WHAT IS PRIVACY AND WHY IT IS IMPORTANT?

EUROPEAN CYBER SECURITY MONTH

Target Audience: eTwinning teachers

Subject: Privacy

According to the Oxford Dictionary, privacy is a "state in which one is not observed or disturbed by other people" or "the state of being free from public attention;" [1] The Cambridge Dictionary says it is "someone's right to keep their personal matters and relationships secret," [2] while Merriam Webster defines it as " freedom from unauthorized intrusion." [3]

We all love to share stuff about our life and talk to our friends and loved ones online. The problem is that the internet is open to everyone, and some people can use this online information for malicious purposes. Therefore, it is important to value and protect our online privacy.

2018 is a really important year for privacy. In May, the new European Union General Data Protection Regulation (GDPR) came into effect, effectively harmonizing how companies handle your data throughout the EU. If you want to know bit more about it, read this short Q&A.

1 https://en.oxforddictionaries.com/definition/privacy
2 https://dictionary.cambridge.org/dictionary/english/privacy
3 https://www.merriam-webster.com/dictionary/privacy

TWO IMPORTANT PRIVACY RULES AND SOME TECHIE RECOMMENDATIONS

1. Think about what you post

Before posting or uploading something online, one should take a break and think.

Is it really necessary to post and share everything? If one constantly shares everything online, it is easier for cyber criminals to profile you and find patterns. As a rule of thumb, one should assume that anyone might read what is posted online.

If every Tuesday and Thursday you take a selfie while you run on the gym's treadmill, for some people this means that you are fit, whereas for malicious actors, it means you are not at home....what a great moment to break into your home and steal everything!

"SHARING PERSONAL INFORMATION" - VIDEO BY THE PORTUGUESE SAFER INTERNET CENTRE

Exercise

Encourage your students to think about what people might learn about them and how that might affect their lives, now and in the future.

Ask them to go back and see what they have posted one year ago: Do they still agree with what they have shared online in the past? Does it reflect the way they currently are or think? Share the outcomes of this exercise in the forum.

When you would like to share things about other people online, try to put yourself in the their shoes: **would I like him or her to share the video, picture or post about me online?** If you feel you would not be comfortable about it, why would you do that to someone else? Ideally you should try to always ask permission when you share moments of other people's life online.

2. Restrict access to your online profiles

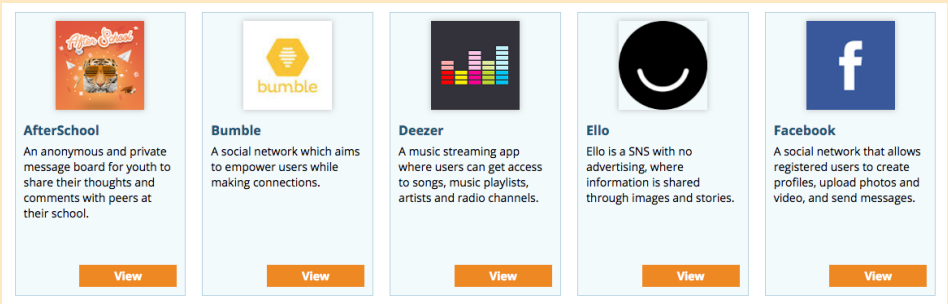
Tell your students about how and who personal posts might reach and who can read them if their online profiles are accessible to everyone. There are stories and news that are better to only be shared with the closest friends. Before you start using a social networking site, a game or an online platform, one should make sure to carefully check the privacy settings. Moreover, do not add people if you do not know them! They might be just curious people chilling online, but it might be someone who is looking to cause harm to you.

"YOUR IMAGE YOUR FUTURE" – VIDEO BY THE UK SAFER INTERNET CENTRE

For an extra layer of security

Some apps and platforms want to access some of your data "in exchange" for their services. It is a trade-off. One should be thoughtful about what information these services look for and how they are collected. When you have time, it is a good idea to take a look at the permissions granted to an app (such as access to your contacts, calendar etc.) and read their privacy policies.

Check out the Better Internet for Kids Guide to Online Services, providing key information about some of the most popular apps, social networking sites and other platforms which are commonly used by children and young people (and adults) today.



Some techie recommendations

Nowadays, it is almost inevitable to leave an online footprint behind us.

The thing is, the bigger your online footprint, the easier it is for people to profile you or track you down. Why? Some online services track people down mainly to display ads and make you click on them. Other people are actually trying to get personal data.

The first two rules were about avoiding flooding the web with personal information. Now, here are some little tech tricks that can limit our digital footprint and avoid our information being intercepted.

Use private browsing and multiple web browsers

Major web browsers have added the possibility of surfing in a “private mode.” The major pro is that, if someone shares a computer with other people at home, people would not be able to view his or her browsing history. Also, in private mode the web browser will not store cookies and sites data, as they will be deleted when the online session is closed.

To be fair, if you would like no-one to see what you do online, private browsing does not help much. It still allows the web browser and service provider to know what websites people are visiting, but private mode is still a good first step.

Also using more than one web browser could limit online tracking. If one uses different web browsers for different activities, one will limit the amount of information – your digital footprint – that can be collected by one single browser.

Use multiple (and possibly private) search engines

Similar to what we have just said, it might be worth using more than one search engine to prevent one tool having access to your full browsing history as well as other personal online information.

The great news is that there are some search engines that claim to be built with “privacy in mind,” meaning they are not interested in collecting or sharing any of your personal information for commercial purposes. Some of these engines are DuckDuckGo and StartPage

Surf on websites with “https”

Have you ever noticed the acronym HTTPS when you surf the web?

HTTPS stands for **H**yper **T**ext **T**ransfer **P**rotocol **S**ecure and means that when data is sent to these websites it is secured through encryption. To put it simply, people cannot snoop the private information sent to the website.

Not every website uses HTTPS. So, if it is not there, maybe you can suggest to your students that they use another service?

Turn off Wi-Fi, Bluetooth and GPS

It is recommended to turn off Wi-Fi, Bluetooth and GPS if they are not being used.

Open Wi-Fi connections do not always use encryption, meaning that someone nearby could potentially intercept precious data that sent over the internet such as your passwords or other details.

Smart malicious people can hack your device through the Bluetooth signal when this is switched on.

Finally, some applications and services can access and collect GPS data, similar to what they do with other data stored in your device.

TURN OFF WI-FI, BLUETOOTH AND GPS IF THEY ARE NOT BEING USED.

For an extra layer of privacy

Consider using Privacy Badgers and HTTPS Everywhere, developed by the Electronic Frontier Foundation, a non-profit organization with the goal to defend civil liberties in the digital world.

Privacy Badger is a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. It can be downloaded here.

HTTPS Everywhere is a browser extension that encrypts your communications with many major websites by enabling the sites' HTTPS protection. The extension activates the website security features when those are available. It can be downloaded here.

Find more resources on the Better Internet for Kids portal!

More cyber hygiene resources in various European languages can be found at the Better Internet for Kids portal. Check out the #SaferInternet4EU campaign page.