



RIIGI INFOSÜSTEEMI AMET



TARK



e-RIIK

Infoturbe teadlikkuse tõstmise koolitus

Jaosmaterjal

- Kuupäev: 11.03.2018
- Koostaja: SecTeam OÜ
- Kontakt: Rünno Reinu, info@ssecteam.ee, +372 520 5558

TEADLIKU ARVUTIKASUTAJA TARKUSED

Käesolev jaosmaterjal on infoturbe teadlikkuse tõstmise koolituse järgseks meelepeaks, mitte koolituse asendamiseks.

Viidad ja tarkvarasoovitused on koolituse hetkel ajakohased, kuid võivad kaotada oma väärtust üldise IT ja turvaolukorra muutumise tõttu.

NB! Kui digitaalse dokumendi viitadel klikkides veebilehte ei leita, siis palun kopeerige aadress käsitsi veebilehitseja aadressiribale.

PALJU PAHANDUST JÄÄB TEKKIMATA, KUI:

- **Andmeid varundatakse sagedasti**, st hoitakse vähemalt kahte eksemplari andmetest eraldiseisvates seadmetes:
 - näiteks kindlas hoiukohas olevale välisele kõvakettale või usaldusväärsele võrgukettale;
 - juhiseid seadmete koduseks varundamiseks:
 - Windows 7: <https://support.microsoft.com/et-ee/help/17127/windows-back-up-restore#1TC=windows-7>
 - Windows 10: <https://support.microsoft.com/et-ee/help/17143/windows-10-back-up-your-files>
 - Mac: <https://support.apple.com/et-ee/mac-backup>
 - iPhone, iPad: <https://support.apple.com/et-ee/HT203977>
 - Android (võib erineda eri tootjatel): <https://www.computerworld.com/article/3215095/android/how-to-backup-android-phones-complete-guide.html>
 - kontoris korraldab varunduse IT-teenuseosutaja.
- **Arvutil ja nutiseadmel uuendatakse sagedasti**:
 - operatsioonisüsteemi
 - Windows: <https://support.microsoft.com/et-ee/help/12373/windows-update-faq>
 - Mac: <https://support.apple.com/et-ee/HT201541>
 - Android nutiseade (võib erineda eri tootjatel): <https://www.wikihow.tech/Check-for-Updates-on-Your-Android-Phone>
 - iPhone, iPad: <https://support.apple.com/et-ee/HT204204>

- kõiki paigaldatud rakendusi ja äppe (Internet Explorer, Firefox, Chrome, Acrobat PDF Reader, Java, MS Office, DigiDoc, nutiseadmete äpid jms);
- kõiki veebilehitseja laiendusi (plugins, addins, extensions - Flash Player, Java, QuickTime Player jms);
- tootjapoolse toeta tarkvara viska arvutist kähku välja (nt Windows XP ja Office 2003)
<https://www.ria.ee/ee/vananenud-tarkvara-kasutamine-on-ohtlik.html>
- **Arvutites ja ka Android nutiseadmetes kasutatakse pahavaratõrje tarkvara:**
 - Pahavaratõrjujate perioodilised võrdlused erinevate operatsioonisüsteemide kaupa: <https://www.av-test.org/en/>
 - näiteks tasuta tõrjujad tootjatelt:
 - Microsoft <https://support.microsoft.com/et-ee/help/4013263/windows-10-protect-my-device-with-windows-defender-antivirus>
 - Avast <https://www.avast.com/en-gb/free-antivirus-download>
 - AVG <http://www.avg.com/ww-en/free-antivirus-download>
 - Bitdefender <https://www.bitdefender.com/solutions/free.html>
 - Avira <https://www.avira.com/en/free-antivirus-windows>
 - Windowsi 7 ja 8 puhul tasuta Microsofti turvatarkvara EMET, mis ei asenda pahavaratõrje tarkvara, kuid tugevdab arvuti vastupanuvõimet rünneteile <https://www.microsoft.com/en-us/download/details.aspx?id=54264>
- **Arvutites kasutatakse tulemüüri tarkvara:**
 - näiteks tasuta tulemüürid tootjatelt:
 - Windows 10 tulemüür <https://support.microsoft.com/et-ee/help/4028544/windows-turn-windows-firewall-on-or-off>
 - Windows 7 tulemüür <https://support.microsoft.com/et-ee/help/17228/windows-protect-my-pc-from-viruses>
 - Zone Alarm <https://www.zonealarm.com/software/free-firewall/>
 - Emsisoft <https://www.emsisoft.com/en/software/internetsecurity/>
 - Mac <https://support.apple.com/et-ee/HT201642>
- **Tarkvara hankimisel ja paigaldamisel:**
 - kasutatakse vaid usaldusväärseid allikaid ja neid ei tõmmata torrentiga, nutiseadmete äppe hangitakse vaid ametlikest Google Play või App Store keskkonnast;
 - erinetakse tüüpilisest kasutajast, näiteks:
 - Windowsi asemel võiks kasutada Apple Mac OSX arvutit või Ubuntu operatsioonisüsteemi (<https://www.ubuntu.com/desktop>);
 - Adobe Acrobat PDF Reader asemel võiks kasutada Foxit PDF Reader (<https://www.foxitsoftware.com/pdf-reader>) või Sumatra PDF (<https://www.sumatrapdfreader.org/download-free-pdf-viewer.html>);
 - Internet Exploreri asemel kasutatakse turvalisemaid veebilehitsejaid Chrome (<https://www.google.com/intl/et/chrome/>), Firefox (<https://www.mozilla.org/et/firefox/new/>) või Edge (ainult Windows 10-ga);

- kaalutakse enne paigaldamist, kas Java või Flash player rakendusi on ikka tungivalt arvutisse vaja;
- edasijõudnud kasutajad kasutavad veebilehitsejates turvalaiendusi, nt:
 - laienduste käivitamise käsitsi lubamine
 - Chrome lehitsejal vanematel versioonidel:
Settings -> Advanced -> Privacy and Security -> Content settings... -> Flash -> Ask first;
 - Firefox lehitsejal avada *Add-ons -> Plugins* ning soovitud plugina rea lõpus valida rippmenüüst *Ask to Activate*
 - skriptide blokeerimine pluginatega Firefox'ile NoScript, Chrome'le ScriptSafe vms;
 - jälitavate veebilehtede blokeerimine pluginatega Disconnect.me, Ghostery vms.
- **Arvuti kasutamisel arvestatakse, et:**
 - kontori ega koduse arvuti külge ei ühendata võõraid mälupulki, -kaarte, väliseid kõvakettaid, nutiseadmeid;
 - enne klikkimist võetakse hetk mõtlemiseks, kas tegu võib olla pahatahtliku lingiga või failiga;
 - arvutit kasutatakse tavakasutaja õigustes, mitte administraatorina;
 - arvuti kõvaketas on täies mahus krüpteeritud, kasutades näiteks:
 - Windows BitLocker Drive Encryption tarkvara (olemas Windows 7 Enterprise ja Ultimate, Windows 8 Pro ja Enterprise, Windows 10 Pro, Enterprise, Education):
[https://technet.microsoft.com/en-us/library/dd835565\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd835565(v=ws.10).aspx)
<https://support.microsoft.com/et-ee/help/4028713/windows-10-turn-on-device-encryption>
https://wiki.itcollege.ee/index.php/Windows_juhend:_Kuidas_k%C3%BCpteerida_kettaid_ja_faile
 - vabavaralist Veracrypt tarkvara:
<https://www.veracrypt.fr/en/Home.html>
 - Mac tarkvara:
<https://support.apple.com/et-ee/HT204837>
 - Android nutiseadmel:
<https://docs.microsoft.com/en-us/intune-user-help/encrypt-your-device-android>
 - Ka välise kõvaketaste ja mälupulkade sisu või üksikud failid on krüpteeritud, kasutades näiteks:
 - ID-kaardi tarkvara DigiDoc Crypto (ainult lühiajaliseks transportimiseks, mitte failide arhiveerimiseks)
<https://installer.id.ee>
 - BitLocker To Go
https://wiki.itcollege.ee/index.php/BitLocker_To_Go
 - välistel andmekandjatel olevad failid kustutatakse turvalisel moel, nt tarkvaraga:
 - SDelete
<https://technet.microsoft.com/en-us/sysinternals/bb897443>
 - Eraser või Free File Shredder

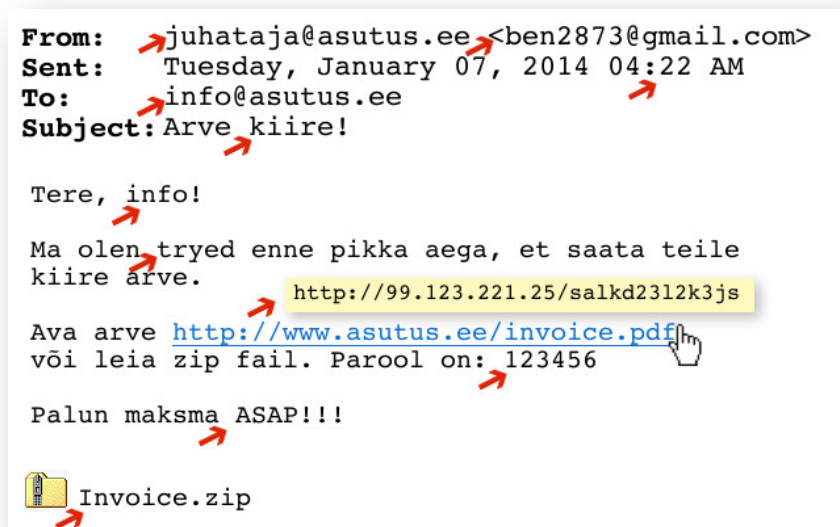
- <https://eraser.heidi.ie/download/>
 - avaliku või võõra WiFi-võrgu asemel kasutatakse võimalusel mobiilset andmesideühendust (3G/4G netipulk, nutitelefoniga jagatud *hotspot*) või VPN-i (erinevaid kolmanda poole VPN teenusepakkujaid leiad <https://vpn-services.bestreviews.net/vpn-comparison/> ja <https://thatoneprivacysite.net/vpn-comparison-chart/>);
 - tööandja faile ja teavet ei kopeerita ilma volituseta pilve (Dropbox, GoogleDrive jms) ega eraarvutitesse;
 - internetti ühenduvad seadmed (asjade internet) häälestatakse turvaliselt: <https://blog.ria.ee/asjade-internet-suurendab-kuberkuritegevust>
<https://blog.ria.ee/esemevorgu-turva>
- **Nutiseadmete kasutamisel arvestatakse, et:**
 - nutiseadmeid tuleb kaitsta sama hoolsalt kui arvuteid - ekraanlukk, tarkvarade uuendamine, pahavarakaitse, mälu krüpteerimine, usaldusväärsed tarkvara allikad, andmete varundamine;
 - nutiseadmetel on aktiveeritud kaughalduse funktsioonid:
 - <https://thetechnorat.wordpress.com/2015/05/07/kuidas-leida-kadunud-ouna-seadet/>
 - <https://thetechnorat.wordpress.com/2015/04/22/kuidas-leida-kaduma-lainud-androidid/>
- **Kahtluste korral kasutatakse pahavara skanneerimiseks:**
 - failide puhul portaali <https://www.virustotal.com>, kuid sinna ei tohi laadida tööandja andmeid ega isikuandmeid;
 - failide puhul edasijõudnud kasutajatele ka pahavara analüüsi CERT-EE "liivakasti" <http://cuckoo.cert.ee/>
 - veebilehtede puhul skannereid:
<https://quttera.com/website-malware-scanner>
<https://sitecheck.sucuri.net>
<https://www.virustotal.com/#url>
<https://app.webinspector.com>

ÕNGITSEMISE TUNNED ÄRA, KUI:

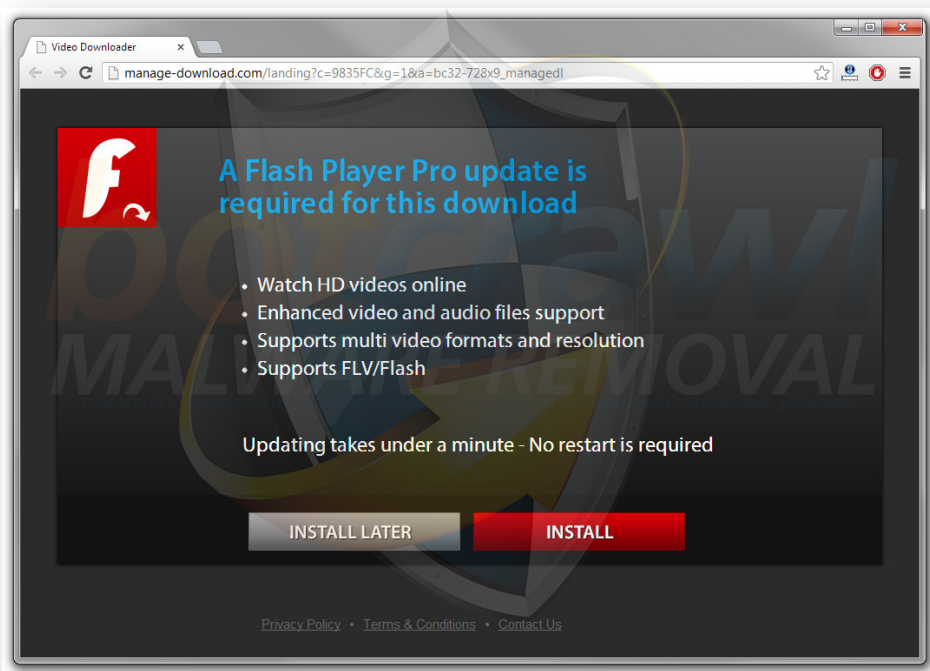
- jälgid, kus veebiriiumis viibid:



- enne klikkimist võtad hetke mõtlemiseks, kas sõnumis on manipulatsioonivõtteid ja veidrat keelekasutust "sõbra" poolt;
- jälgid saadetud sõnumis olevaid õngitsusvihjeid:



- suhtud skeptiliselt, kui tundmatud veebilehed soovivad paigaldada arvutisse tarkvara uuendusi või viirusetõrjujaid:



VEEBIKONTOD JA IDENTITEEDID ON TURVALISED, KUI:

- kõikjal, kus vähegi võimalik, kasutatakse parooli asemel ID-kaarti või mobiil-ID-d:
 - <http://www.id.ee/index.php?id=10585>
 - <http://mobiil.id.ee>
- Kõikjal, kus võimalik, kasutatakse muud 2-tasemelist tuvastamist:
 - Selgitav blogiartikkel <https://blog.ria.ee/multiauthentimisest/>
 - Pikk nimekiri erinevatest teenustest ja nende häälestamise juhenditest, mis toetavad 2-tasemelist tuvastamist: <https://twofactorauth.org/>
 - Google/Gmail
 - <https://blog.ria.ee/kaheastmeline-autentimine-gmail/>
 - <https://support.google.com/accounts/answer/180744?hl=et>
 - Facebook
 - <https://blog.ria.ee/kaheastmeline-autentimine-facebook/>
 - <https://et-ee.facebook.com/help/www/148233965247823>
 - Apple <https://support.apple.com/et-ee/HT204152>
 - Twitter <https://support.twitter.com/articles/20170388>
 - Dropbox <https://www.dropbox.com/help/363/en>
 - Microsoft <https://support.microsoft.com/et-ee/help/12408/microsoft-account-about-two-step-verification>
 - Paypal <https://www.paypal.com/us/webapps/mpp/security/security-protections>
- Paroolid on pikad, piisava keerukusega ja kordumatud, eelistatult lühikesed fraasid (Uimane-p8ial-sorkis-nina, MillaJuba5auna5aab?)
- Paroole hoitakse üleskirjutatult turvaliselt või kavalalt peidetult:
 - šeifis;
 - (ristsõna)raamat, numbrimaatriks, retseptivihik, ostunimekiri jne;
 - suure hulga paroolide korral (peamiselt IT spetsialistid) spetsiaalses paroolihoidlas (KeePass, Password Gorilla, Password Safe), kuid siis taandub kõikide paroolide turvalisus ühe peremees-parooli taha – **see vajab eriti suurt ettevaatust ja hoolikust!**
- aegajalt
 - *guugeldatakse* iseennast;
 - suletakse enda tehtud aegunud veebikontod;
- ei laeta veebilehtedele liigset personaalinfot;
- hoitakse lahus töö ja eraelu identiteet, eriti meiliaadress ja postkast;
- vajadusel luuakse eraelu jaoks lisa võltsidentiteet, millel ei ole ühtegi seost päris identiteediga (ajutise võltsidentiteedi generaator <https://fakena.me/fake-name/>, <https://www.guerrillamail.com/>).

KUI JUHTUS VÕI ON KAHTLUS, SIIS:

- hinga sügavalt sisse ja rahune;
- võta esimesel võimalusel ühendust:
 - oma asutuse infoturbejuhi või IT-spetsialistiga;
 - riikliku infoturbe intsidentide käsitlemise üksusega CERT Eesti:

- cert@cert.ee
- +372 663 0299
- <https://www.ria.ee/ee/cert-kontakt.html>
- kuriteo kahtluse korral politseiga:
 - cybercrime@politsei.ee
 - +372 612 3000
 - veebikonstaablid <http://abiksohvri.ee/et/kontakt>
- isikuandmetega seotud juhtumite korral Andmekaitse Inspeksiooniga:
 - info@aki.ee
 - +372 627 4135
 - <http://www.aki.ee>
- vaheta paroolid usaldusväärses arvutis (ka seal süsteemides, kus kasutasid samasuguseid parooli);
- pahavararakkuse korral ära ürita arvutit iga hinna eest pahavarast puhastada, vaid pigem paigalda kogu operatsioonisüsteem uuesti;
- faile krüpteeriva lunavara (ransomware) nakkuse korral otsi abi lehelt <https://www.nomoreransom.org/et/index.html>

ABIKS LAPSEVANEMALE:

- <http://www.targaltinternetis.ee/>
- <http://www.päriseltkavõi.ee/>
- Windows: <https://support.microsoft.com/et-ee/products/microsoft-account?category=manage-family>
- Apple: <https://support.apple.com/et-ee/HT201060>
- iPhone, iPad: <https://support.apple.com/en-gb/HT201304>
- Android: <https://families.google.com/familylink/>
- Youtube: <https://geenius.ee/rubriik/hea-nipp/kuidas-youtubei-rakendus-lapsesobralikuks-muuta/>

LINKE UURIMISEKS:

- Riigi Infosüsteemi Ameti küberturbe teemalised blogid: <https://blog.ria.ee/>
- Riigi Infosüsteemi Ameti turvateadlikkuse videod ainult avaliku sektori töötajatele (parool: *1nf0Turve!*):
 - <https://vimeo.com/98405698>
 - <https://vimeo.com/98405699>
 - <https://vimeo.com/98406355>
 - <https://vimeo.com/98406356>
 - <https://vimeo.com/98406357>
 - <https://vimeo.com/98406358>
 - <https://vimeo.com/98406359>

