cyVETsecurity

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

SAFE DEVICE USE IN AN UNSAFE DIGITAL WORLD

Document for teachers

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.

cyVETsecurity

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

Duration of the challenge

3-6 hours

Description of the situation

You have received a new digital device as a gift (the teacher will specify which device 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

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

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.

Minimum requirements to carry out the challenge

Previous knowledge	Equipment/software	Training resources
Having had exposure to or use of an internet enabled device such as a PC / Laptop/ Tablet or smartphone	An internet connected device, such as: PC Laptop Smartphone Tablet	• 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 *There are a very large body of resources available for this curriculum. Teachers should use all resources available to them. These are the resources that have been issued to the students in the challenge.*

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.

cyVETsecurity

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

Schedule of the challenge

Suggested below are notional time allocations for the challenge:

- 0,5 hours to identify the parameters of the challenge (possibly including identifying who will carry out which task (s))
- 1 hour to look for information
- 0,2 hours to select information
- 0,2 hours to generate alternatives
- 0,3 hours to present proposals / collate findings and discuss them (within the student´s group)
- 0,2 hour to identify how findings will be presented (if not stipulated by teacher)
- 0,2 hours to prepare findings into appropriate format i.e. PowerPoint for presentation
- 0,15 hours to present / discuss findings
- 0,15 hours to evaluate / assess how you carried out the challenge and how you might make improvements for any future activities

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.

Presentation of the results

The findings can be presented in whatever media the group decide upon. The findings must be in a form that can be retained following the challenge.

This could be a presentation of the findings, which may include but is not restricted to the following formats:

- Video
- Presentation using Software
- Oral \ verbal (This would need to be recorded)
- Written report
- Blog / vlog /wiki
- Any other suitable medium

Note: Teachers should decide the appropriate format for the students to present their results.

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.

Evaluation criteria

The following *guidelines* are **suggestive** only and are provided as guidance to support the teacher.

Public presentation (20%)

A ***suggested*** evaluation table in ***Appendix A*** at the back of this document which contains criteria can be used to help the teacher assess public presentation skills

Teamwork performance (20%)

A **suggested** evaluation table in ***Appendix B*** at the back of this document contains criteria that can be used to help the teacher assess team working skills.

Findings from the challenge (60%). Possibly 10% per item.

1. The team groups multiple risks into 3 physical and 3 virtual.

Possible student responses:

Physical risks	Virtual / Software risks
Leaving device unattended/ device being stolen	Not have any anti-virus on device
Water damage to the device	Not updating to most recent software on device (patching)

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.

Giving your password to someone	Weak security credentials on device (password / pin etc)

2. The team describes a strategy to prevent being compromised.

Items that ***should*** be included in the strategy (for the user of the device):

- Restricting access to the device by requiring user authentication (this should include an emphasis on pin / biometric (i.e. fingerprint) / strong passwords. 2 factor authentication (2FA) should also be **mentioned** as at the time of writing this is the 'direction of travel' for user authentication.)
- Update your device Operating System with latest security patches
- Regularly back up your data
- Use encryption / secure websites where possible
- Disable any unused services, such as wi-fi and Bluetooth
- Be educated (where possible), don't fall for Phishing etc
- Have up-to-date anti-malware software installed

3. The team installs / updates an anti-malware on a given device

This can be installing of new anti-malware (AM) software or ensuring that the current AM software is the most recent version. NIST.org have a list of guidance on available AM:- https://www.nist.org/news.php?extend.45.11

It also includes a free service where the user can upload any given file to be scanned remotely. https://www.virustotal.com/gui/home/upload. This may be of use if users cannot run scans locally on their device.

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.

4. The team generates and tests a secure password

The student ***could*** use the links that are included in the resources section to:

- Generate a password –
- https://passwordsgenerator.net
- Test the generated Password –
- https://howsecureismypassword.net/
- https://www.roboform.com/how-secure-is-my-password
  https://lastpass.com/howsecure.php

5. The team identifies potential vulnerabilities of your new device and possible mechanisms for their protection.

This should be a minimum of 3 potential vulnerabilities and possible protection mechanisms, such as:

Potential vulnerabilities	**Mitigation**
The new device arrives with no authentication	Enable authentication on the device
Services such as wi-fi and Bluetooth are automatically enabled and can be compromised.	Turn off any unused or unnecessary services.
Downloading malware that might be embedded with new apps.	Download only from recommended sites / locations. Ensure anti malware software is installed and up to date.

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.

6. The team identifies sensitive data and possible attacks depending on the nature of the data.

Below are some ***examples***:

Platform / Area of concern	**Type of data**	**Attack vector**
Social networks	Personally Identifiable Information (PII)	Social engineering, Phishing etc
Online Banking	Financial, PII	Social engineering, Phishing etc
Discarding old mail into the bin	Financial, PII	Dumpster diving
Email	Images / pictures	Steganography (concealing information inside images)

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.

cyVETsecurity

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

Appendix A

Presentation evaluation (Team or Individual)

Criteria	Excellent	Very good	Good	Fair	Not Done	Comments/Suggestions:
Oral Introduction: Introduced speaker, captured audience attention	4	3	2	1	0	
Body of Speech: Easy to follow and understand, information seemed accurate and complete	4	3	2	1	0	
Summary: Brief, clear, and provided a wrap-up of the topic	4	3	2	1	0	
Performance: Speaker showed good inflection, proper pronunciation, used expression to demonstrate points, appeared conversational and natural, made eye contact with audience, and voice was loud and clear enough to hear; reliance on notecards was limited	4	3	2	1	0	
Participant's Knowledge: Participant was able to answer questions from the audience after repeating the question	4	3	2	1	0	
Audience Attention: Held audience's attention for the duration	4	3	2	1	0	
Sources: Sources were listed at the end of the speech	1	0	0	0	0	

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.

Appendix B

Goals						
Goals are unclear or poorly understood, resulting in little commitment to them.	1	2	3	4	5	Goals are clear, understood, and have the full commitment of team members.
Openness						
Members are guarded or cautious in discussions.	1	2	3	4	5	Members express thoughts, feelings, and ideas freely.
Mutual Trust						
Members are suspicious of one another's motives.	1	2	3	4	5	Members trust one another and do not fear ridicule or reprisal.
Attitudes Toward Difference						

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.

Members smooth over differences and suppress or avoid conflict.	1	2	3	4	5	Members feel free to voice differences and work through them.
Support						
Members are reluctant to ask for or give help.	1	2	3	4	5	Members are comfortable giving and receiving help.
Participation						
Discussion is generally dominated by a few members.	1	2	3	4	5	All members are involved in discussion.
Decision-making						
Decisions are made by only a few members.	1	2	3	4	5	All members are involved in decision-making.
Flexibility						

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.

The group is locked into established rules and procedures that members find difficult to change.	1	2	3	4	5	Members readily change procedures in response to new situations.
Use of Member Resources						
Individuals' abilities, knowledge and experience is not well utilized.	1	2	3	4	5	Each member's abilities, knowledge, and experience are fully utilized.

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.