Pahavara takistamine

Soovitused:

- Ära jäta veebilehitsejale meelde salasõnasid! Selle asemel kasuta spetsiaalset turvalist lahendust, näiteks veebilehitseja lisana töötav LastPass ja selle Firefoxi lisand ning ka Google Chrome-ile on lisand olemas. Lastpass on väga erinevatele keskkondadele saadaval - tasub vaadata. Eraldi rakendusena töötab KeePass.
- Järjehoidjate turvaliseks varundamiseks ja sünkroniseerimiseks kasuta näiteks veebilehitseja lisandit Xmarks. See töötab hästi koos lisandiga LastPass.
- Ei soovita kasutada veebilehitsejana MS Internet Explorer-it! Kui veebileht muidu ei tööta siis Firefoxi puhul aitab identiteedi vahetamise lisand! Selle abil saab öelda, et veebilehitseja identifitseeritakse kui MS Internet Explorer ja üldiselt see aitab.
- **Turvaline veebilehitsemine** - kasutage enne internetis surfama hakkamist alljärgnevaid klahvikombinatsioone - siis ei jäta veebilehitseja midagi meelde!
    - Internet Explorer - CTRL+SHIFT+P
    - Firefox - CTRL+SHIFT+P
    - Google Chrome - CTRL+SHIFT+N
    - Opera - CTRL+SHIFT+N
    - Safari - tuleb käsitsi rippmenüüst valida *Private browsing*
- kasuta OpenDNS-i - http://www.opendns.com/
    - http://www.opendns.com/parental-controls/ - vanemakontroll
    - http://www.opendns.com/phishing-protection/ - manipuleerimise kaitse
- Loe ka Google selgitusi turvalise veebilehitsemise kohta!
- Ei soovita igapäevaselt kasutada arvutit administraatori ehk siis juurkasutaja õigustes!
- Soovitan riskide hajutamiseks kõvaketas jagada mitmesse ossa, et hiljem oleks lihtsam operatsioonisüsteemi uuesti paigaldada kui pahavara selle ära on rikkunud.
- kasutage pahavara tõrjumisvahendeid (viirusetõrje, tulemüür, veebilehitseja turvamine lisandite abil, nuhkimisprogrammide eemaldaja jne)
- lisaks soovitan Windowsis rakendada rühmapoliitikaid. Lukku tuleks panna juhtpaneel, register jt Windowsi kergesti haavatavad kohad. Kui seda ei tehta siis on Windows endiselt üsna haavatav vaatamata kasutajaõiguste piiramisele.
- e-postiprogrammina soovitan kasutada veebipõhist e-posti või siis näiteks Thunderbird-i. MS Outlook ja MS Outlook Express on väga vastuvõtlikud viirustele jm pahavarale ning seetõttu kergesti haavatavad. Rõhuv enamus pahavarast levibki e-posti teel ja just eelnimetatud programmide kaasabil...
- kui saadate e-kirja rohkem kui ühele saajale siis kasutage pimekoopia (Bcc:) välja! Ärge kasutage saaja (To:) või koopia (Cc:) välju! Kui tõesti on vaja ekstra näidata, kellele veel kiri on läinud siis võib kirja alguses ka nende inimeste nimed loetleda. Sageli ei ole vaja inimeste e-postiaadresse vaid nende nimesid, kes veel on kirja saanud. Enamasti teavad inimesed üksteise e-postiaadresse ja ei ole neid vaja iga kirja päises veel lisaks saata. See on magus saak pahavarale, mis kasvõi ühe kirja saaja arvutis olles korjab need teised aadressid e-kirja päisest ja algab massiline rämpsposti levitamine ning süütute inimeste e-postiaadressid satuvad musta nimekirja ja blokeeritakse omakorda rämpspostifiltrite poolt... Lisaks levitatakse ka pahavara rämpskirjadega. **Kuidas satub minu e-postiaadress rämpsposti hulka?** Rämpspostitajad korjavad kirjade päistest e-postiaadresse ja saadavad nendega rämpskirju välja. Nad teevad seda seepärast, et kuna e-kiri on saadetud välja neile aadressidele siis järelikult on need töötavad aadressid ehk siis iga aadressi taga on konkreetne inimene kes seda loeb ja seetõttu on mõtet sinna ka reklaami vms rämpsu saata. Rämpspostitajate peamine eesmärk on alati leida võimalikult palju töötavaid aadresse ehk siis aadresse, mida regulaarselt loetakse - siis saab sinna ka regulaarselt rämpsposti saata ja ehk mõnda neid ka avatakse. Rämpspostitajad on reaalsed inimesed. Seejärel tuvastavad rämpspostifiltrid need aadressid, millelt rämpsu välja saadetakse ja panevad need e-kirjad rämpsposti hulka. See olukord tekib kui paljudele e-kirja saates pannakse kõikide e-postiaadressid "saaja" või "koopia" aga mitte "pimekoopia" väljale. Nii levivad e-postiaadressid kolmandatele osapooltele ja kusjuures luba küsimata, sest kõik näevad

siis ka kõiki teisi aadresse. Siis piisab kui kasvõi ühe sellise megapäisega kirja saaja arvutis juhtub olema pahavara, mis e-postiaadresse kogub ja ongi käes see olukord kus inimese enda aadressiga saadetakse rämpskirju välja pahavara poolt ilma, et inimene sellest üldse midagi teaks.

- Kui vähegi võimalik siis ei soovita kasutada MS Windowsi! Tasuta ja oluliselt töökindlam (pahavara suhtes sisuliselt immuunne) on näiteks eestlaste Estobuntu! See toetab kohe ID-kaarti, multimeediat jne ning on eestikeelne ja -meelne. Või ka Ubuntu Estonian Remix.
- Microsoft Windowsi pahavara tõrjumisel on viimasel ajal Microsoft Security Essentials silma paistnud. Kui minna aadressile http://windows.microsoft.com/et-EE/windows/products/security-essentials ja vajutada seal seda suurt sinist nuppu "Download now" siis saab valida sobivas keeles oma Windowsi versioonile sobiva. Seda Microsofti viirusetõrjet tohib kasutada kõikjal kus on legaalne Windows - kodus, tööl, firmas jne. Paigaldamisel sooritatakse legaalsuse kontroll ja kui on legaalne siis paigaldatakse, uuendatakse ja saab kasutada. Mitut viirusetõrjet ei ole mõistlik pidada - eelnevalt siis tuleks teine viirusetõrje eemaldada. Eemaldamisel tuleks eemaldada kõik, mida pakutakse eemaldamiseks (sh karantiin vms). Peale seda enamasti palutakse ka taaskäivitus teha. Peale seda siis saab uue pahavara tõrje paigaldada. Lisalugemist leiab siit.

Failide veebipõhine kontroll pahavara suhtes - https://www.virustotal.com/et/

Turvalise veebilehitsemise alustamine:

- Soovitan kasutada eestikeelset Firefoxi - http://www.mozilla.org/et/firefox/
- Paigalda Firefoxi lisand reklaamide eemaldamiseks http://adblock.ee/
- külasta mõnda lehte, kus tavaliselt on palju reklaame - need on nüüd läinud!

Lisaturvalisust saab *Noscript* nimelise lisandiga Firefoxile - https://addons.mozilla.org/en-US/firefox/addon/722
See lisand takistab *JavaScript*-i ja *Flash*-i töötamise ning neid saab ka tööle lubada kui usaldate konkreetset veebilehte.

Teistele keeltele Adblock nimekirjad:

- http://adblockplus.org/en/subscriptions
- http://www.adblocked.eu/

NB! Windowsi kasutajad! Teile soovitan kasutada lisaks sellist programm kui KeyScrambler - http://www.qfxsoftware.com/
See toimib ka erinevates veebilehitsejates.
Seal on ka tasuline versioon kuid see *Personal* on tasuta. Lisainfot, mis vahe on tasuta ja tasulisel, leiab siit.

Lisalugemist turvalisusest leiab arvutikaitse.ee lehelt