cyVETsecurity

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

SEADMETE OHUTU KASUTAMINE EBATURVALISES DIGITAALMAAILMAS

Juhend õpilastele

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.

Kestvus

3-6 tundi

Meeskond

Õpilase / õpetaja poolt jaotatavad ressursid:

Meeskonna nimi:

Meeskonnaliikmete nimed:

Ülesande kirjeldus

Oled saanud kingituseks uue digitaalse seadme (õpetaja täpsustab millist seadet/seadmeid kasutate). Vastutustundliku kasutajana soovid sa, kindlustada, et seadme kasutamine ja informatsioon selles oleks võimalikult hästi kaitstud.

Soovid kasutada seadet tavapäraselt: kasutada e-post, surfata internetis ja kasutada internetipanka,

Sinu ülesanne on demonstreerida oma arusaamu ja teadlikkust küberturvalisuse probleemidest uue digitaalse seadme kasutamisel.

Õpiväljundid

U1L01. Õpilane identifitseerib tehnoloogiaga seotud füüsilisi ja virtuaalseid riske

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. Õpilane rakendab meetmeid riskide ennetamiseks, arendab oma teadmisi ja oskusi nimetatud valdkonnas,

U1LO3. Õpilane oskab viirusetõrje programme installeerida ja neid uuendada.

U1LO4. Õpilane kasutab turvalist parooli, et kaitsta ennast võimalike pettuste eest.

U1LO5. Õpilane oskab kaitsta erinevaid haavatavaid seadmeid võimalike digitaalsete ohtude eest (viirused, andmete õngitsemine jms).

U1LO6. Õpilane oskab identifitseerida andmete sensitiivsust/väärtust ja tunneb ära rünnakud erinevat tüüpi andmetele.

Kasutavad allikad

Mõned soovituslikud allikad:

- 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

Protsess

Ülesande lahendamiseks tuleb tegutseda organiseeritult. Selleks soovitame lähtuda järgmistest sammudest:

1. Selgita välja olulisemad lähtekohad ülesande lahendamiseks. Näiteks käesoleval juhul: tehnoloogiaga seotud riskid, peamised kaitsemeetmed, haavatav informatsioon (mida võidakse rünnata),.
2. Otsi informatsiooni, mis on seotud eelpool nimetatud lähtekohtadega, vaata üle kasutatavad allikad ja otsi ka ise uuemaid allikaid.

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.

3. Selekteeri välja olulisemad allikad ülesande lahendamiseks.
4. Paku välja erinevaid lahendusi.
5. Leidke meeskonnaga ühiselt kõige efektiivsem lahendus.
6. Koostage plaan ülesande lahendamiseks (kui olete kindlaks teinud, mida on tarvis teha, siis kirjeldage ka kuidas te seda teete).
7. Realiseerige oma plaan.
8. Esitlege tulemused (vastavalt õpetaja juhistele).
9. Hinnake, kuidas tulite toime ülesande lahendamisega.

Hindamiskriteeriumid

Meeskond:

- Suudab leida vähemalt 3 füüsilist ja 3 virtuaalset riski.
- Kirjeldab strateegiat riskide ennetamiseks.
- Installeerib / uuendab seadme viirusetõrje rakenduse.
- Genereerib turvalise parooli ja testib selle turvalisust.
- Määratleb uue seadme haavatavusi ja võimalikke kaitsemeetmeid.
- Määratleb sensitiivsed andmed ja võimalikud rünnakud seda tüüpi andmetele.

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.