EGA JUMAL POLE KIIRET LOONUD, JUMAL ON HIIRED LOONUD.

EESTI VANASÕNA

RAAL

Internetiohutuse põhitõed

LOORE LUGU

**Tere, siin kübertark Loore.
See oli nüüd nali. Minusuguseid pensionieelisi nimetatakse mitte kübertarkadeks, vaid pigem elutarkadeks.**

Aga õigusega. Keeruliste eluliste olukordade lahendamist ja üldse elukogemust noorena ette ära õppida ei saa — niisugust kooli või programmi pole suudetud luua. Ikka tuleb oma rõõmud, mured ja raskused isiklikult läbi elada ja läbi nende elutargemaks saada.

Kui küsite, millised on mu suhted kübermaailmaga või digitaalse maailmaga, siis vastan, et head. Küberrumal või küberhull ma ei ole. Ma kuulan vahel raadiost isegi selleteemalisi saateid, et targemaks saada. Infot oskan internetist otsida, sellega töötada ja seda edasi anda. YouTube'ist vaatan kontserte ja oma noorusaja lemmikpoplugusid. Skype on ja e-kirju kirjutan päris palju, Facebooki konto on ka olemas. Twitterit ja Instagrami mul ei ole, kuna ei ole tundnud mingit vajadust nende järele.

Loomulikult olen ma väga palju kordi kuulnud, et mitte ühelegi inimesele ei tohi anda oma pangakonto paroole isegi siis, kui inimene ütleb, et ta on pangast ja ta väga muretseb sinu pärast või väga armastab sind. Ma tean, et mitte ükski pank ei küsi mitte kunagi kellegi paroole. Mulle ei ole ka õnneks helistanud keegi, kes n-ö soodsat investeerimisvõimalust

pakuks, kuigi mul niisugustele sulidele äraütlemisega mingeid raskusi ei tuleks. Oh, mis ma räägin, e-kirju tuleb välismaalt kogu aeg, et keegi tahab minuga võhivõõra inimese pärandust jagada, aga selle kättesaamiseks on vaja teatud summa maksta teisele võhivõõrale inimesele. Need mured, kuidas raha on nii palju, et seda peab täiesti võõraste välismaalastega jagama, on lihtsalt lõbusad vahepalad.

Erinevate paroolidega, e-posti või Facebooki omadega, on mul olnud selline suhe, et kuigi ma kuulsin kogu aeg hoiatusi, et need tuleb teha äraarvamatud, ei kartnud ma midagi, sest midagi polnud juhtunud ja ma mõtlesin, et midagi ei saa ju juhtuda. Minu salasõnad olid minu nimi ja sünniaasta.

Ühel kolleegil kaaperdati aga ühel päeval Facebooki konto ära ja sealt hakati saatma laenusaamise palveid. Õnneks olid kirjad tõlgitud Google'i tõlkega ja kolleegi sõbrad, kellega ta iga päev ei suhelnud, said kohe aru, et asi on veider, kuna õpetaja on päevapealt kaotanud eesti keele kirjutamise oskuse. Meile rääkis ta juhtunust ise, kui tööle tuli. Kui ma õigesti mäletan, siis õhtuks sai ta oma konto tagasi. Kui midagi niisugust juhtub, ärge hakake nutma, vaid pöörduge asjatundjate poole ja teavitage teiste kanalite kaudu võimalikult paljusid sõpru.

Pärast seda sündmust ma nii muretu oma paroolidega enam ei ole. Mul on oma süsteem, millega ei ole raske neid meeles pidada, aga teistel ei ole võimalik neid ära arvata.

Üldiselt arvan ma, et mida vähem oma eraelu näiteks Facebookis eksponeerida, seda parem. Kord paari kuu järel olen mõnest minuga juhtunud toredast loost kirjutanud ja vahel töökaaslased panevad fotosid meie mõnest üritusest, siis eks ma ka olen seal peal ja mul pole selle vastu midagi. Aga oma isiklikku elu ma ei tutvusta. Näiteks kui lapsed või lapselapsed mul külas käivad, siis me ei pane kohe ühisfotot üles. Las nemad otsustavad oma elu üle ise siis, kui nad suured on.

Soovin kõigile kainet meelt kübermaailmas liikumiseks.

Hügieen arvutis: mis, miks ja kuidas?

Arvutid, nutitelefonid ja internet on saanud elu lahutamatuks osaks – seepärast on vältimatu nende kasutamisel korralikku hügieeni pidada. Kuid me ei räägi arvuti klaviatuuri puhaste kätega katsumisest! Küberhügieen on kogum põhimõtetest, hoiakutest ja teadmistest, mis aitavad hoiduda pettustest, õngevõtmistest, arvutiviirustest ja andmete lekkimisest, mille tagajärjed võivad olla valusad nii iseendale kui ka lähedastele.

Parool ehk salasõna

Kõik algab turvalistest paroolidest ehk salasõnadest. Parool on nagu lukk uksel, mis hoiab võõrad eemal meie isiklikust ruumist. Erinevalt päris maailmast, kus meie koduukse lukus olemist võib katsuda ainult meie kodutänavale sattunud kahtlane isik, on internetis kogu maailm omavahel ühendatud ja meie parooli turvalisust võivad katsuda kogu maailmas olevad kahtlased isikud.

Õnneks on turvalise parooli loomine lihtsam ja kiirem kui ukseluku vahetamine. Asjatundjate värskeimate soovituste kohaselt tuleks lihtsa salasõna asemel kasutada „salafraasi": pange kokku kolmest-neljast sõnast koosnev fraas, sõnade vahele võib pikkida tühikuid (jah, salasõnas võib olla ka tühik) või kirjavahemärke. Oluline on, et sellises salafraasis poleks inimese enda andmeid, sest nime või aadressi kaudu parooli äraarvamine on lapsemäng. Ideaalis on selline salafraas paar suvalist sõna, mõni kirjavahemärk ja number, mis võõrale on ebaloogiline, aga salafraasi omaniku jaoks on nende vahel seos ja nii püsib see hästi meeles.

Tasub meeles pidada, et erinevatel internetiteenustel ei tohiks kasutada sama salasõna, vaid mõelda iga koha jaoks välja eraldi salasõna – nii on kindlam, et isegi kui kurikaelad ühe salasõna kätte saavad, ei saa nad sama salasõna kasutades üle võtta ka teisi kontosid ja teenuseid. Niisiis tasub näiteks e-postkastil ja Facebooki kontol hoida erinevaid salasõnu.

Mitmeastmeline autentimine on veel turvalisem

Parool võiks koosneda kolmest-neljast sõnast, mille vahele on pikitud tühikuid või kirjavahemärke. Ära kasuta paroolis oma nime ega aadressi!

Korralikud teenused kasutavad tänapäeval ka mitmeastmelist autentimist ehk siis saab näiteks meilikonto turvalisust seadistada nii, et kontole ei pääse isegi siis, kui keegi teie salasõnale ligi on saanud. See käib nii, et telefoni tuleb sõnum, mis saadab kas unikaalse koodi või küsib üle, kas te ikka soovite sellesse teenusesse sisse pääseda. Kontole pääseb aga ligi alles pärast seda, kui konto omanik on selleks nõusoleku andnud. Kui sa aga ise midagi arvutiga teinud ei ole ja tuleb arusaamatu kood, peaksid minema ja oma salasõna ära vahetama. Mitmeastmeline autentimine on kindlasti hea soovitus ja kui ise sellega hätta jääd, saavad ehk asjatundjamad appi tulla.

Kui salasõna on turvaline ehk lukk tugev, on muretum internetis tegutseda. Ent nii nagu füüsilises maailmas teeme me vahet, kas oleme tänaval või kodus, tuleks pidevalt sama meeles hoida ka internetis.

Mida internetti riputada?

Näiteks tähendab see arvestamist, kas pilt või postitus Facebookis on nähtav kogu maailmale või ainult perele ja tuttavatele. Nii nagu me ei riputa iga mõtet, fotot ja infokildu maailmale lugemiseks oma välisuksele, ei tasu teha seda ka internetis. Küberkurjategijad korraldavadki oma pettusi ja kelmusi avalikult leitava info põhjal. Lisaks võib avalikult tegutsedes panna piinlikku olukorda oma lähedased, kui näiteks lapselapse sünnipäevaks tema seinale postitada beebieas foto ja seda näevad ka kõik võõrad.

Võtmeküsimus on ära õppida see seadistus, kus saab väga täpselt määratleda, kes mingit postitust näeb. Nii paigutame ennast virtuaalselt kas privaatsfääri või avalikku ruumi.

Postituste tegemisel tuleb alati arvestada asjaoluga, et kõik sinna riputatav võib sinna jääda määramatuks ajaks. Isegi kui ise seda kohe üles ei leia, on inimesi, kes valdavad kavalaid nippe ja programme, mis on keerulisemad kui tavapäraste otsingumootorite kasutamine. Nii on võimalik internetist leida asju, mis juba ammu meelest läinud või kadunud.

Ettevaatust petturitega!

Interneti avaliku ruumiga kaasnevatest ohtudest käivad kõige valusamalt rahakoti pihta need, kus pettuse, teeskluse või manipulatsiooniga püütakse heausksetelt inimestelt raha välja meelitada. Näiteks võib ühendust võtta „panga esindaja", kes pakub soodsat võimalust investeerida; „IT-firma esindaja", kes on tuvastanud ohvri arvutis probleemi ja püüab aidata; „abivalmis võõras", kelle sõnul on lapselaps või lähedane hädas ja sellest pääsemiseks on vaja raha; „lotofirma esindaja", kes teatab võidust; „politseinik", kes teatab õnnetusest. Sellised kõned ja kirjad on jultunud katsed meelitada või lausa ähvardada nii kaua, kuni ohver teeb pangaülekande või maksab muudmoodi.

Peenemat sorti pettused on sellised, et raha ei küsita otse, vaid palutakse oma arvutisse laadida uus tundmatu programm. Sellega saab kurjategija sinu arvuti üle kontrolli. Kui aga võimalikul ohvril on ID-kaart, mobiil-ID või Smart ID, siis püütakse välja meelitada PIN-koode või panna inimest tahtmatult digiallkirja andma. Mitte kunagi ei tohi sellist võõrast usaldada ja kindlasti tuleks sellisest kõnest teada anda nii lähedastele kui ka politseile.

Iga petuskeemi ei ole siiski võimalik ennetavalt ära õppida, mistõttu tuleks järgida lihtsat rusikareeglit: enne kellelegi raha või PIN-koodide andmist või oma arvutisse tundmatu faili laadimist pea kindlasti nõu arvutiasjades tugevama lähedasega või otse politseiga. Nii saab suure tõenäosusega suurt kahju ennetada.

Samamoodi nagu arvutiga tuleb olla ettevaatlik ka nutitelefonide ja tahvelarvutitega, sest needki on ju tegelikult arvutid. Nii ei maksa vajutada ka lühisõnumina tulnud arusaamatutele linkidele, kui ei ole teada, kellelt need tulevad.

Kahtlastest kõnedest ja kirjadest anna teada politseile ja oma lähedastele.

Ära häbene, kui oled hätta sattunud

Kui oled hoolimata oma ettevaatlikkusest ja heal tasemel küberhügieenist siiski hätta sattunud ja mõni kavalpea on su kontole ligi pääsenud, siis ära häbene sellest teada anda politseile ja Riigi Infosüsteemide Ameti spetsialistidele või rääkida sellest usaldusväärsete inimestega. Küberkurjategijad võivad välja pressida ka valega ja inimeste häbile rõhudes. Näiteks võidakse väita, et oled käinud mõnel piinlikkust valmistaval internetilehel ja su tegevus on salvestatud ning see info saadetakse su tuttavatele, kui sa kurjategijatele raha üle ei kanna. Selliseid petuskeeme on palju kasutatud ja isegi kui inimesed neil lehtedel käinud ei ole, muutuvad nad siiski murelikuks ja võivad alluda väljapressimisele. Kurjategijate eesmärk ongi inimeste ebakindlust ära kasutades kasu teenida.

Juhul kui midagi sellist juhtuma peaks, teata kindlasti politseile spetsiaalselt selleks avatud veebileheküljel cyber.politsei.ee või telefoni teel. Riigi Infosüsteemide Amet ootab igasugustest küberintsidentidest teateid leheküljel raport.cert.ee.

Kui soovid põhjalikumalt teada, kuidas ennast internetis valitsevate ohtude eest kaitsta, soovitan tasuta eestikeelset küberhügieenikursust aadressil mycyberhygiene.com/et.

PEA MEELES!

- **Kasuta tugevaid salasõnu – igal kontol erinev salasõna!**
- **Facebook ja muu sotsiaalmeedia on avalik ruum – mõtle, mida postitad!**
- **Vaata ette, kuhu klikid või mida oma seadmesse laed!**
- **Ära usu võõraid „heategijaid", kes üritavad õngitseda su andmeid!**

Kasulik teave!