

LAITTEEN TURVALLINEN KÄYTTÖ EPÄTURVALLISESSA DIGITAALISESSA MAAILMASSA

Dokumentti opiskelijoille

Haasteen kesto

3-6 tuntia

Sinun tiimisi

Opiskelijan / opettajan tulisi päättää seuraavat asiat:

Tiimin nimi:

Tiimin jäsenten nimet:

Tilanteen kuvaus

Olet saanut uuden digitaalisen laitteen lahjaksi (opettajan pitäisi tarkentaa mikä laite / laitteet, jotka otetaan käyttöön), Vastuullisena digitaalisena käyttäjänä haluat yrittää varmistaa, että laita ja tiedot ovat suojattuja.

Suunnittelet käyttäväsi laitetta yleisesti, esimerkiksi käyttämällä sähköpostia, sosiaalista mediaa ja verkkopankkia ja selailemalla verkkosivuja,

Haasteenasi on näyttää, että ymmärrät ja olet tietoinen tietoturva-aiheista, jotka ovat luontaisia uusissa digitaalisissa laitteissa.

Oppimistavoitteet

U1L01. Oppija osaa tunnistaa fyysisiä ja virtuaalisia riskejä, jotka liittyvät teknologiaan

U1L02. Oppija osaa soveltaa riskien ehkäisyn strategioita ja pitää tietonsa ajan tasalla

U1L03. Oppija osaa ladata ja päivittää virus/haittaohjelmatorjuntaohjelmiston

U1L04. Oppija osaa suojata itsensä väärinkäytöksiltä käyttämällä turvallisia salasanoja

U1L05. Oppija osaa suojata erilaisia haavoittuvia laitteita digitaalisilta uhilta (haittaohjelmat, kalastelu jne.)

U1L06. Oppija osaa tunnistaa arkaluontoisen / arvokkaan informaation ja hyökkäykset erityyppisessä datassa

Resurssit joita voit käyttää

Joitakin yleisiä resursseja alkuun pääsemiseksi:

- 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>

Suositteltu prosessi

Jotta voitte ratkaista tämän haasteen, teidän täytyy työskennellä järjestelmällisellä tavalla. Suosittelemme seuraavia askeleita:

1. Aseta parametrit, joita tarvitsette haasteen ratkaisemiseen. Esimerkiksi tässä tapauksessa teknologiaan liittyvät riskit, suojaustoimenpiteet, haavoittuva tieto (alttiita hyökkäyksille).
2. Etsikää tietoa, joka liittyy näihin parametreihin (katso ehdotettuja resursseja, mutta voitte myös käyttää muita).

3. Valitkaa mikä tieto on tärkeää haasteen ratkaisemiseksi.
4. Keksikää erilaisia ehdotuksia haasteen ratkaisemiseksi.
5. Valitkaa ehdotus / ehdotukset, jotka ovat tehokkaimmat sinun ryhmäsi näkökulmasta.
6. Suunnitelkaa toimet, joita tarvitsette ongelman ratkaisemiseksi (kun tiedätte mitä tulee tehdä, kuvailkaa miten teette sen).
7. Toteuttakaa toimet.
8. Esittäkää tulokset (noudattakaa opettajan ohjeita).
9. Arvioikaa miten suoriuditte haasteesta.

Arviointikriteerit

- Tiimisi ryhmittelee monipuolisia riskejä 3 fyysisiin ja 3 virtuaalisiin riskeihin.
- Tiimisi kuvaa strategian, jolla ehkäistään riskejä.
- Tiimisi asentaa / päivittää virus/haittaohjelmaohjelmiston annetulle laitteelle.
- Tiimisi luo ja testaa turvallisen salasanan.
- Tiimisi tunnistaa potentiaalisia, haavoittuvia laitteita ja mahdollisia mekanismeja niiden suojelemaan.
- Tiimisi tunnistaa arkaluontoisen datan ja mahdolliset hyökkäykset datan luonteesta riippuen.