Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakute mõistmise ja nendega toimetuleku ülevaade

Küberrünnakutega toimetulemine

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu
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.

CyberPhish
Safeguarding your digital future

Õppe-eesmärgid

Selgitada ja mõista, kuidas küberrünnakutega toime tulla.

Saada aru, kuidas saaks küberrünnakuid vältida või kahju minimeerida.

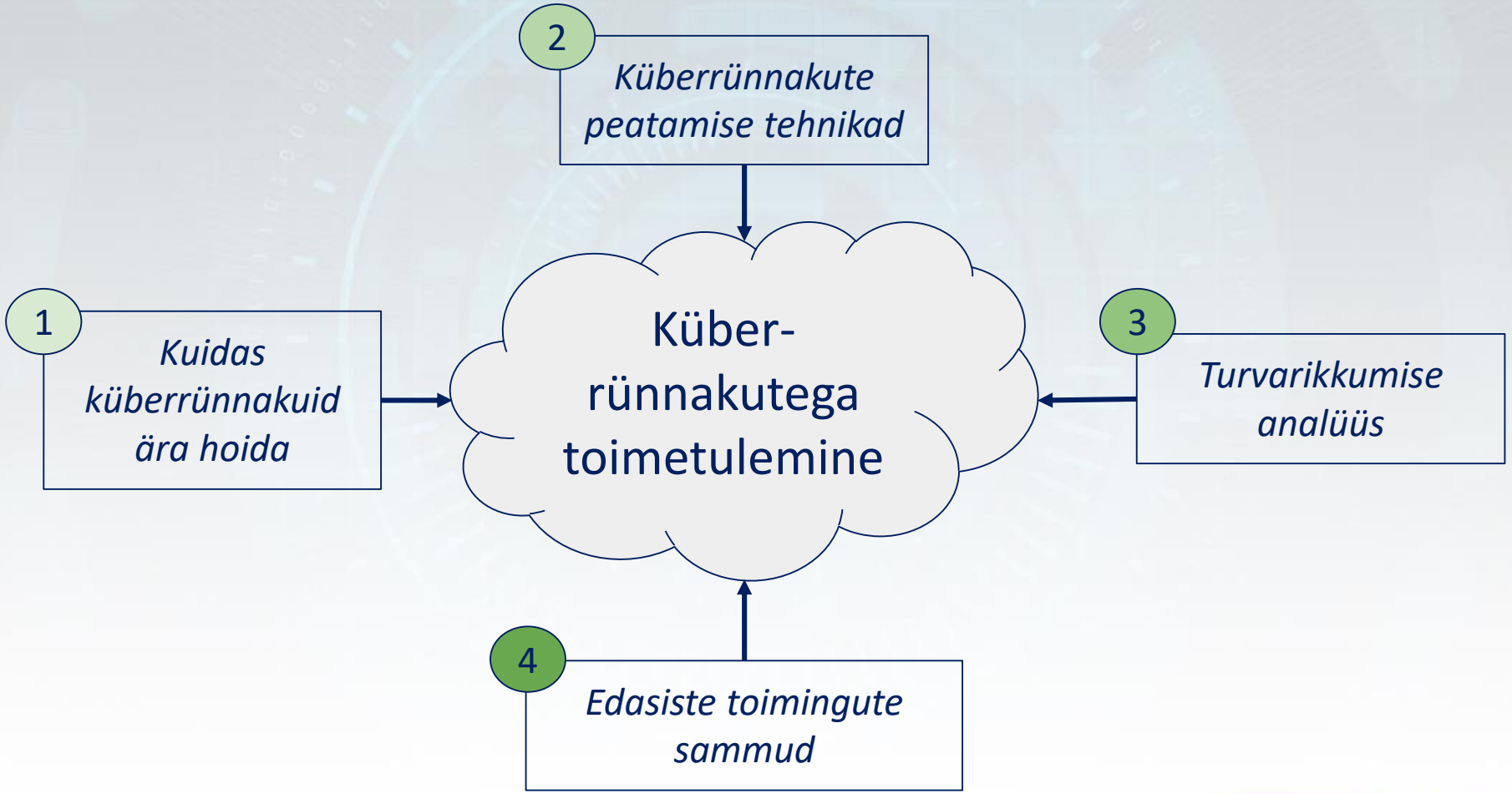
Õpilase töökoormus

Loengud	5 h
Audio- ja videomaterjal	2 h
Juhtumiuuringud	2 h
Lisalugemine	4 h
Eksamiks valmistumine	2 h

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Loenguteemad



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Kuidas küberrünnakuid ära hoida

Kõige tõhusam viis küberrünnakute vastu võitlemiseks on sobivate ennetus (ehk *kaitse*) meetmete kasutamine.

Pole edukat rünnakut - pole kaotusi.

Rünnaku vältimiseks või leevendamiseks peate kujundama mõned harjumused, mida sageli nimetatakse turvahügieeniks või küberhügieeniks.

Kui teie ja teie töötajad järgite turvahügieeni, võib küberrünnaku ohvriks langemise tõenäosust vähendada vähemalt 90 protsenti!

Funded by the Erasmus+ Programme of the European Union

Teadlikkuse tõstmise koolitus

- Esimene ja üks olulisemaid näpunäiteid küberrünnakutega toimetulemiseks on teadlikkuse tõstmise koolitus.
- See tagab, et kõik töötajad vastavalt oma ametikohtadele või kodanikud saavad küberintsidentidega hakkama.

- Koolitus on ka üks peamisi vahendeid riski vähendamiseks.
- Koolitused ei taga 100% turvalisust, kuid võivad riski oluliselt vähendada.

Funded by the Erasmus+ Programme of the European Union

Parimad tavad küberrünnakute vältimiseks

1. Ülevalt alla poliitika teie turvaasendi parandamiseks.

Parimaid tavasid peavad alati toetama õiged poliitikad. See tähendab, et küberturvalisus peaks olema ettevõtte juhtimise lahutamatu osa.

2. Alt-üles tavad küberturbemeeskondade jaoks.

Hästi väljatöötatud poliitikate abil saab küberrünnakute ärahoidmiseks, piiramiseks või leevendamiseks kasutusele võtta mitmeid tavasid.

3. Võtta kasutusele ennetavad meetmed arenenud küberohtude tuvastamiseks ja neile reageerimiseks.

Võib-olla on kõige olulisem parim tava küberturvalisusele ennetav lähenemine.

Funded by the Erasmus+ Programme of the European Union

Võimaliku rünnakuga toimetulemise sammud

- *1. samm: Uurige, millised on kõige tavalisemad küberohud*
- *2. samm: Astuge samme küberturvalisuse režiimi tõstmisek*
- *3. samm: Hinnake riskipositsiooni*
- *4. samm: Töötage välja kaitse- ja tuvastamismeetmed*
- *5. samm: Koostage situatsiooniplaanid*
- *6. samm: Taasteplaan*

Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakute vältimine

- Küberrünnaku vältimiseks on tungivalt soovitatav järgida alltoodud same:

1. Koolitage oma töötajaid.

- Üks tõhusamaid viise küberrünnakute ja igasuguste andmerikkumiste vastu võitlemiseks on oma töötajate koolitamine.

- Andmepüügi vältimiseks peavad nad:

Kontrollima linke enne nende klõpsamist

Kontrollima saabunud meilide e-posti aadresse

Enne tundliku teabe saatmist kasutama tervet mõistust. Enne „päringu" täitmist on parem kontrollida kõnealuse isiku palvet telefonikõne teel.

Funded by the Erasmus+ Programme of the European Union

Küberrünnakute vältimine

- Küberrünnaku vältimiseks on tungivalt soovitatav järgida alltoodud same:

2. Hoidke oma tarkvara ja süsteemid täielikult uuendatuna.

– sageli kasutavad häkkerid ära tarkvara nõrkusi, mis häkkerite kogukonnale teatavaks said varasemalt;

- on nutikas investeerida turvauuenduste automaatse halduse süsteemi;

- Kihiline turvalisus ja hea tarkvara uuendussüteem on osa turbelahendusest.

Funded by the Erasmus+ Programme of the European Union

Küberrünnakute vältimine

- Küberrünnaku vältimiseks on tungivalt soovitatav järgida alltoodud same:

3. Tagage lõpp-seadme kaitse.

- Lõpp-seadme kaitse kaitseb võrke, mis on seadmetega kaugsillatud. Ettevõtte võrkudega ühendatud mobiilseadmed, tahvelarvutid ja sülearvutid võimaldavad juurdepääsu turvatud materjalidele ja ligipääsu turvanõrkustele.

4. Paigaldage tulemüür.

- võrgu tulemüüri taha panemine on üks tõhusamaid viise, kuidas end väliste küberrünnakute eest kaitsta.

Funded by the Erasmus+ Programme of the European Union

Küberrünnakute vältimine

- Küberrünnaku vältimiseks on tungivalt soovitatav järgida alltoodud same:

5. Andmete varundus

- Katastroofi korral (võib olla põhjustatud küberrünnakust) peab teil olema koopia oma andmetest.

6. Kontrollige juurdepääsu oma süsteemidele

- Rünnakud võivad olla füüsilised.

– Oluline on kontrollida, kes teie võrgule juurde pääseb.

Küberrünnakute vältimine

- Küberrünnaku vältimiseks on tungivalt soovitatav järgida alltoodud same:

7. Wi-Fi turvalisus.

- ärge unustage seadistada iga kasutatava WiFi-ühenduse jaoks parooli.

8. Igale töötajale isiklikud kontod.

- iga töötaja peab kasutama isiklikku kontot;

- konto jagamine tuleb keelata.

Funded by the Erasmus+ Programme of the European Union

Küberrünnakute vältimine

- Küberrünnaku vältimiseks on tungivalt soovitatav järgida alltoodud same:

9. Juurdepääsu haldamine

- töötajatel peab olema installitud ainult volitatud tarkvara;

- volitamata tarkvara kasutamine tuleb keelata.

Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakute vältimine

Näpunäiteid turvalisuse suurendamiseks.:

1. Vähendage andmeedastust ja tarbetut suhtlust;

2. Jälgige küberturvalisuse maastikku;

3. Uurige andmete lekete kohta;

4. Töötage välja ja rakendage juhtumitele reageerimise plaan.

Neid kõiki pole lihtne iga päev jälgida, kuid peate nende peale mõtlema.

Funded by the
Erasmus+ Programme
of the European Union

Küberrünnakute vältimine

Kui järgite neid juhiseid, vähendate oluliselt küberrünnakute ohtu.

Aga ärge unustage:

- Võib olla raske teada, kus on nõrgimad kohad.

- Internetis on nii palju teavet, mis mõnikord on isegi vastuoluline.

- Teil on vaja teile sobivat lahendust.

Funded by the
Erasmus+ Programme
of the European Union

Turvaline Interneti sirvimine

- Veebi sirvimise ajal võite koguda nuhkvara, laadida alla pahavara või isegi külastada pettuslikke saite.
- Sageli ei pruugi te olla teadlik, et teete midagi ohtlikku.
- See ei tähenda, et peaksite kartma iga kord, kui klõpsate mis tahes lingil.
- Mõned lihtsad ettevaatusabinõud aitavad teil sirvimise ajal oluliselt turvalisemalt olla.

Funded by the Erasmus+ Programme of the European Union

Turvaline Interneti sirvimine

- **Arvuti kaitsmine pahatahtlike saitide eest:** igal veebilehitsejal on turvafunktsioonid, mis kaitsevad teid pahatahtlike saitide külastamise eest. Luba need funktsioonid !

- **Veebilehitseja ajakohasena hoidmine:** regulaarselt luuakse uut pahavara ja andmepüügiohte. Oluline on hoida veebilehitsejat uuendatuna.

- Veenduge, et teil oleks veebilehitseja uusim versioon.

- Veenduge, et olete installinud kõik viimased värskendused.

Funded by the Erasmus+ Programme of the European Union

Turvaline Interneti sirvimine

- **Domeeni kontrollimine**: Pahatahtlikud saidid kasutavad sageli petlikke domeene, et meelitada kasutajaid uskuma, et nad on seaduslikul saidil. Enamikul veebilehitsejatel on funktsioonid, mis võimaldavad domeeni kontrollida, või saate domeeni kontrollimiseks kasutada spetsiaalseid veebisaite (vähem mugav).

- **Laadige alla ainult usaldusväärsetelt saitidelt**: üks lihtsamaid viise, kuidas pahavara, nuhkvara ja reklaamvara teie arvutile juurde pääseb, on allalaadimine:

- Olge vabavara suhtes ettevaatlik;
- Vältige ebaseaduslikke allalaadimisi;
- Olge P2P-failide jagamisel ettevaatlik.

Funded by the Erasmus+ Programme of the European Union

Turvaline Interneti sirvimine

- **Tühjendage oma vahemälu regulaarselt**

- Veebilehitseja saab kiirendada lehe kuvamise aega, laadides lehti vahemälust.

- Kiire Interneti-ühenduse korral ei pruugi te erinevust märgata.

- Vahemälu võib aja jooksul ruumi võtta, mistõttu teie veebilehitseja aeglustub.

Hea mõte on vahemälu regulaarselt tühjendada, et vabastada arvutis ruumi ja ... eemaldada võimalikud pahatahtlikud failid.

Funded by the Erasmus+ Programme of the European Union

Turvaline Interneti sirvimine

- **Blokeerige hüpikaknad**
  - Hüpikaknad on väikesed brauseriaknad, mis ilmuvad automaatselt teatud saitide külastamisel.
  - Hüpikaknad võivad olla osa saidi seaduslikust toimimisest.
  - Mõned hüpikaknad võivad sisaldada pahavara.

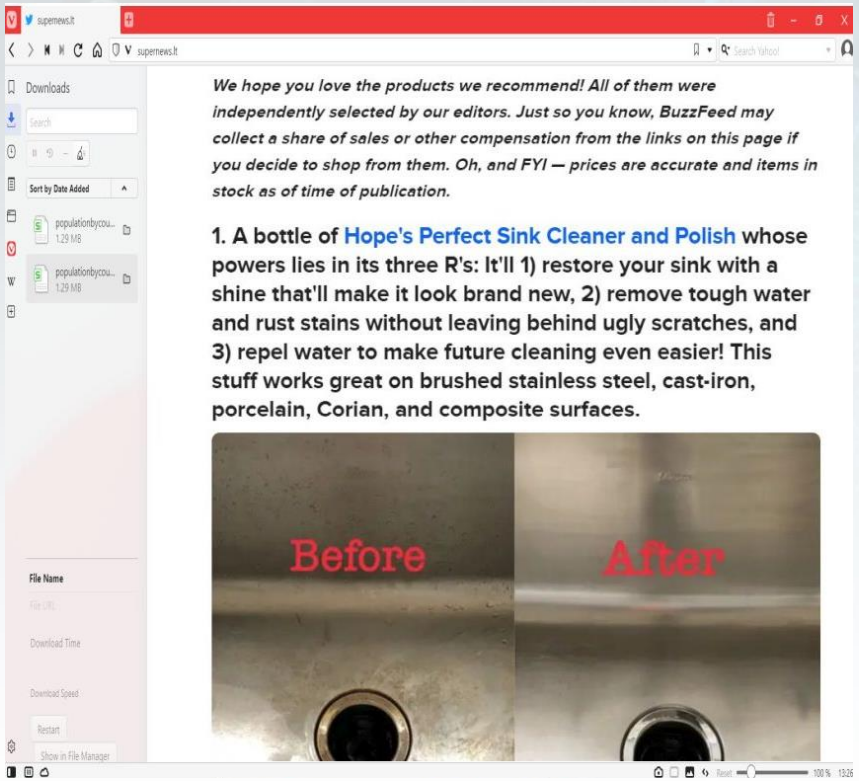
- **Hüpikaknad on hea mõte blokeerida**

Enamikul veebilehitsejatel on spetsiaalsed hüpikakende blokeerijad.

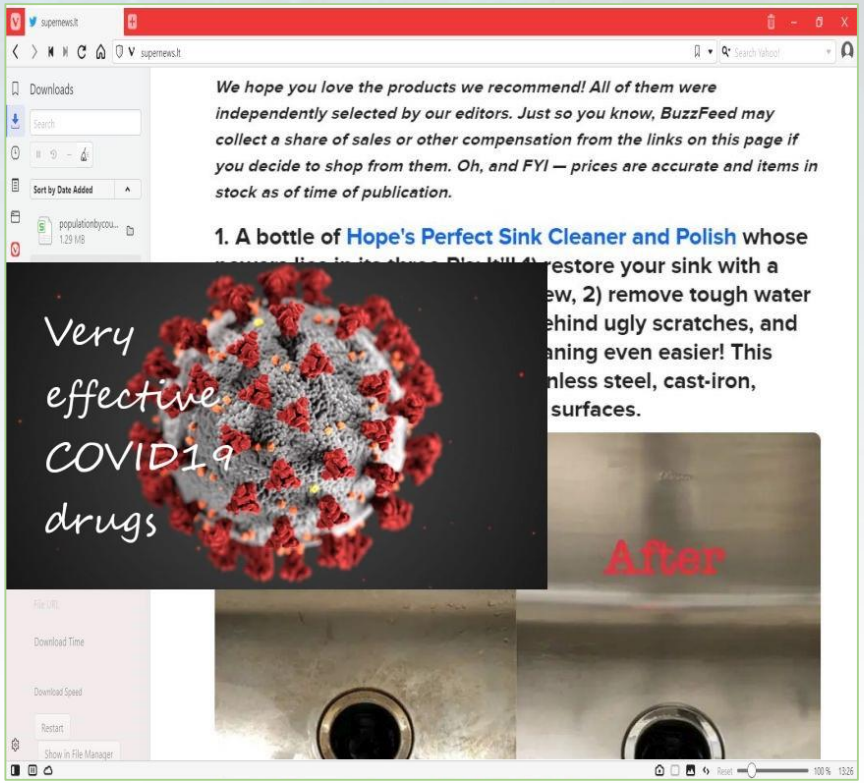
Funded by the Erasmus+ Programme of the European Union

Turvaline Interneti sirvimine:
näited hüpikakendega ja ilma hüpikaknata

Mary blocked pop ups



Jane not ...



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Turvatarkvara installimine

- **Turvatarkvara on küberruumis turvalise töötamise oluline element .**

- Pööra erilist tähelepanu:

1. Installige Interneti-turvatarkvara;
2. Installige tulemüür;
3. Loo alglaadimisketas;
4. Konfigureerige ranged veebilehitseja ja e-posti turvaseaded;
5. Ärge installige/käivitage tundmatuid programme;
6. Keela peidetud failinimelaiendid.

Funded by the Erasmus+ Programme of the European Union

Kuidas teie sirvimistegevust jälgitakse?

- Mõned veebisaidid (Amazon, eBay, Netflix ja paljud teised) koguvad andmeid teie eelistuste kohta: nad soovivad soovitada tooteid, mis teile võiksid meeldida.
- Google jälgib ja analüüsib tegevust, et pakkuda ettevõtetele statistilisi andmeid.
- Mõned valitsused koguvad andmeid teie veebitegevuse kohta, kui seda on vaja kriminaaluurimise või riikliku julgeoleku eesmärkidel.
- **Mõned kurjategijad võivad proovida ka teie tegevust jälgida**.

- Ohutu sirvimisharjumuste kujundamiseks on oluline sellest jälgimisest teadlik olla.

Funded by the Erasmus+ Programme of the European Union

Tugevate paroolide loomine

Parool - tavaliselt peamine tööriist, mis tagab teie turvalisuse kaasaegsetes IT-süsteemides.

Parool peab olema tugev, et tagada kõrge turvalisuse tase.

Milline on tugev parool?

Tugev parool on selline, mida teil on lihtne meeles pidada, kuid teistel on seda raske ära arvata.

Funded by the Erasmus+ Programme of the European Union

Soovitused tugevate paroolide loomiseks

Halb praktika: on kasutada iga konto jaoks sama parooli.

Põhjus: kui keegi avastab teie ühe konto parooli, võivad kõik teised teie kontod olla haavatavad.

Soovitus: on kasutada paroolis numbreid, sümboleid ja nii suur- kui ka väiketähti. See raskendab parooli häkkimist toore jõu rünnaku abil ja selle äraarvamist.

Funded by the Erasmus+ Programme of the European Union

Soovitused tugevate paroolide loomiseks

Halb praktika: isikuandmete, nagu teie nimi, sünnipäev, kasutajanimi või e-posti aadress, kasutamine.

Põhjus: seda tüüpi teave on sageli avalikult kättesaadav, mis muudab teie parooli äraarvamise lihtsamaks.

Kasutage pikka parooli
Rusikareegel: mida pikem on parool, seda parem (aga seda on ka raskem meeles pidada). Kuigi lisaturvalisuse huvides peaks see olema veelgi pikem.

Funded by the Erasmus+ Programme of the European Union

Soovitused tugevate paroolide loomiseks

Halb praktika: kasutada sõnastikus leiduvaid sõnu.

Põhjus: paljud häkkimistööriistad teevad nn sõnavarapõhiseid rünnakuid. Kõigepealt proovige kontrollida tuntud sõnu sõnavaras.

Näiteks **player2002** oleks nõrk parool (sõnavarast ja sünniaastat tähistav number).

Juhuslikud paroolid on kõige tugevamad. Mõelge parooligeneraatori ja paroolihalduri kasutamisele.

Funded by the Erasmus+ Programme of the European Union

*Levinud paroolipr*obleemid

Kõige sagedamini kasutatavad paroolid põhinevad perekonnanimedel, hobidel või lihtsalt mustril. Lihtne meelde jätta, aga ka kergesti ära arvata.

Mõned näited halbade paroolide kohta

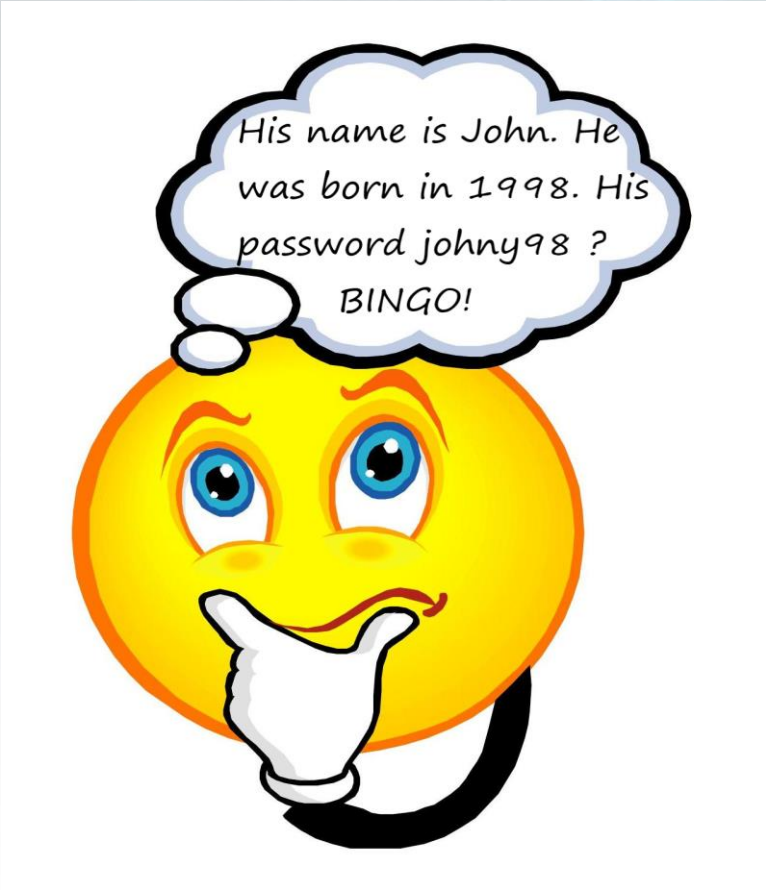
Parool: nick1995 , katie1997

Probleem: näeb välja pikk, kuid kergesti äraarvatav, sest nende sünniaastatega kasutatakse kahte nime (poiss-sõber ja tüdruksõber). Lihtne ära arvata, kui tead sihtmärkide kohta teavet.

Lahendus: sisesta juhuslikud sümbolid, kasuta suur- ja väiketähtede kombinatsioone, nt. **ni%k199o , K$tie199x**

Funded by the Erasmus+ Programme of the European Union

Soovitused tugevate paroolide loomiseks



*Levinud paroolipr*obleemid

Parool: w@kLx

Probleem: näeb välja juhuslik ja raskesti ära arvatav, kuid sisaldab ainult 5 sümbolit. Liiga lühike...

Lahendus: tugevam versioon peab olema palju pikem, soovitavalt vähemalt 10 sümbolit.

Parool: 123abc456cba789

Probleem: lihtne meelde jätta, kuid kasutatud sümbolite kombinatsiooni kontrollitakse esimeste seas

Lahendus: juhusliku parooli generaator, e. g. #eV$pIg&qf

Funded by the Erasmus+ Programme of the European Union

*Levinud paroolipr*obleemid

Parool: Gmail Bd458$%Kl!df; eBay Bd458$%Kl!df; Amazon: Bd458$%Kl!df

Probleem: parool on OK, kuid selle kasutamine erinevatel saitidel on halb tava.

Lahendus: kasutage iga saidi jaoks erinevaid paroole.

Selle asemel, et paroolid paberile kirjutada, saate nende turvaliseks salvestamiseks kasutada paroolihaldurit.

Paroolihaldurid saavad teie parooli erinevatel veebisaitidel meeles pidada ja sisestada, mis tähendab, et te ei pea pikemaid paroole meeles pidama.

Funded by the Erasmus+ Programme of the European Union

Mitmefaktoriline autentimine

Mitmefaktoriline autentimine (MFA) on veelgi parem viis tundlike andmete kaitsmiseks.

Mis on mitmefaktoriline autentimine?

Mitmefaktoriline autentimine on kontrollimeetod, mille puhul on vaja vähemalt kahte erinevat tõendamistegurit.

MFA-d nimetatakse mõnikord 2FA-ks (kahefaktoriline autentimine).

Põhimõtteliselt lisab see täiendava turvakihi.

Funded by the Erasmus+ Programme of the European Union

Mitmefaktorilise autentimise tüübid

Üldiselt on tunnustatud kolme tüüpi autentimisfaktoreid:

Tüüp 1: Midagi, mida tead – sisaldab paroole, PIN-koode, koodisõnu jne.

Tüüp 2: Midagi, mis teil on – hõlmab kõiki objekte, mis on füüsilised objektid (võtmed, nutitelefonid, kiipkaardid, USB-draivid).

Tüüp 3: Midagi mis sa oled – sisaldab biomeetrilisi andmeid (sõrmejäljed, peopesa skaneerimine, näotuvastus, võrkkesta skaneerimine, vikerkesta skaneerimine, häälekinnitus).

Mitmefaktoriline autentimine

Kombineerides nendest kolmest kategooriast vähemalt kaks tegurit, saame mitmefaktorilise autentimise.

Mitmefaktoriline autentimine on sissetungijal palju keerulisem ületada.

Mitmefaktorilise autentimise korral peab ründajal olema rohkem oskusi ja ta peab suutma sooritada mitut rünnakut korraga.

Väga sageli on see äärmiselt raske.

Tuntud näide mitmefaktorilisest autentimisest, mis toetab teenus, on PayPal, Google, Microsoft jne.

Funded by the Erasmus+ Programme of the European Union

Populaarsed mitmeteguri lise autentimise tööriistad

Saadaval on palju mitmefaktorilise autentimise tööriistu.

Levinud autentimisrakendused leiate oma mobiilseadme rakenduste poest:

Google Authenticator;

LastPass Authenticator;

Microsoft Authenticator;

Authy;

ja paljud teised.

Failide krüpteerimine

Mis on faili krüpteerimine?

Failide krüpteerimine on andmete kodeerimise meetod failide turvaliseks edastamiseks.

Mida teeb faili krüpteerimine?

Failide krüpteerimine aitab vältida rikkumist või volitamata juurdepääsu.

Kuidas ile Encyption töötab?

Töötab saadetavate andmete hägustamisena keeruliste algoritmide abil.

Funded by the
Erasmus+ Programme
of the European Union

Failide krüpteerimine

Tähtis:

failis sisalduvale teabele juurdepääsuks peab teil olema võti!

Funded by the
Erasmus+ Programme
of the European Union

Kuidas faile krüpteeritakse

Kaks kõige populaarsemat krüpteerimisstandardit on:

Open PGP – võimaldab avalike ja privaatvõtmete abil faile krüptida ja dekrüpteerida.

ZIP koos AES-iga – failide tihendamine ja krüptimine AES-krüptimisega ZIP- ja GZIP-standardeid kasutades.

Funded by the Erasmus+ Programme of the European Union

Miks kasutada failide krüpteerimistarkvara

- Kihiline andmekaitse

- Turvalisus paljudes seadmetes

- Andmeedastus on turvatud

- Ausus säilinud

- Tagatud vastavus

Funded by the
Erasmus+ Programme
of the European Union

Kuidas valida krüpteerimistarkvara

- Milliseid krüpteerimisstandardeid peate toetama?

- Kui tundlikud on andmed?

- Kas vahetatakse suuri faile?

- Kas failid tuleks krüpteerida või ühendus krüpteerida?

- Kuidas andmeid edastatakse?

Funded by the
Erasmus+ Programme
of the European Union

Kodeerimistarkvara

- AxCrypt Premium
- Folder Lock
- CryptoForge
- NordLocker
- Steganos Safe

Nõuanded küberrünnaku tuvastamiseks

Kui olete juba kahtlase meili või lingi avanud, kontrollige järgmisi asju:

- *Ebatavaline tegevus teie seadmes või võrgus.*
- *Kahtlustate parooli kasutamist teie kontol.*
- *Tuvastage kahtlased hüpikaknad.*
- *Jälgige tavalisest aeglasemat võrku.*
- *Hoidke tarkvara ajakohasena.*
- *Ootamatud või äkilised muutused vabas kettaruumis või mälus.*

Funded by the Erasmus+ Programme of the European Union

Näpunäited turvaliseks veebiostlemiseks

- Internetis ostlemine on väga mugav ja sageli ökonoomne viis millegi ostmiseks.
- Kuid ka väga ohtlik: FBI Interneti-kuritegevuse kaebuste keskus (IC3) leidis, et pool 2019. aasta küberkuritegevusest oli seotud veebiostudega.
- Mujal pole olukord parem.
- Erinevad väärkäitumise allikad:
  - Ohver ei ole saanud kaupa;
  - Pettur ei ole kauba eest tasunud;
  - Eesmärk varastada tundlikke andmeid, eelkõige finantsandmeid, nt. g. krediitkaardi andmed.

Funded by the Erasmus+ Programme of the European Union

Näpunäited turvaliseks veebiostlemiseks

- **1. nõuanne: kasutage ainult tuttavaid või usaldusväärseid veebipoode**

- See on ettevaatusabinõu number üks;

- Uurige klientide arvamust veebipoe kohta;

- Vaata, kui kaua pood on aktiivne (tavaliselt mida kauem on aktiivne, seda usaldusväärsem);

- Proovige vältida poodide kasutamist, millest olete kuulnud hüpikreklaamidest või meilireklaamidest;

- Teatage küberkuritegevusest, kui tundsite end ohvrina!

Funded by the Erasmus+ Programme of the European Union

Näpunäited turvaliseks veebiostlemiseks

- **2. nõuanne: ärge kunagi ostke midagi veebist, kasutades oma krediitkaarti saidilt, kuhu pole installitud SSL-i (secure sockets layer) turvalisust**

– saidil on SSL, kuna saidi URL algab HTTPS-iga mitte ainult HTTP-ga;

– ilmub lukustatud tabaluku ikoon, tavaliselt aadressiribal või alloleval olekuribal URL-ist vasakul;

– HTTPS on nüüd peaaegu standardne kõigil veebilehekülgedel.

Funded by the Erasmus+ Programme of the European Union

Näpunäited turvaliseks veebiostlemiseks

3. Nõuanne: ärge jagage isiklikku teavet rohkem kui minimaalselt vaja

- ükski veebipood ei vaja teie isikukoodi, passiandmeid vms;
- teie krediitkaardi andmed peab teie pank Internetis kinnitama;
- luba oma e-pangas turvaline ostuvõimalus;
- registreerimata ostjaks olemisel on turvalisuse seisukohast sageli eeliseid.

Pidage meeles: mida vähem pettur teist teab, seda keerulisem on teid häkkida.

Funded by the Erasmus+ Programme of the European Union

Näpunäited turvaliseks veebiostlemiseks

4. nõuanne: Kaitske oma kontot

- kasutage tugevaid paroole (vt eespool);
- vahetage regulaarselt paroole (ainult 25% inimestest teeb seda, kui seda ei nõuta);
- kasutada erinevatel ostuplatvormidel erinevaid paroole;
- võimalusel kasutada mitmefaktorilist autentimist;
- kasutada pahavaratõrjet;
- vältige ostlemist mitte-privaatse arvutiga.

Funded by the Erasmus+ Programme of the European Union

Näpunäited turvaliseks veebiostlemiseks

- **5. nõuanne: mõelge mobiilselt**

- ärge kartke ostelda mobiilirakendusi kasutades: need pole vähem turvalised kui lauaarvutis ostlemine;

- kuid kasutage ainult jaemüüja või muu veebipõhise ostuplatvormi pakutavaid rakendusi;

- avalikus kohas makse sooritades peitke oma seadme ekraan;

- kaitske oma mobiilseadet korralikult.

Pidage meeles: turvaliselt ostledes või avalikult makstes peate mõtlema natuke nagu pahalane.

Funded by the Erasmus+ Programme of the European Union

Näpunäited turvaliseks veebiostlemiseks

- **6. nõuanne: jäta kaart vahele, kasuta telefoni**

- kaupade eest tasumine nutitelefoniga on standardiseeritud;

– on tegelikult veelgi turvalisem kui krediitkaardi kasutamine;

- mobiilimaksete rakendused, nagu Apple Pay, genereerivad ostu jaoks ühekordselt kasutatava autentimiskoodi, mida keegi teine ei saaks kunagi varastada ja kasutada;

- teil ei pea krediitkaarti kaasas olema: see on ka ettevaatusabinõu !

Funded by the Erasmus+ Programme of the European Union

Küpsistega tegelemine

- Küpsised on kaasaegse Interneti oluline element, kuid haavatavus teie privaatsuse suhtes.
- Küpsised aitavad veebiarendajatel pakkuda teile isiklikumaid ja mugavamaid veebisaitide külastusi.
- Küpsised jätavad veebisaitidele meelde teid, teie veebisaidi sisselogimisi, ostukorvi ja palju muud. Kuid need võivad kurjategijatele luuramiseks olla ka privaatse teabe varakamber.

- Isegi põhiteadmised küpsistest võivad aidata teil Interneti-tegevusest soovimatuid pilke eemal hoida.

Funded by the Erasmus+ Programme of the European Union

Mis on küpsised?

- **Lihtsustatud kujul**: küpsised on tekstifailid, mis sisaldavad andmeid (nt kasutajanimi ja parool)
- Neid kasutatakse teie tuvastamiseks Interneti-kasutajana.
- HTTP-küpsiseid kasutatakse konkreetsete kasutajate tuvastamiseks ja sirvimise mugavuse suurendamiseks.

- Küpsisesse salvestatud andmed loob server teie ühenduse loomisel. Need andmed on märgistatud teile ja teie arvutile ainulaadse ID-ga.
- Server loeb ID-d ja teab, millist teavet teile konkreetselt edastada.

Funded by the Erasmus+ Programme of the European Union

Küpsiste tüübid

Kaks peamist tüüpi:

- Magic Cookies

- HTTP Cookies

- **Magic cookies** on termin, mis viitab teabepakettidele, mis saadetakse ja võetakse vastu muudatusteta.
- **Kõige sagedamini kasutatakse arvuti andmebaasisüsteemidesse, näiteks ettevõtte sisevõrku, sisselogimiseks.**

Funded by the Erasmus+ Programme of the European Union

Küpsiste tüübid

Kaks peamist tüüpi:

- Magic Cookies
- **HTTP Cookies**

- **HTTP cookies** on Interneti-sirvimiseks loodud magic cookie muudetud versioon.
- **HTTP cookie** kasutatakse teie veebikogemuse haldamiseks.
- Pahatahtlikud inimesed saavad neid kasutada teie võrgutegevuse järele luuramiseks ja isegi teie isiklike andmete varastamiseks.

Funded by the Erasmus+ Programme of the European Union

Milleks küpsiseid kasutatakse?

- **Seansi juhtimine.** Näiteks võimaldavad küpsised veebisaitidel kasutajaid ära tunda ja meelde tuletada nende individuaalseid sisselogimisandmeid ja eelistusi, näiteks spordiuudised versus poliitika.

- **Isikupärastamine.** Kohandatud reklaam on peamine viis, kuidas küpsiseid kasutatakse teie seansside isikupärastamiseks.

- **Jälgimine.** Ostusaidid kasutavad küpsiseid kasutajate varem vaadatud kaupade jälgimiseks, võimaldades saitidel soovitada muid kaupu, mis neile meeldida võivad, ja hoida tooteid ostukorvis, kuni nad ostlemist jätkavad.

Funded by the Erasmus+ Programme of the European Union

Erinevat tüüpi HTTP-küpsised

- **Seansiküpsiseid** kasutatakse ainult veebisaidil navigeerimise ajal. Need salvestatakse muutmälus ja neid ei kirjutata kunagi kõvakettale. Seansi lõppedes kustutatakse seansi küpsised automaatselt.

- **Püsiküpsised** jäävad arvutisse määramata ajaks, kuid sageli sisaldavad paljud küpsised aegumiskuupäeva ja need kustutatakse pärast etteantud perioodi.

Funded by the
Erasmus+ Programme
of the European Union

Persistent Cookies

- Püsiküpsiseid kasutatakse kahel peamisel eesmärgil:

- **Autentimine**: jälgige, kas kasutaja on sisse logitud ja mis nime all. Samuti lihtsustavad need sisselogimisteavet, nii et kasutajad ei pea saidi paroole meeles pidama.

- **Jälgimine**: jälgige aja jooksul mitut sama saidi külastust.

Funded by the Erasmus+ Programme of the European Union

Kuidas saavad küpsised ohtlikud olla

- Kuna küpsistes olevad andmed ei muutu, ei ole küpsised ise kahjulikud.
- Mõned küberrünnakud võivad aga kaaperdada küpsiseid ja oamndada juurdepääsu teie sirvimisseanssidele.
- Oht seisneb nende võimes jälgida üksikisikute sirvimisajalugu.
- Mõnikord võidakse neid kasutada teie arvuti pahavaraga nakatamiseks.

Funded by the Erasmus+ Programme of the European Union

First-Party vs. Third-Party Cookies

- (*First-party cookies*) Esimese osapoole küpsised loob otse teie kasutatav veebisait. Need on üldiselt turvalisemad, kui sirvite mainekaid veebisaite või veebisaite, mida pole ohustatud.

- *(Third-party cookies)* Kolmandate osapoolte küpsiseid loovad veebisaidid, mis erinevad kasutajate praegu sirvitavatest veebilehtedest, tavaliselt seetõttu, et need on lingitud sellel lehel olevatele reklaamidele.
- 10 reklaamiga saidi külastamine võib genereerida 10 küpsist, isegi kui kasutajad neil reklaamidel kunagi ei klõpsa.
- Kolmanda osapoole küpsised võimaldavad reklaamijatel või analüüsiettevõtetel jälgida üksikisiku sirvimisajalugu kogu veebis nende reklaame sisaldavatel saitidel.

Funded by the Erasmus+ Programme of the European Union

First-Party vs. Third-Party Cookies

- Zombie-küpsised on kolmanda osapoole küpsised ja püsivalt installitud kasutajate arvutitesse, isegi kui nad otsustavad küpsiseid mitte installida.
- Need kipuvad pärast kustutamist uuesti ilmuma.
- Nagu teisi kolmanda osapoole küpsiseid, saavad veebianalüütikaettevõtted kasutada zombiküpsiseid, et jälgida unikaalsete isikute sirvimisajalugu.
- Veebisaidid võivad teatud kasutajate keelustamiseks kasutada ka zombisid.

Funded by the Erasmus+ Programme of the European Union

Nõuanded küpsistega toimetulemiseks

- ELi seadus nõuab küpsiste kasutamiseks kasutaja nõusolekut. GDPR-i ja e-privaatsusdirektiivi alusel küpsiseid reguleerivate eeskirjade järgimiseks peate järgnevat tegema:
- *Saama kasutaja nõusoleku enne küpsiste kasutamist, välja arvatud hädavajalikud küpsised.*
- *Esitama täpset ja konkreetset teavet iga küpsise jälgitavate andmete ja nende eesmärgi kohta lihtsas keeles enne nõusoleku saamist.*
- *Dokumenteerima ja salvestama kasutajatelt saadud nõusolek.*
- *Lubama kasutajatel oma teenusele juurde pääseda isegi siis, kui nad keelduvad teatud küpsiste kasutamise lubamisest*
- *Muutma kasutajatele nõusoleku tagasivõtmine sama lihtsaks, nagu nende jaoks oli nõusoleku andmine.*

Funded by the Erasmus+ Programme of the European Union

Nõuanded küpsistega toimetulemiseks

- Enamik kaasaegseid brausereid võimaldavad teil hallata teie arvutisse salvestatud küpsiseid.
- Näiteks võite soovida nõustuda kõigi küpsistega, kustutada teatud veebisaidi küpsised või keelduda kõigist küpsistest.
- Peate otsima brauseri juhendit või abisüsteemi, et leida võimalusi, mida brauser küpsiste haldamiseks pakub.

Funded by the Erasmus+ Programme of the European Union

Pahavaraga tegelemine

- Pahavara on ründetarkvara, mis võimaldab ründajal omada täielikku või piiratud kontrolli sihtsüsteemi üle.
- Need võivad kahjustada või muuta süsteemis olevat teavet ja varastada teabe süsteemist.
- Pahavara on erinevat tüüpi, näiteks viirused, troojalased, ussid, juurkomplektid, nuhkvara ja lunavara.

- Pahavara võib süsteemi siseneda meilide, failiedastuste, juhusliku kolmanda osapoole tarkvara installimise või kvaliteetse viirusetõrjetarkvara mittekasutamise kaudu.

Funded by the Erasmus+ Programme of the European Union

*Erinevus **viiruse** ja **ussi** vahel*

Viirus

- kinnitub programmi või faili külge ja levib ühest süsteemist teise.
- paljundab ja käivitab ennast.
- muudab süsteemi kasutaja teadmata.
- levib programmeeritud kiirusega.

Uss

- viiruse alamklass, mis on disainilt sarnane, paljuneb ühest arvutist teise.
- kasutab nõrga turvalisusega OS-i.
- põhjustab süsteemi või võrgu toimimise lõpetamise.
- levib kiiremini kui viirus.

Funded by the Erasmus+ Programme of the European Union

Viirusetõrjetarkvara

- Viiruse- või pahavaratõrjet kasutatakse süsteemis oleva pahavara tuvastamiseks, ennetamiseks või eemaldamiseks.
- Oskab regulaarselt läbi viia süsteemi kontrolle ja uuendada süsteemi turvalisust.
- Erinevad viirusetõrjetarkvarad on turul saadaval tasuta või tasulisena.

- Viirusetõrjetarkvara mittekasutamine on "küberkuritegevuse liik"! Te ei saa mitte ainult langeda rünnaku ohvriks, vaid teie arvutit võidakse kasutada küberrünnaku vahendina.

Funded by the Erasmus+ Programme of the European Union

Näpunäiteid pahavara ennetamiseks

- Sarnane sellega, mida me varem rääkisime, kuid seda tuleb siiski meeles pidada:

- *Hoidke oma arvuti ja tarkvara ajakohasena.*
- *Kasutage võimaluse korral mitte-administraatori kontot.*
- *Mõelge kaks korda, enne kui linkidel klõpsate või midagi alla laadite.*
- *Olge ettevaatlik meilimanuste või piltide avamisel.*
- *Ärge usaldage hüpikaknaid, mis paluvad teil tarkvara alla laadida.*
- *Piirake oma failide jagamist.*

Funded by the Erasmus+ Programme of the European Union

Hinnake turvarikkumist

Kaks olulist küsimust:

- Usaldusväärsete allikate jälgimine: kui olete laiema rünnaku ohver, mis on mõjutanud mitut ettevõtet või isikut, järgige olukorra lahendamise eest vastutavate usaldusväärsete allikate soovitusi.

- Määrake kindlaks rikkumise põhjus: olenemata sellest, kas olete osa laiemast rünnakust või olete ainus ohver, peate määrama kindlaks ka rikkumise põhjuse oma konkreetses asutuses, et saaksite sama tüüpi rünnakuid kordumise ära hoida.

Funded by the Erasmus+ Programme of the European Union

Hinnake turvarikkumist

Proovige leida vastused järgmistele küsimustele:

- *Kuidas rünnak algatati?*
- *Kellel on juurdepääs nakatunud serveritele?*
- *Millised võrguühendused olid rikkumise ilmnemisel aktiivsed?*

Funded by the
Erasmus+ Programme
of the European Union

Hinnake turvarikkumist

- Näiteks võite olla võimeline tuvastama, kuidas rikkumine algatati, kontrollides oma turvaandmete logisid tulemüüri või meiliteenuse pakkujate, viirusetõrjeprogrammi või muul viisil.
- Võimalik, et peate küsima abi küberturvalisuse spetsialistidelt.
- Ärge kõhelge nõu küsimast, kui tunnete teadmiste vajakajäämist.

Funded by the Erasmus+ Programme of the European Union

Hinnake turvarikkumist

- Tehke kindlaks need, keda rikkumine mõjutab:

- - Väga oluline on välja selgitada, keda rikkumine võis mõjutada, sealhulgas teie töötajaid, kliente ja kolmandatest osapooltest tarnijaid.
- - Hinnake andmete rikkumise tõsidust, määrates kindlaks, millisele teabele (nt sünnipäevad, postiaadressid, e-posti kontod ja krediitkaardinumbrid) juurdepääs või mis sihiti.

Funded by the Erasmus+ Programme of the European Union

Hinnake turvarikkumist

- Käivitage oma küberrünnaku protokoll:

- - Teie töötajad peaksid olema teadlikud teie andmetega seotud rikkumiste eeskirjadest.
- - Pärast rikkumise põhjuse avastamist kohandage ja edastage oma turvaprotokolle, et tagada sama tüüpi intsidentide kordumine.
- - Kaaluge oma töötajate juurdepääsu andmetele piiramist nende tööülesannete alusel.

Funded by the Erasmus+ Programme of the European Union

Hallake küberrünnakute tagajärgi

Kui rünnak oli ettevõtte vastu: teavitage rikkumisest juhte ja töötajaid ning kõiki teisi, keda teie vastu suunatud rünnak mõjutada võib.

See sisaldab:

- Suhelge oma kolleegidega, et anda neile juhtunust teada.

- Määrake meeskonnaliikmetele selged volitused probleemiga suhtlemiseks nii sisemiselt kui ka väliselt.

- Andmerikkumisest taastumisel on meeskonnaga tihedas kontaktis püsimine ülioluline.

- Võimalik, et vajate õigusnõu intsidendi õiguslike aspektide kohta.

Funded by the Erasmus+ Programme of the European Union

Hallake küberrünnakute tagajärgi

Kui rünnak toimus ettevõtte vastu: teavitage rikkumisest juhte ja töötajaid ning kõiki teisi, keda teie vastu suunatud rünnak võib mõjutada.

See hõlmab:

- Kui teil on kübervastutuskindlustus, teavitage sellest oma partnerit. Kui mitte, proovige kaaluda, kas kindlustuse saamine võib olla kasulik.

- Kübervastutuskindlustus on loodud selleks, et aidata teil taastuda andmete rikkumisest või küberturvalisuse rünnakust.

- Võtke esimesel võimalusel ühendust oma operaatoriga, et näha, kuidas ta saab teid aidata pärast küberrünnakut teha.

Funded by the Erasmus+ Programme of the European Union

Hallake küberrünnakute tagajärgi

Kui rünnak oli ettevõtte vastu:

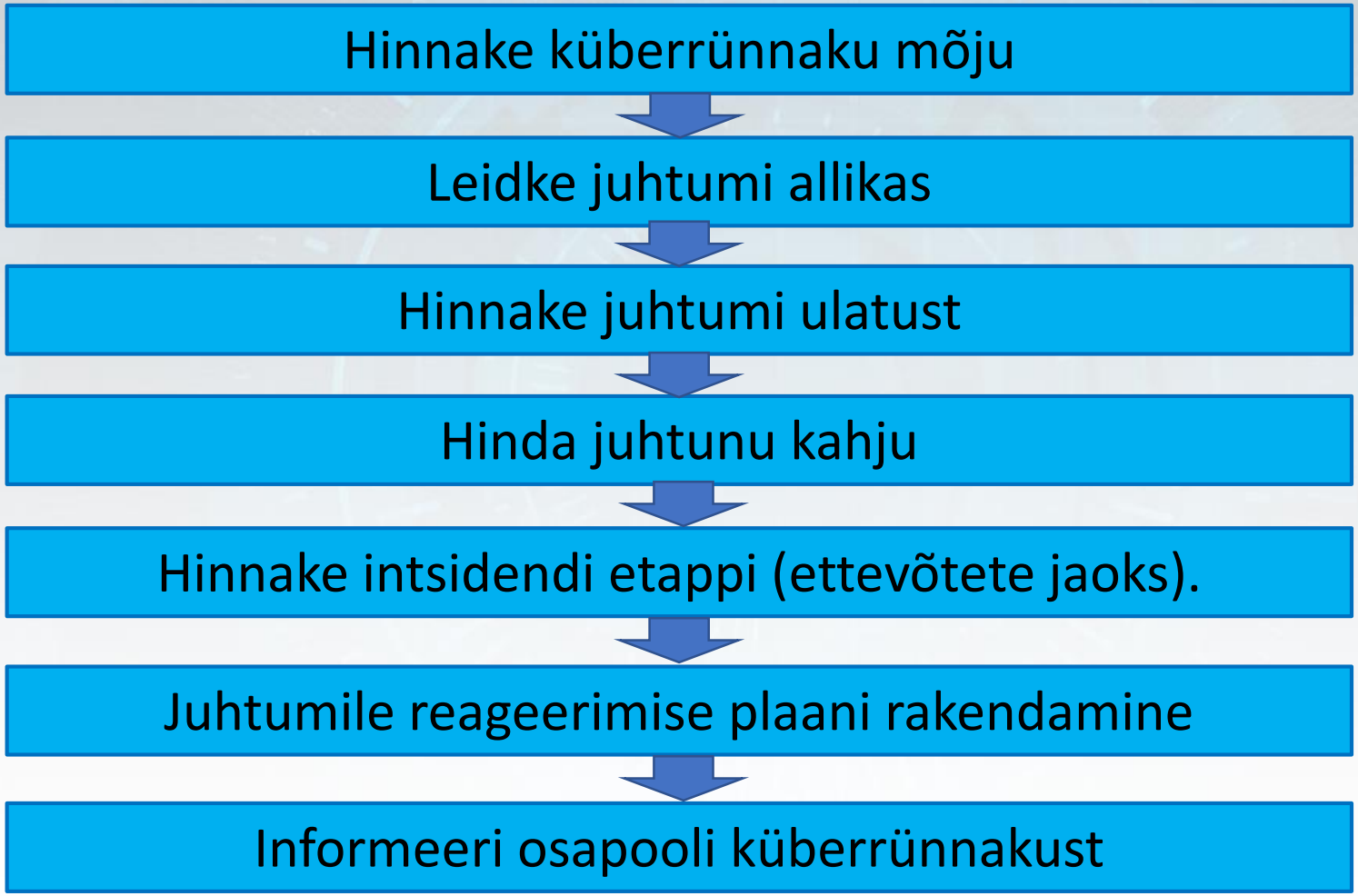
teavitada kliente

See sisaldab:

- Rõhutage oma valmisolekut olla oma klientidega läbipaistev, kaaludes spetsiaalse abitelefoni loomist, mis on mõeldud konkreetselt mõjutatud isikute küsimustele vastamiseks.

- Suhtlemine võib olla võtmetähtsusega positiivsete ja professionaalsete suhete hoidmisel oma klientidega ja võimalike kahjude minimeerimiseks.

Küberrünnaku hindamine



Küberkuritegudest teatamine

- Teatage rünnakust vastutavale asutusele:
  - Igal riigil on vastutav asutus nt CERT.
- Olenevalt küberrünnaku tüübist ning kohalikest ja rahvusvahelistest eeskirjadest võib teil olla vaja õiguskaitseasutusi teavitada.
- Kui kardate, et tundlikud finantsandmed võivad sattuda ohtu, peate võib-olla võtma ühendust oma krediitkaardiettevõttega.
- Öelge finantsorganisatsioonile, et vaidlustate petturite poolt teie kaardil tehtud volitamata tasud kui kahtlustate, et teie kaardinumbrit on ohustatud.
- Arutage finantsorganisatsiooniga edasisi tegevusi.

Funded by the Erasmus+ Programme of the European Union

Küberkuritegudest teatamine

- See on eriti oluline, kui jälgite kriminaalse tegevusega seotud tegevusi:

- näete, et see ei olnud ego häkkimise juhtum (nt noor häkker üritas end proovile panna).

- Kui avastate, et olete pettuse ohver:

- Võtke ühendust oma IT-/turvaosakonnaga, kui teil see on;
- Võtke viivitamatult ühendust oma finantsasutusega, et taotleda raha tagasivõtmist;
- Pöörduge oma tööandja poole, et teatada palgaarvestuse maksete ebakorrapärasustest.

Sammud pärast vahetu ohu eemaldamist

- Uuendage oma tarkvara. Installige vajalikud turvaparandused.
- Muutke paroole kogu süsteemis.
- Ettevaatusabinõuna muutke teiste süsteemide paroole.
- Kaheastmelise kinnitamise meetodite rakendamine haavatavatele kontodele juurdepääsuks.

- WAF-i (*veebirakenduse tulemüüri*) paigaldamine teie veebisaidi kaitsmiseks, kui olete veebisaidi administraator või teil on veebisait.
- Veenduge, et teie e-kaubanduse platvorm vastaks PCI-DSS-i (maksekaarditööstuse andmeturbe standardid) 1. taseme nõuetele.

Funded by the Erasmus+ Programme of the European Union

Mida edasi teha

- "Kuuskümmend protsenti väikeettevõtete ja isiklikest rikkumistest viimase 3 aasta jooksul on tingitud välistest teguritest. Sellest tulenevalt peaksid töötajate koolitused olema ka regulaarselt toimuvad ja kõikehõlmavad. Veenduge, et töötajad suudavad tuvastada kahtlaste e-kirjade ja manuste hoiatusmärgid ning teavad, kuidas kõigist juhtumitest teatada. Koolitage neid ka isikliku või tundlikku teavet krüpteerima.
- *Mike Tanenbaum, executive vice president and head of cyber for Chubb North America*.

Funded by the Erasmus+ Programme of the European Union

Kui teie Gmaili või Youtube'i kontole on häkitud

- Kui märkate oma Google'i kontol, Gmailis või muudes Google'i toodetes harjumatut tegevust, võib keegi teine seda ilma teie loata kasutada.

1. samm: logige sisse oma Google'i kontole

2. samm: vaadake tegevust üle ja uurige abimaterjale kuidas oma häkitud Google'i kontot kaitsta

3. samm: rakendage rohkem turvameetmeid

For more details see: https://support.google.com/accounts/answer/6294825?hl=en

Funded by the Erasmus+ Programme of the European Union

Kui teie Facebooki kontole on häkitud

Facebooki soovituste kohaselt võidi teie kontole häkkida, kui märkate:

- Teie e-posti aadress või parool on muutunud.
- Teie nimi või sünnipäev on muutunud.
- Sõbrakutsed on saadetud inimestele, keda te ei tunne.
- On saadetud sõnumeid, mida te pole kirjutanud.
- On tehtud postitusi, mida te pole loonud.

Kui arvate, et teie kontot on häkitud või üle võetud, peaksite külastama lehte: https://www.facebook.com/hacked

Funded by the Erasmus+ Programme of the European Union

Mida teha, kui teie teisele kontole on häkitud

- Seal on tohutult erinevaid süsteeme, mida saab häkkida
- Kõigi süsteemide üksikasju on võimatu esitada

- Üldised soovitused on järgmised:

- otsige nõuandeid abisüsteemist
- proovige ühendust võtta toote eest vastutava ettevõttega

Funded by the Erasmus+ Programme of the European Union

Kokkuvõte

Küberrünnakute vältimine on teostatav.

- Koolitage ja arendage teadlikkust;
- Kujundage vajalikke harjumusi;
- Kasutage sobivaid tööriistu;
- Tehke plaan, kuidas küberrünnaku korral käituda.

Ülesanne

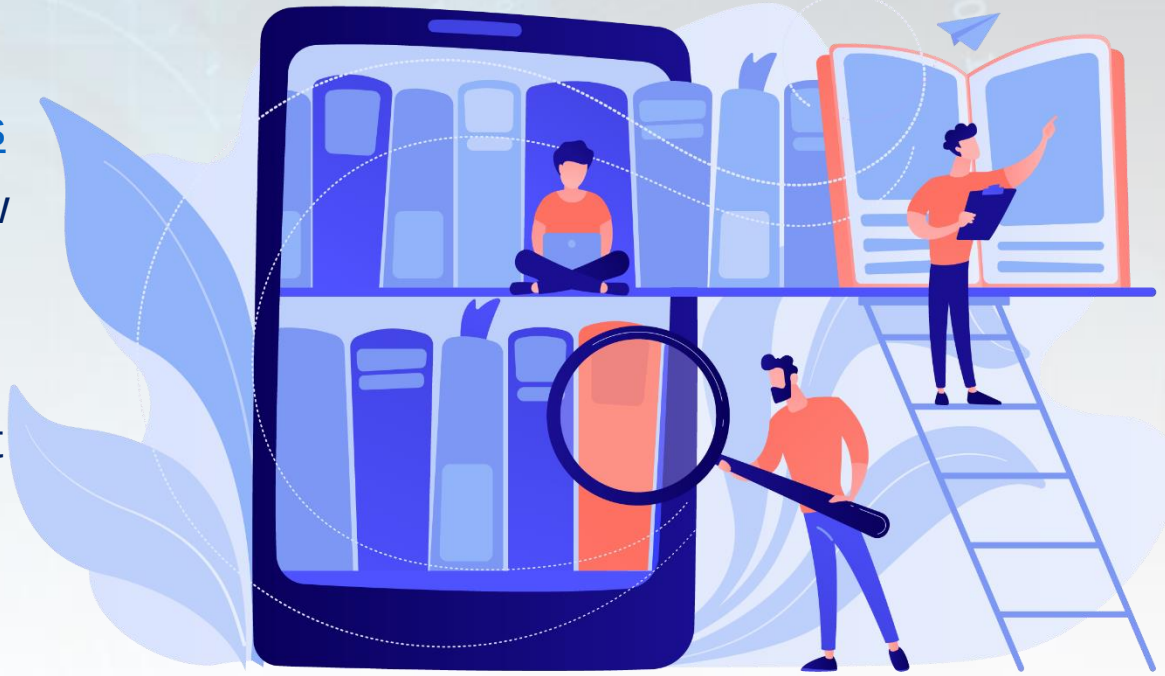
Hinnake küberturvalisuse olukorda ettevõttes

- Turvalisuse olukorra hinnang
- Kasutatud tööriistade kvaliteet
- Paroolide kvaliteet
- Reageerimisplaan
- Pärast rünnakut toimunud muudatused

Funded by the Erasmus+ Programme of the European Union

Lisalugemine

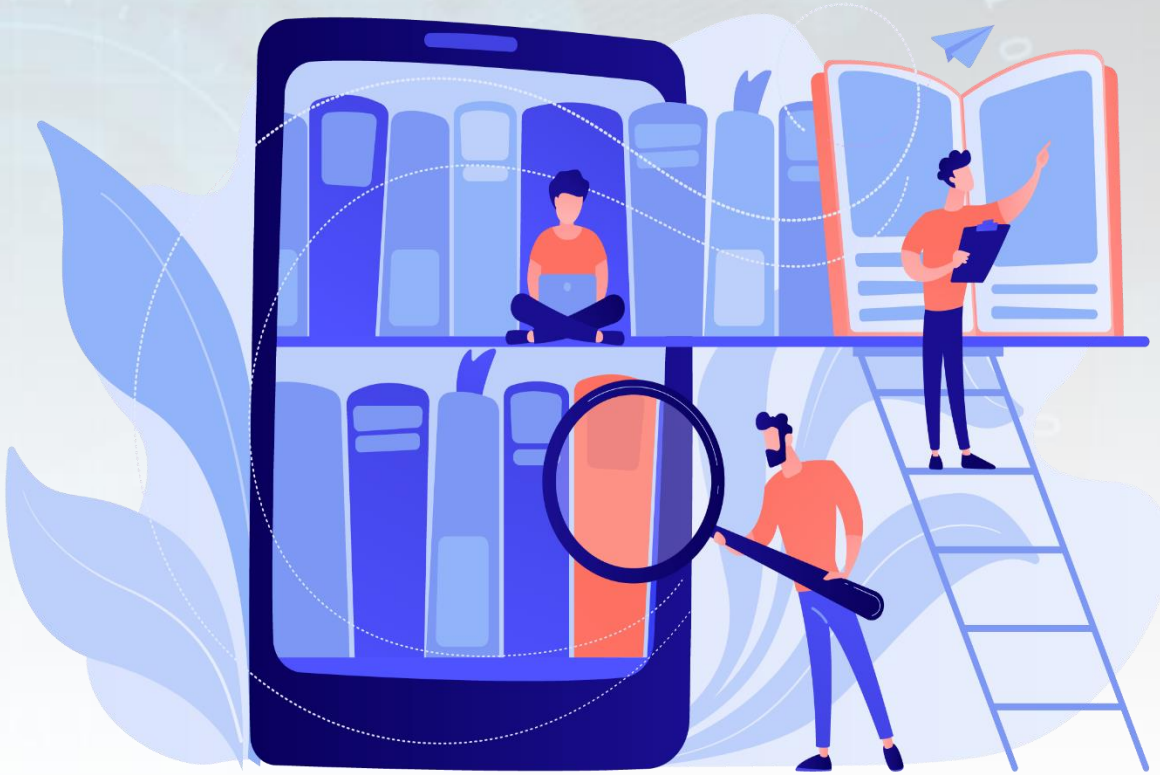
- Protect your business from cyber threats. Australian Government Guidelines. https://business.gov.au/online/cyber-security/protect-your-business-from-cyber-threats
- Yuchong Li, Qinghui Liu. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, September 2021
- Atul S Choudhary; Pankaj P Choudhary; Shrikant Salve. A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks. In Proc. of IEEE 2018 3rd International Conference on Inventive Computation Technologies



Funded by the Erasmus+ Programme of the European Union

Lisalugemine

- Federal Communications Commission. Cybersecurity for Small Business. https://www.fcc.gov/general/cybersecurity-small-business
- State of Cybersecurity in Local, State & Federal Government. Ponemon Institute Research Paper. https://www.ponemon.org/local/upload/file/State%20of%20Cybersecurity%20in%20Government%20FINAL2.pdf
- NCSS Good Practice Guide. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/ncss-good-practice-guide



Tänan kuulamast!