KOOLITUSKESKUS WALK
УЧЕБНЫЙ ЦЕНТР WALK
EDUCATIONAL CENTER WALK
MĀCĪBU CENTRS WALK

KOOLITUSKESKUSE WALK

Õppematerjal

Koolitus:

Kaug -töötamise ja -õppimise koolitus

Teema

Küberruumi riskid

2020

Sisukord

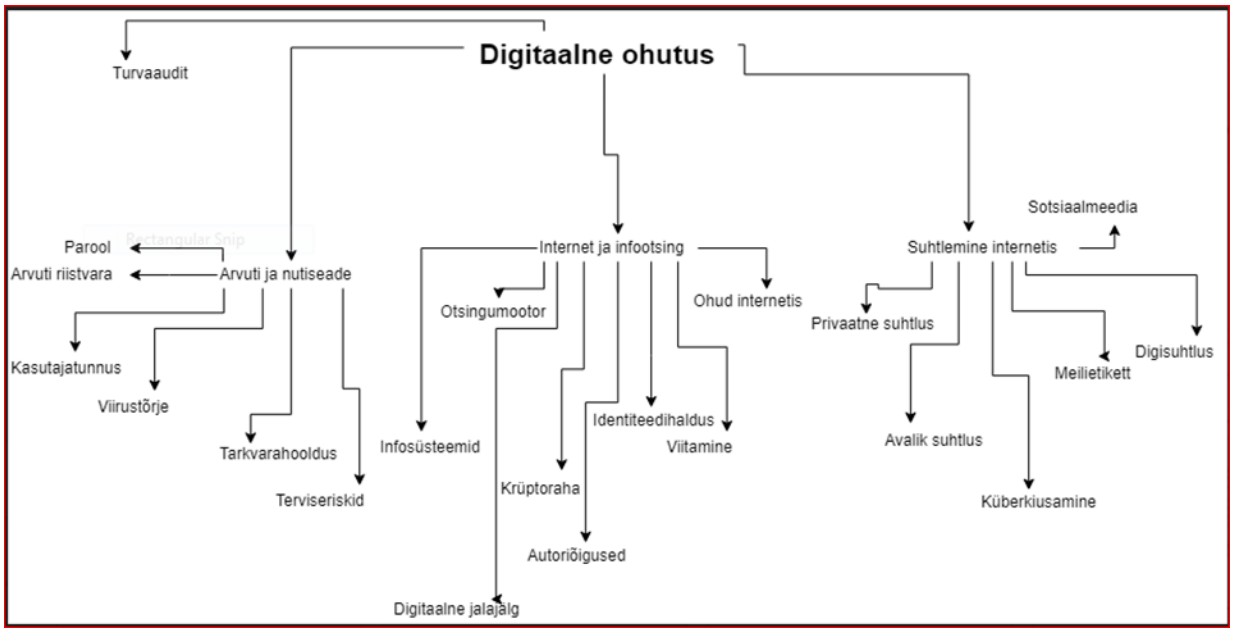
Teema: Küberruumi riskid 2
1.1. Liigid 2
1.1.1. Pahavara 3
1.1.2. Arvutiviirus (ehk viirus) 3
1.1.3. Trooja hobune (ehk troojalane) 3
1.1.4. Lunavara 3
1.1.5. Nuhkvara 3
1.1.6. Õngitsemine 4
1.1.7. Sotsiaalmanipulatsioon 4
1.1.8. Küberkiusamine 4
1.1.9. Pahavara poolt põhjustatud kahju 4
Küberhügieen 4
Ülesanne 4
Täiendavad allikad – loe lisaks 5
Kasutatud allikad 6

Teema: Küberruumi riskid

Õpiväljundid:

- teab küberruumi riske;
- oskab end kaitsta ennast veebipettuste ja küberkiusamise eest;
- oskab kaitsta oma isikuandmeid;
- saab aru teiste inimeste õigusest privaatsusele.

1.1. Liigid



Õppesisu:

Pahavara (Malware), selle erinevad liigid.

Õngitsemine.

Rämpspost.

Sotsiaalmanipulatsioon.

Ohud sotsiaalvõrgustike kasutamisel.

Kontode kaaperdamine

Botid ja virtuaalsed arvamusliidrid.

Pahavara poolt põhjustatud kahju

Küberkiusamine.

Ohud nutiseadmete kasutamisel.

Küberhügieen

Viirusetõrje

Tarkvara uuendused.
Kasutajakontod ja paroolid.
Linkide, kodulehtede ja e-posti turvalisuse kontrollimine.
Pahatahtlike rakenduste leidmine Facebookist ja Google Chrome'ist.
Failide allalaadimised.
Turvaline surfamine.
E-posti turvaline kasutamine (käitumisreeglid, sildid ja filtrid).

1.1.1. Pahavara

Pahavara malware (MALicious softWARE) (ka kahjurvara, kurivara, õelvara, ründevara, ründetarkvara) on arvutiprogramm, mis on kirjutatud spetsiaalselt selleks, et arvutit ilma selle haldaja ja valdaja teadmata kahjustada või kuritarvitada. (Kurivara) Kurivaral on hulgaliselt alaliike, allpool on mõnede enamlevinumate tutvustus

1.1.2. Arvutiviirus (ehk viirus)

Pahavara, mis on võimeline end iseseisvalt kopeerima ning arvutit nakatama. (Arvutiviirus). Mõistet „viirus" kasutatakse ekslikult ka sellist tüüpi pahavara puhul, millel ei ole isepaljunemisvõimet.

1.1.3. Trooja hobune (ehk troojalane)

Pahavara, mis tavaliselt tuleb kaasa koos mõne teise arvutiprogrammi või failiga. (Trooja hobune)

1.1.4. Lunavara

Pahavara, muudab kasutaja arvutis (ka nutiseadmetes ja kasutaja pilveteenustes) olevad failid kasutuskõlbmatuks ning nõuab töö taastamiseks üldjuhul lunaraha virtuaalses krüptorahas BitCoin.Lunavara levitatakse nii e-kirjade kui ka veebilehtede kaudu. (https://blog.ria.ee/kuberturvalisuse-abc/)

1.1.5. Nuhkvara

Pahavara, mis kogub arvutikasutaja isiklikku infot, ilma et sellest kasutajat oleks selgesõnaliselt teavitatud. Nuhkvara alaliik on klahvinuhk (keylogger), mis salvestab kasutaja klahvivajutusi. Nuhkvara saadab talletatud info edasi kurjategijatele.

1.1.6. Õngitsemine

Õngitsuslehtede ja -kirjade eesmärk on kätte saada kasutaja isiklikke andmeid – kasutajatunnuseid, paroole, krediitkaardiandmeid jms. Kasutatakse võlts e-kirju, veebilehti või telefonikõnesid. Veebilehed ja e-kirjad tehakse visuaalsele sarnaseks päris kaubamärgiga.

1.1.7. Sotsiaalmanipulatsioon

Küberkurjategijate ründeviis konfidentsiaalse informatsiooni kättesaamiseks. Kasutatakse ära inimloomuse nõrkasid kohti. Selmet kasutada keerukaid programme, millega arvutisüsteemi otse rünnata, proovitakse saada infot otse inimese käest. Põhivõtted: vaatlemine, üle õla vaatamine (shoulder surfing), prügikastis tuhnimine (dumpster diving), sappavõtmine (tailgating), maskeerimine, küsimustike kasutamine, USB-mälupulga mahajätmine, sotsiaalmeedia ja veebisaitide kasutamine, Info saamine telefoni teel, juhi identiteedi kasutamine.

1.1.8. Küberkiusamine

On kiusamine digivahendite abil. Näiteid: teise inimese nimele tehtud libakontod, sõimamine ja ähvardamine ning õelad kommentaarid foorumites, võõraste piltide ülesriputamine ja moonutamine jms.

1.1.9. Pahavara poolt põhjustatud kahju

Küberhügieen

Käitumiste ja võtete jada kasutamisel loodud olukord, kus on hoolikalt läbi mõeldud nii inimese enda andmete kui ka asutuse või organisatsiooni andmete kaitsmine. (https://et.wikipedia.org/wiki/K%C3%BCberh%C3%BCgieen)
Eesmärk vähendada peamiselt kasutajat ohustavaid küberohte: – andmekadu (nt varukoopiad puuduvad) – andmelekked (info juhuslik või sihilik sattumine volitamata isikute kätte) – erinevad võrgupõhised turvariskid (rämpspost, pahavara, sotsiaalmanipulatsioon, otsesed ründed).
Eeldab inimese käitumise muutumist. Lihtsalt infost on vähe, et käitumist muuta.
Kordamisküsimused (Testi küsimused) ja ülesanded.

Ülesanne

Selgita pildil toimuvat. Pilt asub https://commons.wikimedia.org/wiki/File:Botnet.svg

Täiendavad allikad – loe lisaks

- Veebileht Arvutikaitse https://www.arvutikaitse.ee/
- Veebileht Targalt Internetis https://www.targaltinternetis.ee/
- Küberturvalisuse ABC https://blog.ria.ee/kuberturvalisuse-abc/
- Kasulikke näpunäiteid internetist ostmisel https://ostatargalt.ee/internetipoed/
- Internetiturvalisuse test (eesti keele valik olemas)
- https://cybersecuritymonth.eu/references/quiz-demonstration/welcome-to-the-network-and-information-security-quiz
- Kas minu parool on lekkinud https://haveibeenpwned.com/

Kasutatud allikad

Arvutiviirus

Allikas: https://et.wikipedia.org/wiki/Arvutiviirus

Kurivara

Allikas: https://et.wikipedia.org/wiki/Kurivara

Trooja hobune. Allikas:

https://et.wikipedia.org/wiki/Trooja_hobune_(informaatika)

ANDMEKAITSE JA INFOTURBE LEKSIKON (https://akit.cyber.ee/)