

"Ära kliki igale poole!"

Küberhügieen - kuidas muuta kasutajate hoiakuid ja käitumist küberruumis turvalisemaks?

Kaie Maennel, doktorant, TalTech
kaie.maennel@taltech.ee

Vahest on uudistes...

Kadri Põlendik • Äripäev • 28. juuni 2017

Jaga lugu:    

UUDISED

Rahvusvaheline küberrünnak jõudis Eestisse

Eesti ettevõtte langes erakordse küberpettuse ohvriks ja maksis hakeritele kopsaka summa



Aivar Pau
ajakirjanik



18. august 2018, 0:00

Politsei ja Delfi veebilehti tabas küberrünnak

31. august 2018 18:00

Politsei- ja piirivalveameti (PPA) kodulehte tabas eile pärastlõunal küberrünnak. Sama saatus tabas ka Delfi portaale.

Riigi Infosüsteemi Ametile (RIA) teada olevalt ei olnud eile poole tunni jooksul võimalik külastada politsei kodulehte. Veebileht oli kättesaamatu alates kella 14st, kuna langes teenustööstusründe



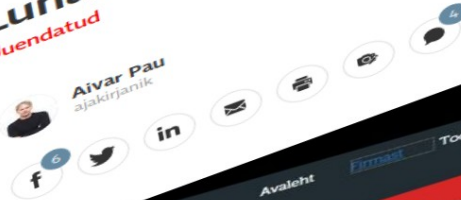
Foto: Pixabay

Lunavararünnak FEBile leidis kinnitust

23. august 2018, 10:21



Aivar Pau
ajakirjanik



Seoses tehnilise rikkega on kauplused kuni 27.08 suletud, vabandame ebamugavuste pärast!

Viimased uudised (16. nov)...



RIIGI INFOSÜSTEEMI AMET

Riigi infosüsteem

Küberturvalisus

[Avaleht](#) > [Uudised](#) > [Küberkurjategijad on sihikule võtnud ettevõtted](#)

Küberkurjategijad on sihikule võtnud ettevõtted



16.11.2018

2018. aasta viimase kvartali suundumused näitavad, et tavakasutajate asemel sihivad küberkurjategijad järjest enam ettevõtete raha eest otsustajaid. Raha püütakse välja petta keerukate ja aeganõudvate petuskeemidega ning eriti ettevaatlik tuleks olla siis, kui koostööpartner palub muuta pangakonto numbrit.

Millest plaanin rääkida...

- Küberintsidentide vastu pole 100% kaitset
- Küberturvalisuse tagamine:
 - inimesed, protsessid ja tehnoloogia
- Räägime inimestest (nõrgim lüli?), kelle:
 - teadmised küberturbest loosungite tasemel
 - teadmised turvalisemas käitumises ei väljendu
- Kuidas **küberhügieeni parandada** ja muuta teadmised turvaliseks käitumisnormiks?

Mis on 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/>)

Mõttekoht: Kas ainult andmed?



Eesmärk...

... **vähendada** peamiselt kasutajat ohustavaid küberohte:

- andmekadu (nt varukoopiad puuduvad)
- andmelekked (info juhuslik või sihilik sattumine volitamata isikute kätte)
- erinevad võrgupõhised turvariskid (rämpspost, pahavara, sotsiaalsed manipulatsioonid, otsesed ründed)

Kas peaks muretsema?

Maailmas:

- 57% ettevõtteid usuvad, et võivad langeda küberrünnaku ohvriks
- 52% ettevõtteid usuvad, et risk tuleneb töötajate teadmatusesest või hoolimatusesest
- Hooletu töötaja põhjustas 46% küberintsidentidest (esimesel kohal pahavara).
- Töötaja ei ole mitte ainult 'rüндеvektor' vaid risk on ka pahatahtlik käitumine (30% küberintsidentidest)

Eestis: 2018.a oktoobris **302** (septembris 354) raporteeritud küberintsidenti (ja mitte kõike ei raporteerita!)

Allikad: IT Security Risks Survey 2017, global data, <https://www.kaspersky.com/blog/the-human-factor-in-it-security/>

<https://www.ria.ee/et/kuberturvalisus>

Kus on riskid ja kuidas võidakse rünnata?

- Inimfaktori ja -käitumisega riskide top:
 - Töötajad jagavad liigselt infot mobiilide kaudu 47%,
 - Mobiilide kaotus tekitab ettevõttele turvariske 46%,
 - IT resursside mittesobiv (ebaturvaline) kasutus 44% - *NB: suurem risk väikeettevõtetes*
- Peamised rünnakuviisid:
 - Viirused / pahavara 49%
 - Eksploitid (nõrkuse ärakasutusele suunatud ründe vahendid) / andmekaotus mobiilide kaudu 30%
 - Õngitsemine / sotsiaalmanipuleerimine 28%

Allikas: IT Security Risks Survey 2017, global data, <https://www.kaspersky.com/blog/the-human-factor-in-it-security/>

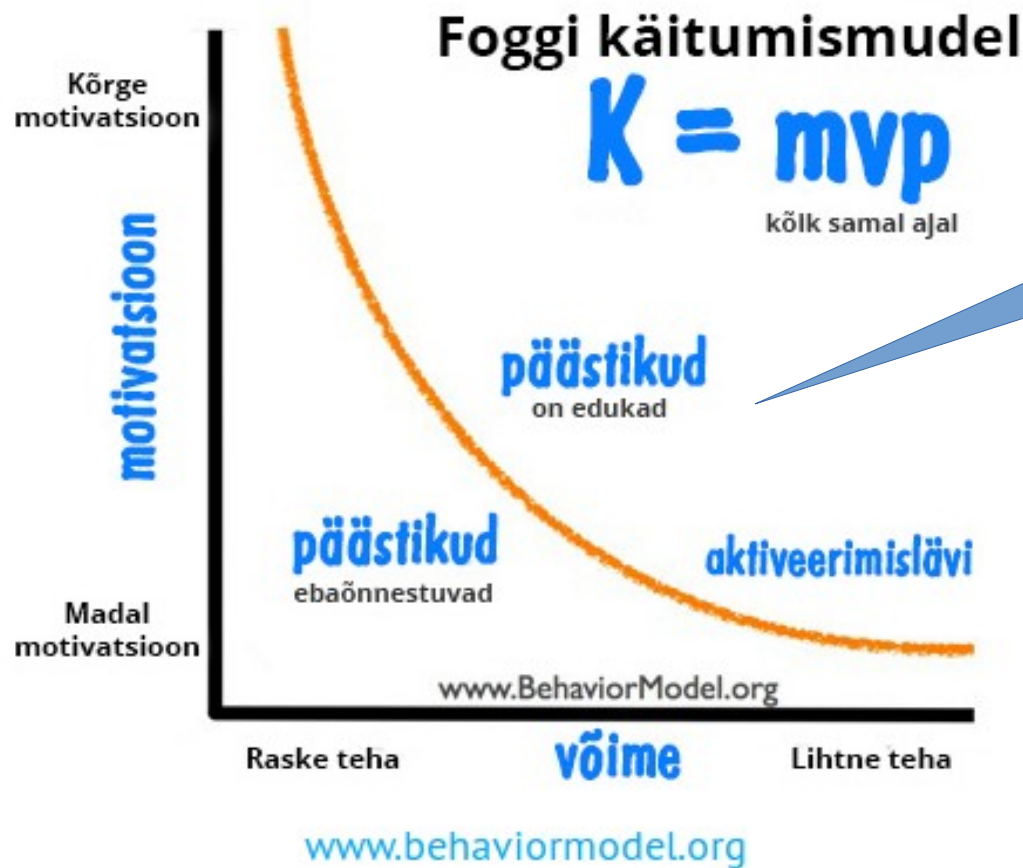
Miks käitumine ei muutu ja koolitused läbi kukuvad?

Käitumise muutmiseks on vaja rohkemat, kui lihtsalt info jagamist riskide kohta ja õigete käitumisviiside kohta:

- Inimene peab infost aru saama
- Olema võimaline seda rakendama
- Tahtma niimoodi käituda
 - See eeldab aga suhtumise ja kavatsuste muutmist

Allikas: M. Bada and A. Sasse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," 2014.

Et käitumist muuta ei piisa lihtsalt teadmiseest....



Mis on turvalise interneti
käitumise puhul 'päästik'?

Mis on internetikäitumise puhul ‘päästik’? (Foggi mudelis)

- Internetis puuduvad selgelt ohumärgid!
- Inimesed ei ole internetiohtudega harjunud
- Seega enne töötajale ülesande andmist (*nt tee ja kontrolli varukoopia*) mõtle,
 - kas töötajal on piisavalt kõrge motivatsioon?
 - kas tegevus on tema jaoks piisavalt lihtne?
 - Kui vastus on **EI**, siis mõistlik midagi muuta (nt muuda tegevus lihtsamaks)
 - Motivatsiooni tõstmine kõige viimane võimalus (so kõige raskem ja sõltub väga paljudest allumatutest teguritest)

Miks me Internetis ebaturvaliselt käitume ja kuidas
käitumist muuta?
Palju tõestamata või osaliselt tõestatud teooriaid...

Soolised erinevused

- Erinevused naiste ja meeste vahel:
 - arvutikasutusoskus
 - eelnev kogemus
 - 'päästikud' (*cues-to-action*)
 - omaalgatus ja
 - initsiatiiv oma käitumist raporteerida
- Leiti, et kuna naiste omaalgatusvõime on madalam kui meestel, siis peaks just seda 'päästikut' rõhutama küberturvalisuse koolitusprogrammides naistele

Allikas: Anwar, Mohd, et al. "Gender difference and employees' cybersecurity behaviors." Computers in Human Behavior 69 (2017): 437-443.

Rahaline väärtus

- Kasutajad **käituvad riskantsemalt kui neil on võimalus kaotada raha** (vähem riskantsemalt kui võimalus võita) – kasutada seda käitumise mõjutusvahendina, et õpetada riske hindama sõltumatult lubatud 'tasudest'
- Ekperiment – veebilehitseja pistikprogrammi allalaadimine, mis ohustab turvalisust:
 - (1) hoiab ära boonuspunklide kaotuse tudengikontolt (kaotuse vähendamine)
 - (2) annab topelt boonuspunktid tudengikontole (võidu saamine)
- Vastust veel ei ole, aga **hüpotees** on, et inimesed:
 - riskeerivad turvalises käitumises rohkem, kui tulemuseks on kaotuse vältimine, seega teadlased arvavad, et plug-ini laaditakse alla eelkõige esimesel juhul

Allikas: Smith, Samuel Noah, et al. "The Impact of Monetary Value Gains and Losses on Cybersecurity Behavior." Proceedings of the Midwest Association for Information Systems Conference. 2017.

Mõttemudelid

- Inimesed kasutavad erinevaid mõttemudeleid turvalisuse riskidest arusaamiseks:
 - Küberkaitse (a cybersecurity) (ebaturvaliste veebilehete võimalus – turvahoiatused)
 - haigus (a disease) (haigete inimeste võimalus – köhimine ja aevastamine)
 - füüsiline turvalisus (a physical security) (füüsilise kallaletungivõimalus – pime tänav)
 - kuritegevus / kuritegelik käitumine (a crime/criminal behavior) (krediitkaardi pettus – kahtlase tegevuse hoiatus).
- Mudelid on erinevad, mõtlemine ja käitumine sarnased ja arvatavasti ei mõjuta kasutajate otsuseid või käitumist internetis

Allikas: Brase, Gary L., Eugene Y. Vasserman, and William Hsu. "Do Different Mental Models Influence Cybersecurity Behavior? Evaluations via Statistical Reasoning Performance." Frontiers in psychology 8 (2017): 1929.

Sinu arvuti 'jäljed'...

- Kasutajad on jagatud 4 kategooriasse:
 - Mängurid (gamers)
 - Professionaalid (professionals),
 - Tarkvaraarendajad (software developers),
 - Muud (others)
- Arvutis olevad tunnused, nt .exe failid, allkirjastama admed, veebist allalaetud andmed, internetis 'reisimise' ajalugu, jne
- Neid võrreldi Symantec viirusetõrjeprogrammi poolt avastatud pahavara rünnakutega
- Tarkvaraarendajad on kõige riskantsem kategooria!

Allikas: Ovelgönne, Michael, et al. "Understanding the relationship between human behavior and susceptibility to cyber attacks: a data-driven approach." ACM Transactions on Intelligent Systems and Technology (TIST) 8.4 (2017): 51.

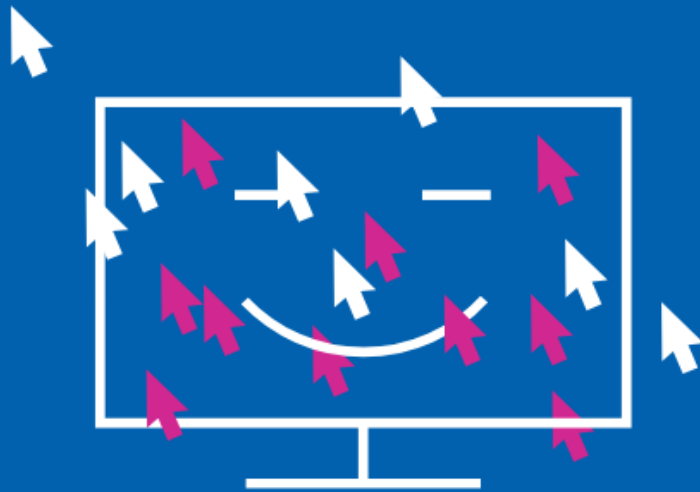
Kokkuvõtvalt

- Palju tõestamata või osaliselt tõestatud teooriaid...
- Alles uurime :)
 - Kui teada miks -> võimalus positiivselt mõjutada..
- Pidev muutumine



Mõttepaus... :)

Ukraina ettevõtted
nakatasid ise tahtlikult
oma arvutisüsteemid
viirusega.



CyberSec juhtumid – nr. 1

Ukrainlased leiutasid uue viisi, **kuidas** makse **vältida**. Kohalik “IT-nohik” vahistati NotPetya pahavara **levitamise eest** – tema vabandus oli, et ta tahtis aidata kohalikke äriettevõtteid maksude **tasumise pikenduse saamisel** (vähemalt 2017. aastal oli pahavaraga nakatumine piisav põhjendus maksupikenduse taotlemisel).



go.ttu.ee/csgame

CyberSec juhtumid...



<https://sites.google.com/view/tty-csgame/eesti>
(saab kaardid ka alla laadida!)

Mõned võimalikud ohuolukorrad ettevõtetes ja soovitused...

Finantsjuhi pettus

... töötajat, kes on volitatud tegema makseid, petetakse maksma võltsitud arveid või tegema autoriseerimata kandeid ettevõtte kontolt

- Mida ettevõtte ja juhtkond saab teha:
 - Ole teadlik võimalikest riskidest ja räägi töötajatega
 - Julgusta maksete nõuetesse suhtuma ettevaatlikkusega
 - Võta maksete sooritamiseks kasutusele selged protseduurid – nt e-maili teel saabunud maksenõuete õigsuse osas helistada vms
 - Loo regulaarne raporteerimine
 - Vaata üle veebilehe informatsioon (kas vajalik avalikustada?)
 - Hoolitse tehnilise turvalisuse eest (nt SPF kontrollib, et ettevõtte nimel saaks kirju välja saata vaid kindlaksmääratud serveritest)

Elust enesest ...

Näidis kirjavahetusest

Eelmisel kuul juhtunud «tegevjuhi petuskeemi» näidis, kus Eesti ettevõtte reaalselt maksis kurjategijatele 29 000 eurot.

The diagram illustrates an email exchange between Markus Boss and Kati Tõnisson, with five numbered annotations (1-5) highlighting key details:

- 1. kiri** (Red circle): Points to the email header of the first message from Markus Boss. Annotation: "Jäigi meilisaidi aadressi - .ee on firma juhi puhul muutunud märkamata .es-ks" (The .ee domain in the email address was not noticed as it changed to .es for the company head).
- 2. kiri** (Blue circle): Points to the body of the first message. Annotation: "Tere hommikust. Mis on meie panga saldo? Kas saame maksta 29T täna? Tervitused" (Good morning. What is our bank balance? Can we pay 29T today? Greetings).
- 3. kiri** (Red circle): Points to the header of the second message from Markus Boss. Annotation: "Jäigi eesti keelt: Palun maksta asemel on kirjas palun maksta - ilmselge Google Translate'i tõlge." (I stayed in Estonian: Please pay instead it is written please pay - obviously a Google Translate translation).
- 4. kiri** (Blue circle): Points to the header of the third message from Kati Tõnisson. Annotation: "Tere. Maksekorraldus lood. Terv. Kati" (Greetings. Payment arrangement is being made. Greetings. Kati).
- 5. kiri** (Red circle): Points to the body of the third message. Annotation: "Sama kahtlane maksekorraldus juba teist korda ja veelgi suuremalt - panane latern võiks eredalt põleda!" (The same suspicious payment arrangement already for the second time and even more - the lantern should burn brightly!).

The email content includes details such as the sender's name (Markus Boss), the recipient's name (Kati Tõnisson), the subject (Makse), the date (Friday, October 19, 2018), and the bank details (HSBC, IBAN: GB60HBUK40471173877981, BIC: HBUKGB4109T).

Allikas: PM 6.11.18 Aivar Paju

Arve pettus

... ettevõttega võetakse ühendust (telefon, kiri, e-kiri vms) ja väidetakse end esindavat tarnijat/teenuse pakkujat/kreeditori paludes tulevaste arvete pangaandmete (st pangakonto saaja andmeid) muutmist. *Uus konto on aga petiste valduses.*

- Mida ettevõtte ja juhtkond saab teha:
 - Ole teadlik võimalikest riskidest ja räägi töötajatega
 - Loo protseduur maksenõuete kontrollimiseks – nt ebakorrapärasuste kontrollimine (sama konto, sama riik, jne)
 - Välismaise partneriga lepi kokku suhtluskanalis ja ära piirdu vaid e-postiga
 - Vaata üle veebilehe informatsioon (kas vajalik avalikustada?)

Pangaandmete õngitsuskirjad

... võltsitud saatjaga e-kirjade kasutamist, mis meelitavad saajat enda isikuandmeid, finants- või turvainformatsiooni jagama

- Mida ettevõtte ja juhtkond saab teha:
 - Ole teadlik võimalikest riskidest ja räägi töötajatega
 - Hoia tarkvara uuendatud
 - Ole valvas, kui 'panga' e-kiri küsib tundlikku informatsiooni (nt pangakonto salasõna)
 - Vaata e-kirja tähelepanelikult (võrdle aadressi varajasemate kirjadega)
 - Kontrolli, kas esineb halba õigekirja või grammatikat
 - Ära vasta kahtlastele e-kirjadele (saada pangale edasi kirjutades meiliaadressi ise)
 - Ära kliki lingile ega lae alla manust, vaid kirjuta aadress enda brauserisse ise
 - Kui kahtlustad, siis kontrolli panga kodulehekülge või helista panka

Nt: 2018 septembris Loki-Bit pahavara: kirjas palutakse kontrollida manuses olevaid pangaandmeid ja väidetakse, et tehtud ülekanne on ebaõnnestunud. Tegelikuses sisaldab manus LokiBoti pahavara, mis nakatumisel püüab varastada paroole ja krüptorahakotte

Positiivne lähenemine ja organisatsiooni kultuur

- Miks öelda, et 95% on halvad - ütle parem, et 5% on tublid...
- Turvakäitumine ja -kultuur kui norm (*lennundusest laenatud mõte - 'just culture'*)
- ABC – Awareness, Behavior and Culture (teadlikkus, käitumine ja kultuur)
- Koolitusest pole kasu, kui ettevõtte sisemine kultuur seda ei toeta...
- Rolliga seotud teemad (tekita isiklik seos) – nt raamatupidaja ja sekretär vs laotöötaja või müüja (*what's in it for me?*)
- Isiklik vs. tööelu lahushoidmine...

Põhjalikumad lugemist: ABC model, Marmalade Box, UK

<http://cyber.uk/dr-jessica-barker/>

Kokkuvõtvalt:

- Lootus, et minuga/minu ettevõttega ei ole strateegia
- Riskid:
 - Petturist töötajad, hooletud töötajad, häkkerid ja eesmärgiga tegutsejad, pahavara, sõltuvus kolmandast osapooldest, nõrgad IT kontrollid, hankijad ja teenusosutajad
- Tagajärjed:
 - Andmekadu, tootlikkuse vähenemine, intellektuaalse vara kaotus, usalduse kaotus, tulude kaotus, seaduste rikkumine
- Riskide aksepteerimine ja nende maandamine:
 - Terviklik kaitse – intergreerituna inimesed, protsessid ja tehnoloogia
 - Ründaja valib neist rünnakuvektoriks kolmest nõrgima lüli

Mõned turvalised küberhügieeni
käitumisharjumused, millele tähelepanu pöörata ja
teistega ka jagada...

Salasõnad

Milline pakutud salasõnadest on kõige turvalisem?

(1)Meil_Aia_Aarne_Tanava5_Nii_Arma5!

(2)kiisuke

(3)parool

(4)Qwerty

(5)12345678

(6)YHs56@mK.

(7)Leeni96

Salasõnad

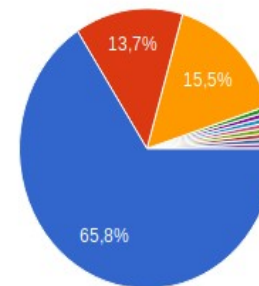
Kuna kasutame palju erinevaid teenuseid, on raske pidada meeles kõiki paroole. *Milline oleks hea strateegia?*

- (1)Salvestan kõik erinevad paroolid ühte faili: kui mul on ühte neist vaja, leian selle kergesti üles
- (2)Eelistan siiski kasutada iga kord erinevat parooli
- (3)Kasutan üht ja sama parooli iga teenuse jaoks, mida kasutan

Salasõnad

Hoian oma salasõnasid järgnevalt:

161 vastust

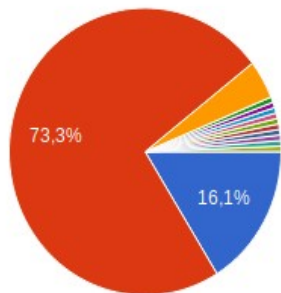


- Meeldejäätmine
- Kirjutan üles (paberkandjale ja/või...
- Kasutan password manageri (nt Ke...
- Genereerin igale veebilehele ise ni...
- Samuti kõik kolm, tegelt peaksite si...
- Password manager ja meeldejäatmi...
- Sõltub - Üleskirjutatud ja seifis on k...
- Jätan meelde või kirjutan lühendin...

▲ 1/2 ▼

Mis on teie arvates turvaline parool?

161 vastust

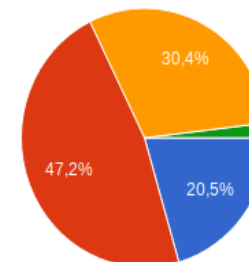


- Mida pikem, seda parem (nt. lausef...
- Sisaldab numbreid eriti tähti (nt. pun...
- On seotud isikliku mälestuse või te...
- Tähed ja numbrid
- suurtäht - väiketäht-numbrid kombi...
- Kaks esimest pointi
- sisaldab suuri tähti, väikseid tähti j...
- esimese ja teise combo (lause + er...

▲ 1/2 ▼

Kas <https://gotcha.pw>, <https://haveibeenpwned.com/> või teiste avalike allikate andmetel on mõni teie emailide paroolidest lekkinud?

161 vastust



- Jah
- Ei
- Ei tea
- Mind ei huvita, kas mu paroolid on lekkinud

Allikas: TalTech tudengite kursusetöö
(Sept 2018) (NB: ei saa väita et
represantiivne terve Eesti kohta!

Autentimine

... ehk tuvastamiseks on kolm võimalust:

- Teave – nt parool, PIN-kood, muster (telefoni ekraanilukk)
- Millegi omamine – nt mobiiltelefon, PIN-kalkulaator või ID-kaart
- Kasutaja ise – nt sõrmejalg või hääl

- Ühetasandilise autentimine – ainult üks viis kasutaja tuvastamiseks (nt e-posti ja parooliga sisselogimine veebilehele)
- Kui võimalik, kasuta kahetasandilist (nt Facebook, Google/gmail, Instagram, Twitter, jne), so 2 viisi koos...

Tarkvara uuendamine

Räägitakse, kui tähtis on regulaarselt ajakohastada ja paigata arvutite operatsioonisüsteeme (OS). Kui mõtlete sellele, siis *OSi paikamine...*

- (1) Lahendab probleemid ja muudab OSi turvalisemaks
- (2) Võimaldab jätkata oma tarkvara kasutamist ilma lisatasuta
- (3) Parandab OSi tööfunktsioone

Mõtle ka: vanad programmid?

Viirusetõrjetarkvara

Pahavara eest kaitseb viirusetõrjetarkvara. Ent isegi sellest ei piisa, kuna viirusetõrjet tuleb pidevalt uuendada. *Mida arvate vajaduse kohta uuendada viirusetõrjet?*

- (1) Viirusetõrjet tuleb uuendada ainult siis, kui ei paika regulaarselt oma OSi
- (2) Viirusetõrje uuendamine kaitseb arvutit kõige uuema pahavara eest
- (3) Viirusetõrje uuendused tagavad arvuti nõuetekohase jõudluse

Krüptoraha kaevandamine

Teie arvuti töötamine aeglustub järsku, eriti veebilehitsemine võtab tavapärasest rohkem aega. IT-kolleegi sõnul kasutatakse teie arvutit krüptoraha kaevandamiseks. *Kuidas oleks saanud seda vältida?*

- (1) Kasutades ajakohast viirusetõrjetarkvara
- (2) Lisades veebilehitsejale krüptoraha kaevandamise eest kaitsev pistikprogramm (nt No Coin, AntiMiner, minerBlock)
- (3) Kontrollides veebilehitsejate seadeid ja blokeerides ebavajalikud funktsioonid (nt JavaScripti ja Flashi automaatkäivitus)

Mobiilirakendused

Olete innukas mobiiltelefoni rakenduste kasutaja. Kui näete mõnda huvitavat rakendust, siis kindlasti laadite selle alla ja paigaldate oma telefoni. *Ent ohutuse ja turvalisuse tagamiseks on parim viis...*

- (1) Kontrollida, et rakenduse allalaadimisega ei kaasne varjatud kulusid
- (2) Kontrollida, kas rakendus pärineb usaldusväärsest allikast
- (3) Vältida liiga paljude rakenduste paigaldamist

Arvuti- ja mobiilikasutus

Mida arvate oma isikliku nutitelefoni laadimisest tööarvutist?

- (1)ei ole ohtlik, sest aku laadimisega ei kaasne andmevahetust
- (2)ei ole ohtlik, kui kasutada tootja originaalkaablit
- (3)ei ole ohtlik, kui laetav nutitelefon on välja lülitatud
- (4)on ohtlik, sest ka nii võib tööarvuti nakatuda pahavaraga

Õngitsuskirjad

Leiate postkastist e-kirja sõbralt, kellest ei ole kaua kuulnud. Kirjas on tekst “Tere, palun klõpsake siin <http://shorturl.jafghc.com>, seal ootab teid üllatus”. *Mida peaksite tegema?*

- (1) Ei tee selle e-kirjaga midagi ja kindlasti ei klõpsa viidatud lingil
- (2) Klõpsate lingil, kuna tunnete e-kirja saatjat (oma sõpra)
- (3) Klõpsate lingil ainult siis, kui see tundub teile tuttav

Mälupulk

Kuidas toimiksid, kui leiad kontori ruumidest mälupulga?

- (1)võtan üles ja viin IT-töötajale või hävitan
- (2)võtan üles, kustutan sisu ja kasutan isiklikuks otstarbeks
- (3)ei võta üles

Lisaks mõttekoht: mida teeksid kingitud või teistes arvutites kasutatud mälupulkadega?

Kas kasutad krüpteeritud mälupulka?

Sotsiaalmeeidia

Madli on saatnud keegi Juhani nimeline FBs sõbrakutse. Madli Juhani ei tunne, aga näeb, et nad on käinud samas koolis, neil on sarnased huvid ja tööalane taust. Uudishimu saab võitu ja ta otsustab kutse vastu võtta. *Mida arvate Madli otsusest?*

- (1) Toimis õigesti, sest kontrollis kutse saatnud inimese profiili ning nägi, et neil on piisavalt palju ühiseid huvisid, et kutsele vastata
- (2) Ei toiminud õigesti, sest võttis vastu sõbrakutse inimeselt, keda ta ei tunne.
- (3) Toimis õigesti, sest sotsiaalmeeidia ongi mõeldud uute inimestega kontakti loomiseks ja suhtlemiseks ja ei tule kontrollida

Lisaks mõttekoht: kas isegi teadaolevat sõbralt tasub alati kutse vastu võtta?

Sotsiaalseadmeedia – mõned mõtted...

- Umbes 15% Twitteri ja Facebooki kontodest on libakontod
- Kui kahtled:
 - Fake Follower Check: <http://fakers.statuspeople.com>
 - Twitteraudit - <http://twitteraudit.com>
- Kontrolli oma konto privaatsussätteid...
- Arvesta, et on suur võimalus, et info mida seal jagad (ka nt Messengeris) lekib
 - Kontrolli, kas Sinu andmed lekkisid:
<https://geenius.ee/uudis/vaata-siit-kas-sinu-facebooki-konto-anges-samuti-hiljutise-runnaku-ohvriks/>

Üleõla surfamine

Anna avab bussis sõites tahvelarvuti e-postkasti, kus leiab töökaaslase kirja konfidentsiaalse infoga. Ta otsustab koosolekuks valmistuda ja süveneb dokumentidesse. *Kas Anna toimis õigesti?*

- (1)ei, sest luges dokumente nii, et need olid kaasreisijatele nähtavad
- (2)jah, sest kui ka keegi dokumente nägi, siis ei juhtu sellest midagi
- (3)jah, aga ainult juhul, kui Anna kasutab privaatsusfiltrit

Info jagamine

Jaan saab kõne meesterahvalt, kes tutvustab end ettevõtte IT-toe teenusepakkujana ja soovib süsteemitesti läbiviimiseks täpsustavat infot. Jaan leiab end andmas üksikasjalikku infot (kasutajanime jms). *Kuidas oleks Jaan pidanud toimima?*

- (1) Toimis õigesti, sest selline info ei ole konfidentsiaalne
- (2) Oleks pidanud enne küsimustele vastamist paluma vestluspartneril end täpsemalt identifitseerida ja talle tagasi helistama (numbri leiaks sõltumatust allikast)
- (3) Jaan ei oleks tohtinud telefoni teel sellist infot jagada, vaid paluma vestluspartneril küsimuste esitamiseks kohale tulla

Lunavara

Kuidas saaks kaitsta lunavarakampaania eest?

(1)kasudes viimast tarkvaraversiooni (sh uuendused)

(2)tehes regulaarselt varukoopiad

(3)kontrollides, et varukoopiad on võimalik taastada

Mõttekoht: ettevõttes ka süsteemi kasutajate õiguste piiramine ja töötajatega rääkimine sel teemal

Arvutikasutus

Kui lahkud tööarvuti tagant või kontorist, mida oleks turvaline teha?

- (1) arvuti monitori välja lülitada
- (2) arvuti lukustada
- (3) rakendustest välja logida
- (4) arvutist välja logida

WIFI

Surfate kohviku WiFi võrgus. Kohvik ei küsi tüütut salasõna. *Milline on kõige turvalisem viis interneti kasutamiseks avalikus ruumis?*

- (1) avalik salasõnavaba internet
- (2) avalik salasõnaga kaitstud internet
- (3) oma telefoniga 3G/4G internetiühenduse loomine

Kodu(-kontori) internet

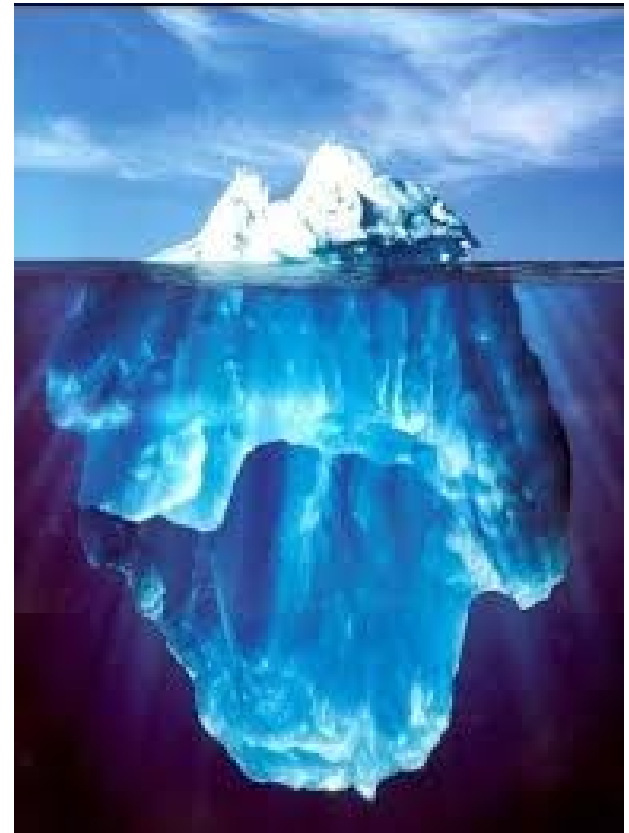
Kodu(-kontori) WiFi puhul tasub üle vaadata seadistused. *Mida peaksite tegema?*

- Muutma ruuteri admin kasutajatunnus ja parool
- Muutma tehase poolt antud WiFi võrgunimi
- Kontrollima, kas ruuteri suhtlus on krüpteeritud (*kasutab WPA2*)
- Ei ole vaja midagi teha (ruuteri turvalise seadistamise eest vastutab teenusepakkuja)

Teemasid oleks veel...

Kui sa tervet rehkendust ei
jõua tee pool
... aga tee korralikult.

*Oskar Lutsu "Kevade" õpetaja Lauri
sõnad Tootsile*



Kasulikud infoallikad:

- RIA ja CERT:

<https://www.ria.ee/et/kuberturvalisus>

- Veebileht *Arvutikaitse*:

<https://www.arvutikaitse.ee/>

- Veebileht *Targalt Internetis*:

<https://www.targaltinternetis.ee/>

- Testi ennast või oma töötajaid (EE):

<https://cybersecuritymonth.eu/references/quiz-demonstration/welcome-to-the-network-and-information-security-quiz/>

Meelespead, mida ka teistega jagada...

Üldine meelepea...

- Vali turvalised paroolid
- Uuenda pidevalt tarkvara (nii OS kui rakendustarkvara)
- Ole ettevaatlik tundmatute failide ja veebiviidete avamisel
- Eelista turvatud (HTTPS-) ühendusega veebilehti
- Eelista kaheastmelist autentimist
- Rakenda üldist ettevaatut
- Varunda oma andmeid pidevalt
- Vali tarkvara läbimõeldult ja kontrollitult

Allikas: <https://et.wikipedia.org/wiki/Küberügieen>

Sotsiaalmeeedia meelespea...

- Ära jaga privaatseid andmeid
- Sea privaatsussätteid sobivaks
- Ära jaga liiga palju ajalugu
- Jälgi detaile, mida postitad
- Suhetes usalda, aga kontrolli
- Otsi iseennast (tee eneseaudit)
- Vähem ja kvaliteetselt vs. rohkem ja avalikult
- Kontrolli kommentaare

Allikas: <https://et.wikipedia.org/wiki/Küberügieen>

Teavitus küberintsidendi kohta...

...olukord, kus rikutakse organisatsiooni, asutuse või üksikisiku infosüsteemi ja/või selles oleva info konfidentsiaalsust, terviklikkust ja käideldavust (sh kasutatakse omavoliliselt kellegi teise infosüsteemi või häiritakse tahtlikult selle toimivust)

<https://www.ria.ee/et/kuberturvalisus/cert-ee.html>

CERT kontaktid

Üldtelefon: **663 0299**

E-post: **cert [at] cert.ee**

CERT-EE töötab 24/7

AITÄH!

Peatu, mõtle ja alles siis kliki!

Küsimusi?

Kirjuta: kaie.maennel@taltech.ee