KÜBERHÜGIEENI TEEMALINE ÕPITUBA

SISSEJUHATUS

Me elame ajastus, kus me sõltume tehnoloogiast ja elu ilma selleta tunduks peaaegu võimatu. Ent tehnoloogia järsu arenguga viimase paarikümne aasta jooksul, käib kõikide nende mugavuste ja innovaatiliste lahendustega kaasas ka ohud, riskid ja kahjud. Nutiseadmed on saanud meie lahutamatuks parimaks sõbraks, sest me saame kiirelt ja mugavalt teha tähtsaid toimetusi sammu pealt. Peaaegu kogu meie elu on üle kolinud internetti ja andmebaasidesse. Interneti kõikvõimas olemus on tegelikult haavatavam ja ohtlikum, kui meile pealtnäha tundub.

ÕPITOA EESMÄRK:

- Miks ja kuidas kaitsta enda andmeid seadmetes
- Anda lühiülevaade internetis ringluses olevatest pahavaradest
- Suunata turvalisemalt ja viisakamalt käituma internetis

AKTUAALSUS: Euroopa noorte interneti harjumused

EU Kids Online (Livingstone, Haddon, Görzig, & Ólafsson, 2010) uuring, mille eesmärgiks oli internetiturvalisuse teadusliku tõendusmaterjali kogumine näitas, et intervjueeritud 25 Euroopa riigist 25 142 last, on 21% 11-16 aastastest lastest on kokku puutunud ühe või enama 4 potentsiaalselt kahjuliku veebisisu tüübiga, 9% samas vanusegrupis on kokku puutunud nende isikuandmete väärkasutamisega. Laste interneti kasutamisharjumus kujuneb üha enam nooremas eas – keskmine esmasurfaja vanus on Taanis ja Rootsis 7 aastat ja kaheksas teises Põhjamaa riigis 8 aastat. Kokku kasutab internetti igapäevaselt üks kolmandik 9-10 aastastest lastest, 15-16 aastaste seas tõuseb see näitaja 80%. Vähemalt iganädalaselt kasutab internetti 93% 9-16 aastastest lastest ning samas vanusegrupis 60% kasutab iga päev või peaaegu iga päev. 59% 9-16aastastest lastest omavad suhtlusportaalis profiil. 26% on 9-10aastastel lastel profiil, 49% 11-12 aastastel, 73% 13-14 aastastel ja 82% 15-16 aastastest. Suhtlusportaalide kasutajate hulgas on 26% avalikud profiilid ehk seda võivad näha kõik ning 28% väidavad, et nende profiil on osaliselt privaatne, mis on nähtav sõprade sõpradele.

KÜBERHÜGIEEN

Küberhügieen - hoolikalt läbi mõeldud inimese kui ka asutuste enda andmete kaitsmine, privaatsuse ja turvalisuse tagamine küberruumis.

Küber – pole täielikult defineeritud, kuid see tavaliselt liidetakse mingi põhisõna juurde, luues põhisõnale uus alaliik.

- Küber + oht -> küberoht
- Küber + turvalisus -> küberturvalisus

Hügieen – teadusharu, mis tegeleb tervise edendamisega ning säilitamise, läbivaks ideeks on tervise sälilitamine ja tervislikult elamine

SEADMETE KAITSMINE

Arvuti ja nutiseadmed on täpselt samasugune vara nagu meie kodu – me lukustame lahkudes kodu uksed ja aknad, et võõrad ei pääseks sisse. Nii nagu meie kodu, sisaldavad ka meie seadmed meie kohta isiklikke andmeid ja informatsiooni, mis võiks jääda meie teada ja ainult meie seadmetesse. Keegi meist pole õnnelik, kui meie koju tungitakse sisse ja võetakse kaasa asju, eriti veel asju, millel on suur tähendus ja mida ei saa uuesti osta, näiteks pildid vanavanematest või lapsepõlve pildid. Kuid kaitsmata arvuti pakub soodsaid võimalusi kurjategijatel selle teostamiseks.

KUIDAS KURJATEGIJAD JÕUAVAD SINUNI?

Väga paljud kurjategijad võivad üritada tungida sinu seadmesse operatsioonisüsteemis või rakendusprogrammides olevate turvaaukude kaudu ning sinna nad jõuavad ebaturvaliste veebilehtede, alla laetud rakenduste või isegi e-maili kaudu.

Created by Adriana Danaila
from Noun Project

Security Breach by Adriana Danaila from the Noun Project

PAHAVARA

Pahavara tuntakse ka kurivara nime all ja nagu ütleb ka nimi, ei ole tegemist heatahtliku tarkvaraga. Pahavaraks nimetatakse sellist tarkvara, mis üritab tungida omaniku teadmata kasutaja arvutisse või teise seadmesse selle kahjustamiseks. Pahavara on mitut liiki: troojalased, ussid, lunavara, reklaamijad ja palju muud.

PAHAVARAST ÜLDISELT

Pahavara kirjutavad inimesed, keda ajendab uudishimu või soov tekitada teistele kahju ja saada raha. Satub arvutisse turvaaukude kaudu. Kahju suurus sõltub pahavara liigist. Kuna tänapäevaks on neid nii mitut liiki tekkinud, siis iga pahavarale on omane oma kahju tekitamise viis

LUNAVARA

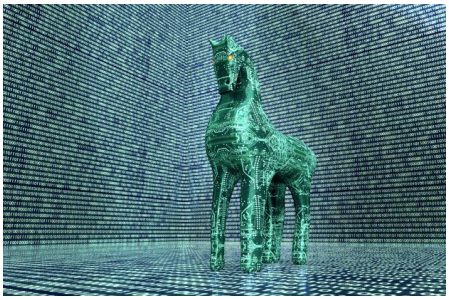
Lunavara tuntakse rohkem ingliskeelse nimetuse all *ransomware*, kuid seda tuntakse ka krüptoviirusena. See on selline pahavara, mis krüptib kasutaja arvutis, kas teatud failid või kogunisti terve kõvaketta ja nõuavad lahti krüpteerimise ees lunaraha. Ehk lunavara lukustab sinu failid, millele enne said ligi ja neid vaadata, ja kui nüüd tahad uuesti neile ligi ja neid vaadata, peab sul olema selleks võti, et need lahti lukustada. Selleks on kurjategijad loonud šifri ehk võtme, millega saab lukustatud failid jälle loetavaks teha. Kuid võtme saamiseks, nõuavad kurjategijad raha, mis muidugi ei garanteeri seda, et ohver saab ka päriselt võtme failide avamiseks.

Lunavara liigitatakse omakorda veel lukustaja-lunavaraks ja krüpto-lunavaraks. Neil kahel on sama omadus krüpteeritud asja eest nõuda lunaraha, kuid nende erinevus seisneb selles, et lukustaja-lunavara lukustab kogu arvutisüsteemi ja muudab arvuti kasutamiskõlbmatuks ja krüpto-lunavara lukustab ainult seadmes olevad failid, kuid kasutaja pääseb arvutile endiselt ligi.

http://nationalinterest.org/blog/the-buzz/made-north-korea-the-wannacry-ransomware-attack-20686

TROOJALANE

Troojalast kutsutakse ka Trooja hobuseks ja selle pahavara omaduseks on see, et see sokutab ennast arvutisse pealtnäha süütu rakendusena, kuid käivitamisel hakkab see kahjustama arvutit. Nimi tuleneb vanakreeka mütoloogiast, kus kreeklased kinkisid Trooja linnale hiiglasliku seest tühja puust hobuse, mille sees peitsi ennast kreeklased ja öösel ründasid Trooja linna. Tavaliselt kasutatakse selliseid programme isikliku informatsiooni varastamiseks kasutaja iga klahvivajutuse jälgimisega. Varastatakse näiteks krediitkaardi numbreid, paroole või muud sensitiivset informatsiooni. Troojalasi kasutatakse ka teiste viiruste levitamiseks või lihtsalt arvuti sooritusvõime halvendamiseks. Troojalane võib sattuda arvutisse e-kirjades olevate manuste või linkide kaudu, ebaturvaliste veebilehtede või reklaamiga täidetud hüpikakende kaudu või on rakendustesse sisse ehitatud.



https://blog.eset.ee/wp-content/uploads/2017/02/shutterstock_397755184-623x410.jpg

USSVIIRUS

Ussviirus erineb märgatavalt teistest pahavaradest oma levimisviisi poolest. Kui tavaliselt arvutiviirus haagib end mõne teise programmi külge ja vajab levimiseks kasutaja kaasabi, siis uss on võimeline levima ja paljunema iseseisvalt, kasutades rakenduste või operatsioonisüsteemi turvaauke. Ussiga nakatunud arvuti võib pealtnäha tunduda täiesti korras, kuid tegelikkuses kontrollib arvutit võrgus asuv küberkurjategija. Samuti ummistavad võrke ja aeglustavad arvuti sooritusvõimet. Üks usside salakavalamaid levimistaktikaid on saata välja ohtliku manusega meilisõnumeid kõigile nakatatud kasutaja aadressiraamatus sisalduvatele aadressidele. Sellisel moel maskeerib uss end usaldusväärselt sõbralt tulnud meiliks.

https://www.hs-academypages.com/hubfs/lp/academy/computer-worm.png

NUHKVARA

Enamjaolt sõltub nuhkvara tegevus kurjategija eesmärgist. Mõni tahab ära kasutada isikuandmeid, mõni tahab lihtsalt koguda infot ohvri brausimisharjumustest. Saadud infot võidakse ära kasutada näiteks turunduseesmärkidel ja tuua endaga kaasa tohutus koguses rämpskirju. Seega, mitte kõik nuhkvarad tegelevad delikaatsete andmete kogumisega, seega nad ei riku su privaatsust. Mõni reklaamitarkvara peaks samuti kuuluma nuhkvara hulka, kuid on tegelikult seaduslik reklaamitarkvara. Nuhkvara levib arvutisse eksitava kasuliku tarkvara nime all. Näiteks mingisugused programmide laiendused või uuendused, nuhkvara otsiva programmina, kuigi tegelikult eemaldab teised nuhkvarad, et saaks ise jälgida kasutajat, veebilehitsejate turvaaukude kaudu. Näiteks suunab kurjategija ohvri pahavaralistele veebilehtedele ja viskab ette ebaturvalisi hüpikaknaid ja kui kasutaja külastab mõnda sellist veebilehte, laeb nuhkvara ennast ise arvutisse. Viimasest näitest saab ka öelda, et nuhkvara levib teiste pahavarade kaudu.

ÕNGITSEMINE

Õngitsemise käigus üritatakse kasutaja inimpsüühikaga manipuleerida nii, et ta annaks ise oma juurdepääsuandmed ja paroolid ja muud informatsiooni kurjategijale. Õngitsemist tehakse nii-öelda söödaga. Näiteks võidakse kasutajale saata e-mail, kus teenusepakkuja palub sisestada nende kodulehele oma andmed. Tegelikkuses on koduleheks teise teenuse välimust kopeeriv leht. Kui kasutaja sisestab sinna lehele oma andmed, arvates, et see turvaline ja jõuabki õigesse kohta. Tegelikult on tegemist plagiaat lehega, kus andmed jõuavad hoopis kurjategijani. Tänapäeval on see üks levinumaid küberkuriteo vorme, kuid see on ka üks lihtsamini tuvastatav ja välditavam. Luku ikoon aadressiriba kõrval ning https:// aadressi alguses näitavad, et leheküljel kasutad turvatud ühendust.

https://www.denestor.be/wp-content/uploads/2017/05/phishing.jpg

ESIMESED PAHAVARAD

BRAIN VIIRUS

1986. aastal pidasid kaks venda Istanbulis arvutipoodi, kus müüsid edasi floppy diskidel tarkvara arvutitele. Kui nad said teada, et nende kirjutatud tarkvarast tehakse koopiaid ja antakse edasi teistele, tahtsid nad anda õppetunni ostjatele. Nad lõid viiruse Brain, et kaitsta oma tarkvara piraatluse eest ja oli suunatud autoriõiguste rikkumise vastu. Nad ei varjanud oma identiteeti ja panid viirusesse kirja enda nimed, aadressi, telefoni numbri ja ettevõtte nime, et nakatunud kasutajad saaksid ühendust võtta.

THE MORRIS WORM

1988. aastal lõi ülikooli õpilane Robert Tappan Morris ussviiruse, et mõõta Interneti suurust. Tema eesmärk polnud teha kahju, kuid tema uudishimu tõttu aeglustas see arvutite tööd nii palju, et arvutit muutusid kasutuskõlbmatuks.

AIDS TROJAN

1989. aastal lõi teadlane ja AIDSi uurija dr. Joseph Popp trooja-lunavara, mis pidid analüüsima kasutaja riski saada AIDS. Pealtnäha tunduski pahavara süütu programmina, kuid peale 90. arvuti käivitamist krüpteeris viirus failid ja nõudis nende tagasi saamiseks raha. Saadud raha annetas ta AIDSi uuringuteks.

KUIDAS KAITSTA OMA SEADET?

1. VIIRUSETÕRJETARKVARA JA TULEMÜÜR

Viirusetõrje on tavaliselt kõige esimene ja kõige võimekam kaitsja sissetungijate eest. Tavaliselt see sisaldab juba tulemüüri, reklaamvara tõrjujat, spämmifiltrit ja vahendeid kahjustunud failide ning operatsioonisüsteemi taastamiseks. Tulemüür otsustab, millistel rakendustel on õigus meie arvutisse siseneda ja millistel mitte. Tulemüürina on võimelised käituma ka WiFi ruuterid. Suure tähtsusega on nende pidev uuendamine, sest teenusepakkujad üritavad alati pakkuda kõige paremat ja usaldusväärsemat tarkvara.

2. OPERATSIOONISÜSTEEMIDE JA PROGRAMMIDE UUENDAMINE

Eelnevalt saime juba teada, et paljud arvutitarkvarad ja operatsioonisüsteemid sisaldavad endas turvaauke, mis on jäänud loojatel kahe silma vahele. Selleks, et pakkuda head ja kvaliteetset toodangut, mis töötaks korralikult, proovivad tootjad leida ja parandada turvaaugud võimalikult kiiresti. Seega iga uuendusega proovitakse veel paremaks muuta oma tarkvara või süsteemi ja likvideerida võimalikult palju turvaauke.

3. KONTROLLI, KUST MIDA LAED

Tihti peale võib juhtuda nii, et me pole isegi teadlikud, kui meie arvuti on midagi laadinud, külastades ebaturvalisi veebilehti. Kõige turvalisem on alla laadida programme nende kodulehekülgedelt või osta. Me ei saa kunagi kindlad olla, mis võib olla kaasa pandud teistele mitte usalduslikele failidele. Enne failide käivitamist kontrollida üle, kas fail on ikka turvaline: http://cuckoo.cert.ee/.

4. EBATURVALISED E-KIRJAD JA LEHEKÜLJED

Kui meilile tuleb tundmatult isikult kiri, mille tekst on vigane ja ebausaldusväärne, siis kohe kindlasti mitte avada kirjale lisatud manuseid ja linke. Kohe kindlasti seda mitte teha, kui kiri on su sõbralt, aga on võõrkeeles või ebaselge. Küsige üle, kas ta teab saadetud kirjast midagi. Samuti konsulteerida kellegi targemaga!

5. VARUKOOPIAD

Varukoopiate tegemine pole kasulik ainult küberründe puhul, vaid ka sisse löönud pikne võib hävitada fotokogu, e-kirjad ja palju muid. Seda saab ennetada, tehes varukoopiaid eraldi välisel andmekandjal, sest küberkurjategijad saavad pilve laetud koopiaid ka kätte, kui need on samas internetivõrgus.

6. TUGEVAD PAROOLID

Kui kasutate paroolina keerulisi tähtede ja numbrite kombinatsioone, on suurem tõenäosus, et sissetungija ei jõuagi parooli lahenduseni ning paneb sissetungija oma ettevõtmisest loobuma.

7. ADMINISTRAATORI KONTO JA KOHALIK KASUTAJA

Luua arvutile kaks kasutajat: administraatori ja kohalik kasutaja. Administraatori kasutajat kasutada siis, kui on vaja teha muudatusi arvutis, mille jaoks pole kohalikul kasutajal õigus. Muuta kohaliku kasutaja õigused nii, et tehes kohalikus kasutajas suuri muudatusi, küsib see enne administraatori kasutaja luba. Kui kohalikus kasutajas üritab mingi viirus ennast alla laadida ja käivitada, siis selle käivitamiseks küsib ta administraatorikasutaja luba.

SOTSIAALMEEDIA

Interneti sotsiaalvõrgustik on virtuaalne kogukond, kus inimesed suhtlevad, loovad ja jagavaid ideid või teavet. Sotsiaalmeedia kanalite kaudu saame vahendada hetke emotsioone, pilte, tegevusi, uurime teiste inimeste tegevuste, emotsioonide ja mõtete kohta, loeme uudiseid, saame uusi teadmisi ja palju muud. Paljud inimesed kasutavad sotsiaalmeediat meelelahutusena, informatsiooni saamiseks või turunduses. Võimalusi sotsiaalmeedia kasutamiseks on seinast seina. Kõik need on lihtsustanud meie elu ja teinud meile informatsiooni kergesti kättesaadavamaks. Kuna sotsiaalmeedia annab meile peaaegu vabad käed tegutseda ja uurida internetivõrgustikus ringi, kaasneb selle kõigega väga palju riske ja ohtusid – valeinformatsioon, petlikud reklaamid, võlts ettevõtted, väljapressimised jms. Et ohutult ja turvaliselt ringi liikuda, peab meeles pidama mõningaid punkte, millele toetuda.

PROFIIL

Profiili loomine küberruumi on virtuaalse sina loomine – sa esindad ennast küberruumis. Profiili luues peab läbi mõtlema mitmetel küsimustele, enne kui midagi avaldad.

- Kes su profiili vaadata saavad? Kas see on kõigile vaatamiseks?
- Mis infot sa enda kohta avaldad?
- Mida sa enda kohta internetti postitad? – pildid, postitused, videod
- Kas sul on täielik kontroll kes sinu asju näevad või ei?

Profiili luues ära sisesta liigselt isiklikku informatsiooni, kui see pole vajalik, näiteks telefoni number, kodune aadress, pangakonto andmeid ja muu sellist. Samuti ära avalda informatsiooni ka oma lähedaste kohta. Me ei saa kontrollida täielikult kuhu ja kelleni meie isiklik informatsioon võib jõuda. Ei ole vaja avaldada liigset informatsiooni kõikidele lugemiseks, mis hiljem võib kahju tuua.

PRIVAATSUS

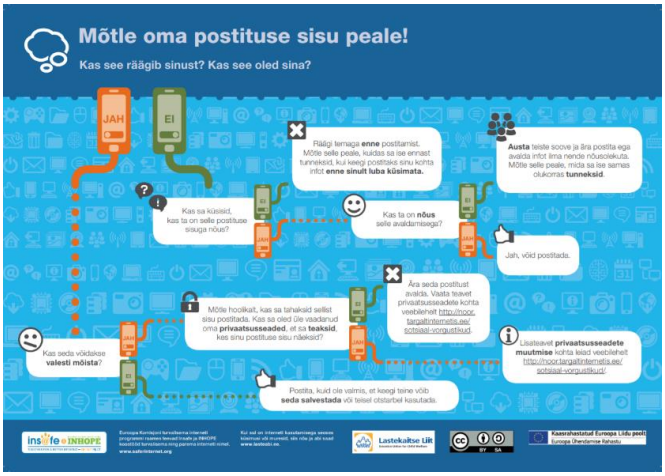
Sotsiaalmeedias on lihtne suhelda sõprade ja tuttavatega erinevate suhtluskanalite kaudu nagu näiteks Facebook. See on mugav ja kiire viis võtta ühendust oma sõpradega või lisada endale juurde uusi sõpru. Tihti peale ei ole meie sõbralistis ainult inimesed, keda me päriselt teame, vaid ka inimesed, keda me teame oma sõprade-sõprade kaudu ehk kaudselt. Sellega kaasneb suurem kohusetunne mõelda oma privaatsuse peale, sest me ei tea, kes need inimesed õigemini ongi ega saa neid usaldada. Sealt tekib küsimus, et miks me oleme internetis sõber inimestega,

keda me päriselt ei tunnegi? Kas tegelikult on vahet, kui me nad sõbralistist kustutaks või ei lase ennast kuskil mujal jälgida? Kas on mõistlik jagada kõiki postitusi võõrastega, keda me isegi ei tunne? Samuti kehtib see ka inimeste kohta, keda me päriselt teamegi. Kui ei raatsi piirata oma sõprade arvu või kui sul on sõbralistis ainult inimesed, keda sa ka päriselt tead, siis ei tee see halba ikkagi üle vaadata oma privaatsusseaded.

http://noor.targaltinternetis.ee/wp-content/uploads/2015/12/Decision-tree-2_ET_trykk.pdf

POSTITUSED

Enne postitamist mõtle alati läbi, kas see on sobilik, kas seda võidakse valesti mõista, ega see pole solvav ja kas see võib olla kõigile nähtav või pigem võiks jääda see teatud ringkonnale. Et hoiduda probleemidest, mitte postitada ka ebaseaduslikku ja rõvedat teksti. Samuti pole mõtet postitada asju, mida päris elus ei julge öelda. Enamus sotsiaalvõrgustikes saab kontrollida, kes postitusi näevad ja alati saab ka saata inimestele privaatselt informatsiooni, pilte ja videoid. Tähtis on meeles pidada, et postitusi saab mitmel erineval viisil salvestada läbi erinevate funktsioonide näiteks *screenshottides* ehk kuvatõmmise tegemine ja kui see korra on juba postitatud, siis ei saa kindel olla kas keegi on selle endale salvestanud.

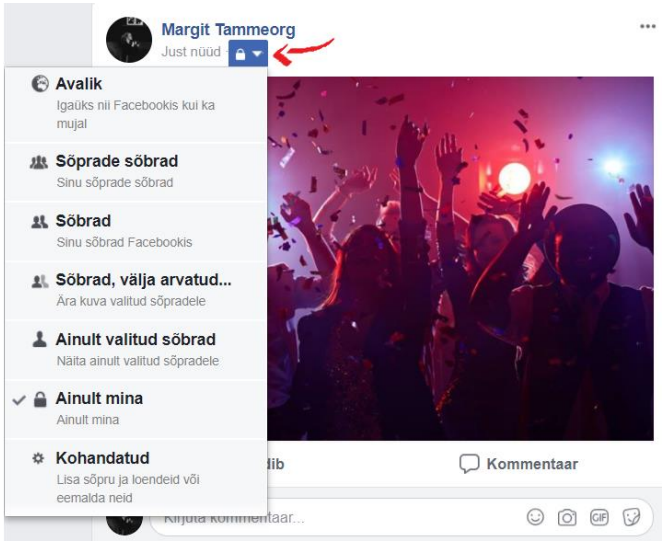


http://noor.targaltinternetis.ee/sotsiaal-vorgustikud/

POSTITUSED – PILDID JA VIDEOD

Internetti üles laetud pilte on raske kontrollida, kelleni need võivad jõuda. Need võivad hakata kiirelt levima ja elama täiesti oma elu. Me ei tea kunagi, kes on pildist koopia teinud või *screenshottinud* ehk kuvatõmmise teinud ja kelleni see võib olla levinud? Pilt või video, mis tundus tol hetkel naljakas, võib lõpus teha kellelegi või isegi sulle väga haiget, kui see satub pahatahtlike inimeste kätesse, mis võib isegi viia kiusamiseni. Kuid positiivne on see, et nii Facebookis, Youtubes, Instagramis, Snapchatis ja igalpool mujal saab tegelikult kontrollida, kes sinu postitusi näevad või kes sind *followida* ehk jälgida saavad ja selle funktsiooniga saab piirata postituste publikut. Kuid see ei garanteeri alati, et need ei lähe levima. Siiski pole välistatud kuvatõmmise ja screen recorder võimalus.

Enne postitamist peab läbi mõtlema enda peas küsimusi, kas pilt on sobilik ja mitte solvav? Kas see tekitab piinlikust sulle või kellelegi teisele ja kas see on alandav? Kas see võib sulle kunagi tulevikus tekitada piinlikust? Kas need võivad tulevikus takistada sul saavutada mõningaid eesmärke, näiteks saada töökoht või kooli? Kas need võivad õhutada kedagi kiusama? Kas pilt sisaldab seadusega vastuolulist informatsiooni, näiteks alaealised alkoholi tarbimas või suitsu kimumas?



KOMMENTEERIMINE

Kommentaarid näitavad inimeste seisukohti ja arvamusi, ent tihti peale ei ole meeles kõigil, et avalikult kommenteeritud postitused on kõigile nähtavad ja võivad tekitada suuri probleeme. Väga paljudes uudiste portaalides sai vanasti kommenteerida anonüümselt, mis viis selleni, et inimeste kommentaarid olid väga ebasündsad, ebaviisakad ja rõvedad, ei vastanud Eesti Vabariigi seadustele või rikkusid kolmandate isikute õigusi. Näiteks keelas Postimees 2016. aastal anonüümse kommenteerimise. Anonüümsuse kaotamisega pidid inimesed hakkama

võtma vastutust oma sõnade eest. Avalikult oma nime alt kommenteerides peab olema ettevaatlik, sest sinu nimi on kõikidele nähtav ja sa pead vastutama täielikult oma sõnade eest. Kuid siiski leidub väga paljude interneti postituste all ebameeldivaid kommentaare, kus halvustatakse põhjendamatult teisi isikuid, rasse või on ebasündsad teiste suhtes. See tähendab seda, et probleem pole lahendatud sellega, et anonüümsus kaotati. Selleks on Eesti Ajalehtede Liit koostanud „Online kommentaaride hea tava leppe," mis annab ülevaate, millistest kommentaaridest hoiduda ja kuidas kommenteerida. Hea tava järgi kommentaar ei sisalda roppust, ei ole alandav teiste inimeste suhtes ega halvusta teisi inimesi, ei õhuta sõda ja vaenu, ei kutsu üles narkootikumide ja relvade kasutamist ning ebaseaduslike tegevuste elluviimist, ei levita vale informatsiooni ja ei kutsu üles inimeste suhtes vägivalda. Seega hea kommentaar peaks olema võimalikult neutraalne ning kõiki oma arvamusi ja seisukohti, sõltumata, kas see on positiivne või negatiivne, saab edasi anda viisakalt ja arukalt. Kui sa ei julge seda öelda päris elus, siis ära ütle seda ka sotsiaalmeedias.

Eesti Ajalehtede Liidu „Online kommentaaride hea tava lepe"
http://www.eall.ee/lepped/online.html

KUHU PÖÖRDUDA ABI VAJADUSEL?

- Suhtlusportaalides on *report* või teavita nupp, mida kasutades saab teada anda oma probleemist
- Pöördu usaldusväärse täiskasvanu poole, kes oskab sind aidata
- Helista lasteabitelefonile 116111 või pöördu veebikonstaabli poole