cyVETsecurity

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

SAFE DEVICE USE IN AN UNSAFE DIGITAL WORLD

Document for students

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

Duration of the challenge

3-6 hours

Your team

Student / teacher should allocate the following:

Team name:

Team member names:

Description of the situation

You have received a new digital device as a gift (the teacher should specify which device / devices you will use). As a responsible digital user, you want to try to ensure that the device and any information are protected where possible.

You plan to use the device for general use, such as email, browsing the web, social networking and online banking.

Your challenge is to demonstrate your understanding and awareness of the cyber security issues that are inherent with new digital devices.

Learning objectives

U1LO1. The learner is able to identify physical and virtual risks associated with technology

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

U1LO2. The learner is able to implement the strategies to prevent risks and updates themselves in this matter

U1LO3. The learner is able to install / update anti malware software

U1LO4. The learner is able to protect themselves from fraud by using secure passwords.

U1LO5. The learner is able to protect different vulnerable devices from digital threats (malware, phishing etc…)

U1LO6. The learner is able to identify sensitive/valuable information and attacks on different types of data

Resources you can use

Some general resources to help you get started:

- https://en.wikipedia.org/wiki/Computer_security
- https://en.wikipedia.org/wiki/Digital_security
- https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more
- https://passwordsgenerator.net
- https://howsecureismypassword.net/
- https://www.roboform.com/how-secure-is-my-password
- https://lastpass.com/howsecure.php

Recommended process

In order to solve your challenge, you need to work in an organised way. We suggest you follow these steps:

1. Establish the parameters you need to solve the challenge. For example, in this case these could be: risks associated to technology, protective measures, vulnerable information (prone to be attacked).

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

2. Look for information related to those parameters (see resources proposed, but it is suggested you use others)
3. Select which information is important to solve the challenge.
4. Come up with different proposals to solve the challenge.
5. Select the proposal/proposals which are more effective from your group´s point of view.
6. Plan which actions you need to solve the challenge (once you know what you need to do, describe how you will do it).
7. Implement the actions.
8. Present the results (following teacher´s instructions).
9. Evaluate how you carried out the challenge

Evaluation criteria

- Your team groups multiple risks into 3 physical and 3 virtual.
- Your team describes a strategy to prevent being compromised.
- Your team installs / updates an anti-malware software on a given device.
- Your team generates and tests a secure password
- Your team identifies potential vulnerabilities of your new device and possible mechanisms for their protection.
- Your team identifies sensitive data and possible attacks depending on the nature of the data

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