WHAT IS A PASS-WORD AND WHY IT IS IMPORTANT?

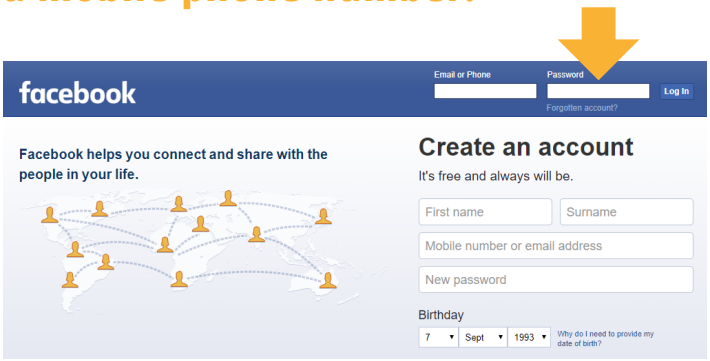
EUROPEAN CYBER SECURITY MONTH

Target Audience: eTwinning teachers

Subject: Passwords

The dictionary defines password as "a secret word or phrase that must be used to gain admission to a place."

It is typically used with a username, which can be anything ranging from a name, an email or a mobile phone number.



Passwords are important to keep personal information safe or to access an online service.

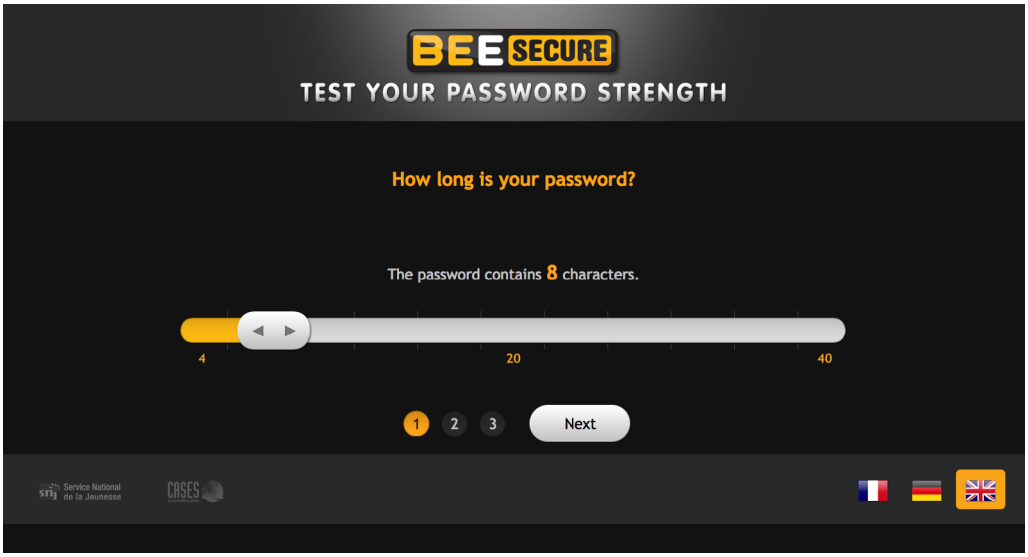
FIVE RULES ABOUT PASSWORDS SECURITY EVERYONE SHOULD FOLLOW

1. Create a strong password: MilkFootballMonday2018!

There are many articles online on what makes a strong password – and it can be incredibly confusing. Let's start with the top 10 passwords one should NEVER use:

PICTURE SOURCE: DAILYMAIL.CO.UK

These passwords are too simple, short and are usually the first ones that cyber criminals attempt when they try to access online accounts. Test your password strength with the following tool created by the Luxembourg Safer Internet Centre: https://pwdtest.bee-secure.lu/?lang=en.



To create a strong password, use three random words such as:

“milk” and “football” and “monday”

Put them together in the order you prefer:

“milkfootballmonday”

Make it stronger by using some upper case letters

“MilkFootballMonday” Or “milKfootbalLmondaY”

It will take a computer 898 thousand years[1] to guess such a password.

Cool video: https://www.youtube.com/watch?v=1mM0zrFyILU

For an extra layer of security

You can think of increasing the complexity of your password:

1. Choose three random words, use upper cases and add a number. “MilkFootballMonday2018”

2. To make it even more difficult to guess, add a special character for a final layer of protection: “MilkFootballMonday2018!”

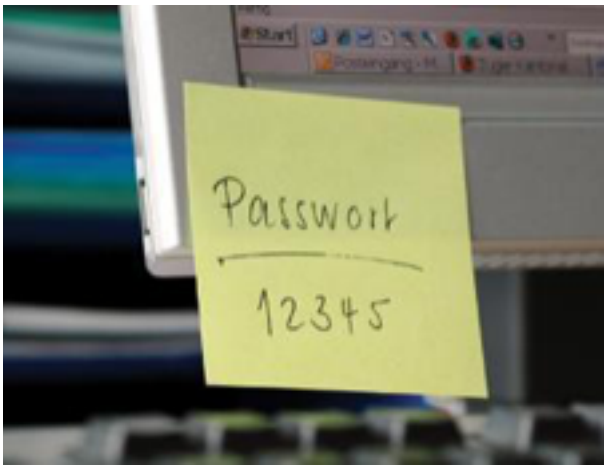
To guess the password“MilkFootballMonday2018!”, it will take a computer 252 sextillion years.

1 https://howsecureismypassword.net/

2. How to remember passwords: write them down and put them in a safe place

Creating a strong password is not difficult, but the problem is remembering all of them. The suggestion here is to write them down.

But be aware, one should never write down a password and stick it to the screen of the computer. Anyone can easily find it and use it to access your accounts!



It is true that if someone found that piece of paper, it could access all the websites and apps that are protected by those passwords. First, we suggest to not write on the same line the website/app and the password you use to access it. Even if someone found the password's paper, it would be harder for this malicious person to know what password is used to enter a specific website. Second, and most importantly, it is important to put that piece of paper in a safe place, where none could access it. Some suggest to hide the list of passwords inside a paperback book – away from the device.

VIDEO: "HUNT THE PASSWORD" BY GET SAFE ONLINE

For an extra layer of security

Instead of using a safe, a password manager can be a useful tool to keep passwords safe. The advantage of a password manager is that it stores all passwords and usernames in a single place. It is useful, but also risky. In theory, someone with access to a computer, could also access the password manager and steal usernames and passwords. However, password managers require to set up an initial master password, in order to keep all the others safe. Some of the most popular web browsers have a password manager integrated. If you would like to know more, read this article on Wikipedia and choose the perfect password manager from this list.

3. Don't tell a personal password to anyone

Some things are better kept secret, even from the closest friends. One should never tell anyone else their password or where they are stored.

Do not be like them (https://www.youtube.com/watch?v=UzvPP6_LRHc)!

4. Use different passwords for different accounts

It is important to have a different password for every device, application and website. In case these are hacked, passwords and usernames can be revealed and spread all over the internet and then used by cyber criminals to access accounts that are protected by them.

If having a different password for every account is too much to manage , then another tip could be to think of groups of passwords. For social media like Facebook and Instagram, you can have one password; for the school account, another one. If one decides that is the way to go, a good rule of thumb is: the more important the website, the more unique the password should be. If a website or application stores really important information, one should have a strong password and use it only for that website.

IT IS IMPORTANT TO HAVE A DIFFERENT PASSWORD FOR EVERY DEVICE, APPLICATION AND WEBSITE.

5. If you change your password, change it entirely

It is ok to change passwords from time to time, but when is done, one should change the entire password and not a small piece of it. Smart criminals can make educated guesses from previously used passwords and deduce how passwords are created.

For example, if one finds out that you change your password usually...

MilkFootballMonday2018

MilkFootbalMonday2019

MilfFootbalMonday2020

...it would not be difficult to guess what the next password will be!

For an extra layer of security

- Some public internet connections, such as in airports and in coffee shops, can be misconfigured and unsafe. Cyber criminals could have infected them and be ready to intercept the information that are transmitted online. Therefore, it would be better to **avoid entering passwords when these public Wi-Fi connections** are used and, more generally, **on computers that are not your own**. In this case, someone could have installed a program memorizing everything that is typed on the keyboard, including usernames and passwords.

- Some websites offer an extra layer of protection and use **multi-factor authentication**: this can be quite burdening, but one should consider using multi-factor authentication for websites that are particularly valuable to you, such those storing financial information. If you interested, please click on this link to see how to set up two factor authentication.

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.