also important to highlight some positive uses of technologies. Once we are clear on how to encourage responsible use of these technologies by students, we will be able to take advantage of all their educational and social advantages as teachers:

- The times when students had to research with the only help of school library resources or the nearest public library is over. They are no longer conditioned by the amount of accessible information, but have an environment that contains all the information they need. All they need is connection and adequate information skills to know where to locate the information and filter it properly. This is something we take for granted, but it has really been a tremendous transformation and it has happened very quickly. As teachers we can take advantage of this in a number of ways:
    - Asking students to do work in which they must research, search, filter, and rework information in different languages. This will allow us to develop their digital competence and basic communication and teamwork skills, as well as their critical thinking and creativity.
    - We can also transform the information obtained into non-technological formats and ask them to make artistic elaborations using plastic elements such as painting, collage, sculpture or other techniques of expression.
- With the development of the web 2.0 Internet not only became a great library but also allowed to give voice to Internet users. In this way we have stopped being passive subjects in front of information. Our students have a loudspeaker at their fingertips to share their ideas, projects and work. The generation of shared knowledge is undoubtedly a magnificent advantage that in the hands of teachers is a leap in the way we relate to information. Some of the educational possibilities offered by this technology are:
    - Generate a web space fed by students about a specific topic
    - Conduct a research paper and try to get it published on Wikipedia
    - Initiate an online project in which students act as community managers, promoting the dissemination of valuable information.

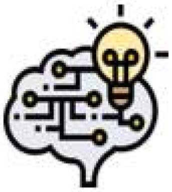
POSITIVE USES OF TECHNOLOGY II

Let’s see some more positive uses:

- The expansion of mobile technology has made it possible to have immediate access quickly and conveniently and has increased our potential for socialization and communication. Through social networks we can communicate anytime and anywhere with other people, share ideas, and concerns. Response times have been drastically reduced and it is no longer necessary to wait to be able to communicate with someone, confirm an information or agree to meet in person. This allows us some interesting uses at an educational level:
  - Ask students to interview experts on a particular topic. To do this, you will have to search for these experts on the net, communicate with them and request their collaboration in order to interview them in person or online.
  - Initiate a dynamic communication with students through social networks such as Twitter to encourage their curiosity and inquiry into the matter.

- Technologies are also a space for fun. Their interactive and playful component makes them attractive to students. Knowing and using tools that capture their attention and interest is of great help to promote their motivation. The key is to know how to take advantage of them for the benefit of the learning and teaching process. Here are some ideas to do it:
  - Gamify! Integrate game dynamics using technological resources. You have an example in https://zombiologia.com , a gamification project in biology that has turned out to be a success.
  - You can use video games as didactic tools, for example the educational version of Minecraft allows to learn contents of sciences and humanities.

Take advantage of all the good that the technologies offer you in benefit of the learning and integral development of your students. Well used only offer advantages that will be very useful to you and them.

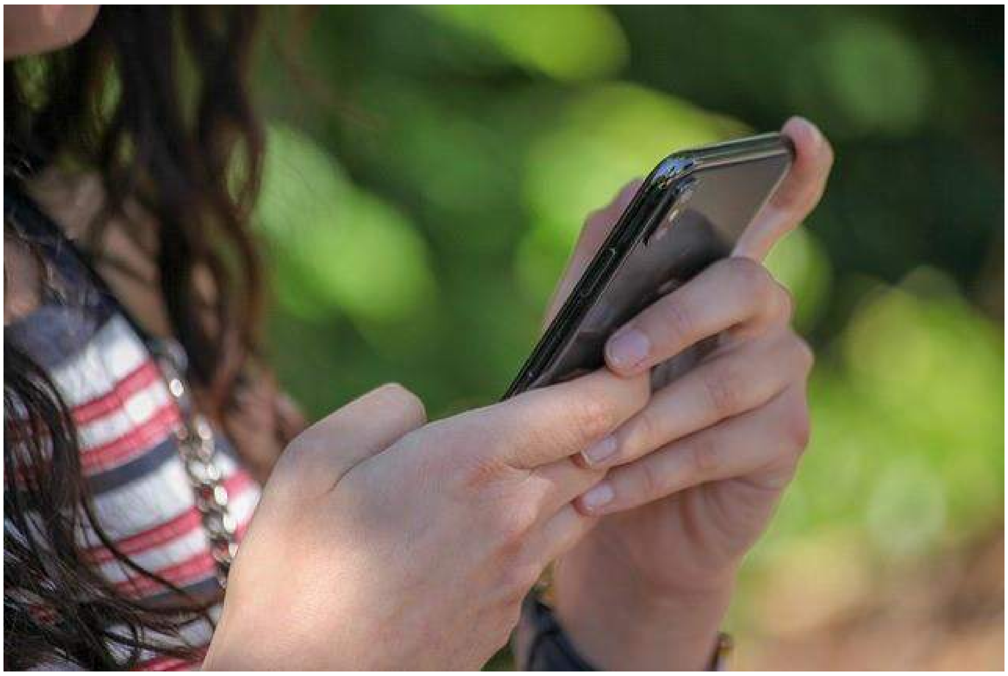


Practical tips

- Get to know your students and their habits in the face of technology. Knowing what apps they use and how they do it, knowing their interests will be of great help to schedule your classes connecting with their concerns and ways of having fun.

- Awaken your creativity and critical thinking so that your students can do it too. Think big, document, plan and harness technologies at your fingertips.
- When you ask students to make some personal elaboration from information obtained on the Internet, don't forget:
    - Give them guidelines about the conditions that the analysed information should meet, especially if they are still developing their informational competence.
    - Make clear the purpose of the exercise, the work process and how it will be evaluated. If when you deliver the work you do not meet the minimum quality standards that you expected, check if it is something generalized, then you must adapt the guidelines that you offer them.
    - Offer elaboration options so as not to condition their creativity.
    - Track the process to guide them when necessary and help them solve problems.
    - Be fair by valuing the process as a whole and not just the outcome.
    - Have them share their work to give it visibility and encourage their sense of responsibility in the work.

SUMMARY



Source: www.Pixabay.com

In this lesson we have begun by analyzing the impact of technologies on our lives, acquiring a broader sociological view of their function and influence. Some positive effects have been analyzed, such as the ease of communicating and sharing information in a simple and fast way, which allows the dissolution of spatiotemporal barriers. Other less positive effects have also been analyzed, such as the manipulation of information or the existence of the digital breach, among others.

The lesson then focused on the use of technologies made by our adolescent students and the main psychosocial risks they face. The following were specifically analyzed:

- Access to inappropriate content for their age
- Cyberbullying
- Technology addiction
- And other psychosocial risks such as family conflicts or the abandonment of other "non-technological" activities.

At the same time, the role of the educational centre in the definition of a policy that favours the responsible use of technology to avoid possible risks derived from misuse was analysed and some advice was revised to adapt to the data protection law or to deal with some conflicts derived from the misuse of WhatsApp groups, information shared on social networks or the use of mobile devices in the centre.

Throughout the lesson, some essential guidelines have been provided to encourage responsible use of technologies among students, as well as some advice to help their families to reinforce work outside the classroom. Examples, didactic materials for application in the classroom and other useful activities in non-school contexts have been provided. All this in order to promote in an efficient and coordinated way the responsible use of adolescents and the technological resources available to them.

REFERENCES

- Bender, William (2014). Penso, ed. Aprendizagem Baseada em Projetos: educação diferenciada para o século XXI (en portugués). Porto Alegre, Brasil. p. 15. ISBN 978-85-8429-001-7.
- Cañón, R., Grande, M. y Ferrero, E. (2018) Ciberacoso: revisión de la literatura educativa en español. Revista Latinoamericana de tecnología educativa. Vol. 17 Núm. 2 (2018). Recuperado de: https://doi.org/10.17398/1695-288X.17.2.87
- Comisión Europea. (2012). Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones. Estrategia europea en favor de una Internet más adecuada para los niños. OPOCE. Retrieved from https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52012DC0196&from=EN
- Hoffman, D.L, Novak, T.P. y Schlosser, A. E. (2001) The evolution of the digital divide: Examining the relationship of race to Internet access and usage over time. En Compaine, B. Digital Divide. Cambridge, Massachussets: The MIT Press
- <https://www.is4k.es> . Retrieved on March, 2019.
- <http://www.tudecideseninternet.es> Retrieved on March, 2019.
- <https://www.incibe.es> Retrieved on March, 2019.

- <http://digital.csic.es> Retrieved on March, 2019.
- <https://www.esrb.org/ratings/ratings_guide.aspx> Retrieved on March, 2019.
- <http://www.rtve.es/contenidos/documentos/Codigo_proteccion_infancia.pdf> Retrieved on March, 2019.
- <https://pegi.info> Retrieved on March, 2019.
- <https://www.europol.europa.eu/stopchildabuse> Retrieved on March, 2019.
- Lévy, P., & Medina, M. (2011). Cibercultura: Informe al consejo de Europa (1a, 1a reimp ed.). Rubí, Barcelona: Anthropos.
- Marí, V. M. (1999). Globalización, nuevas tecnologías y comunicación. Madrid: Ediciones de la Torre.
- Mcluhan, M. (1968). In Fiori Q. (Ed.), Guerra y paz en la aldea global (J. Méndez Herrera Trans.). (1985ª ed.). Barcelona: Planeta - Agostini.
- Save the Children. (2017). Acceso a las nuevas tecnologías de los menores de edad. Retrieved from https://www.savethechildren.es/sites/default/files/imce/acceso_internet_menores_edad_1.pdf
- Soto, Antonio; de Miguel, Natalia; Pérez Díaz, V. (2018). Abordaje de adicciones a nuevas tecnologías: una propuesta de prevención en contexto escolar y tratamiento de rehabilitación. Papeles Del Psicólogo, 39(2), 2–12. Retrieved from https://www.redalyc.org/articulo.oa?id=77855949007
- Vuorikari, R., Punie, Y., Carretero Gómez, S., & Van Den Brande, G. (2016). DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model. - European Commission. https://doi.org/10.2791/11517