TAL TECH

KAITSEMINISTEERIUM

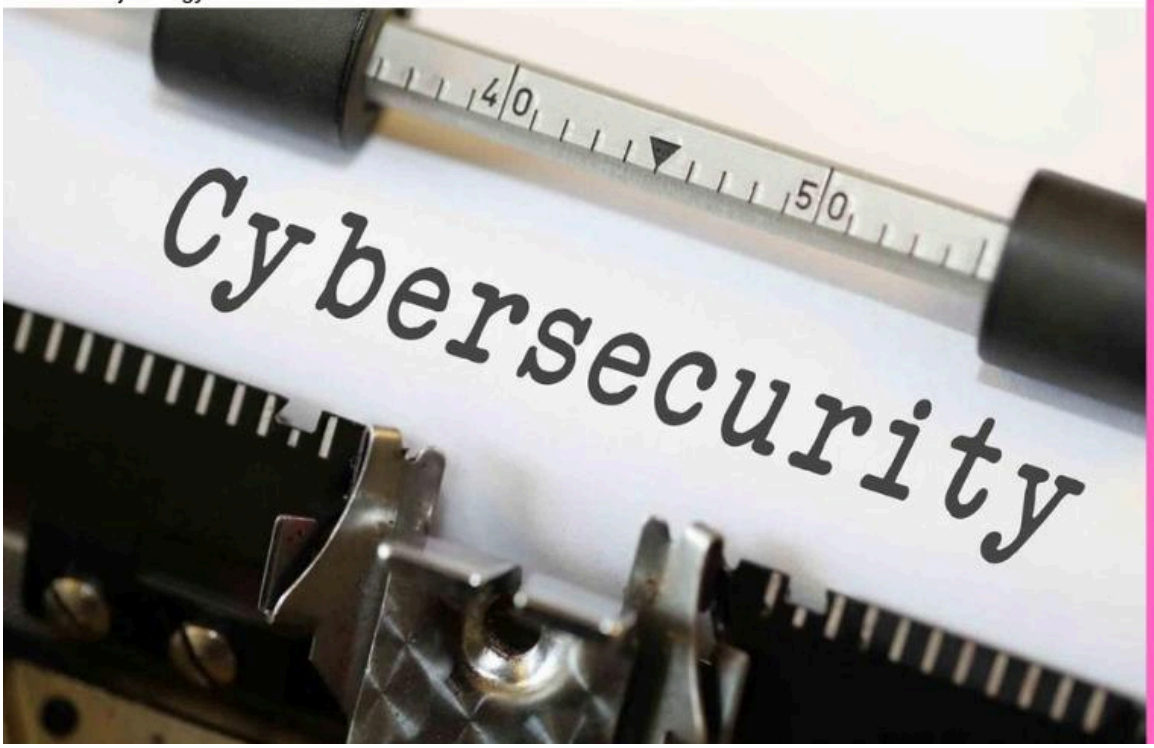
Eesti Interneti SA

Jaanuar 2018

KüberPähkel

uuring

Autorid: Birgy Lorenz, Tiia Sõmer, Kairi Osula, Kristiina Ääsmäe, Anto Veldre, Hillar Põldmaa, Maarja Punak, Mari-Liis Üürike
Toimetaja: Birgy Lorenz



Küberpähkli 2018 talv uuringu ülevaatest tulenevad soovitused

Küberpähkli uuringu läbiviimist toetas Kaitseministeerium. Uuringu viis läbi Tallinna Tehnikaülikooli Küberkriminalistika ja Küberjulgeoleku Keskus.

Küberpähkli uuringut on alates 2015 viinud läbi Hariduse Infotehnoloogia Sihtasutus erinevatel üritustel (Robotex, õpilasvõistlused) võistlusena, enamasti osales kuni 600 vastajat. Alates 2017 sügis viib tegevusi läbi Tallinna Tehnikaülikool läbi e-uuringu või testina, mille eesmärgiks on anda ühiskonnale soovitusi, kuidas küberhügieeni taset Eestis tõsta ja arendada. 2017. aastal viidi uuring läbi 4.-9. klassi õpilaste hulgas, uuringu läbiviimist toetas ka Eesti Interneti Sihtasutus. Käesolev uuring viidi läbi 2018 jaanuari-veebruar ja uuringus võis osaleda kogu eesti alates 10. aastast alates.

Küberpähkli uuringu läbiviimisel ja analüüsimisel osalenud eksperdid:

- Birgy Lorenz, TTÜ, uuringu projektijuht, teadur (birgy.lorenz@ttu.ee)
- Tiia Sõmer, TTÜ doktorant
- Kairi Osula, TLÜ statistika lektor
- Kristiina Ääsmäe, TLÜ magistrant
- Mari-Liis Üürike, TTÜ magistrant
- Anto Veldre, välisekspert
- Hillar Põldmaa, välisekspert
- Maarja Punak, välisekspert

Metoodika

Käesolev uuring viidi läbi 15.01.-11.02.2018 veebikeskkonnas www.küberpähkel.ee kasutades vahendit nimega Limesurvey. Kutse uuringus osalemiseks saadeti erinevate sotsiaalmeedia, meediakanalite, e-posti listide jt. kanalite kaudu. Uuringus oodati osalema kõiki eesti keelt mõistvaid inimesi, alates vanusest 10. eluaastat.

Uuringus oli 41 küsimust: 9 taustaküsimust ning 32 uuringu-testi küsimust. Uuritavad teemad olid: privaatsus ja turvalisus, tehniline taiplikkus, kriitiline mõtlemine ja sotsiaalne manipulatsioon (inimkäitumist mõjutavad küberkelmused) ja hoiakud.

Uuringu aluseks olnud dokumendid olulisuse järjekorras:

- Lorenz, B., & Kikkas, K. (2012, June). Socially engineered commoners as cyber warriors-Estonian future or present?. In Cyber Conflict (CYCON), 2012 4th International Conference on (pp. 1-12). IEEE.
- Tallinna Tehnikaülikool, (2017) Küberpähkli 2017. aasta uuringu ülevaatest tulenevad soovitused https://kyberpahkel.c-lab.ee/?page_id=154
- Majandus- ja Kommunikatsiooniministeerium (2014) Küberjulgeoleku strateegia 2014-2017 https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf

- The Digital Competence Framework 2.0 (2017) https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework
- Õppekava Gümnaasium, küberkaitse on 2017 aastal avaldatud dokument, mis annab soovitusi, kuidas peaks gümnaasiumides küberkaitse valdkonnas algtaseme kursust õpetama. Dokumendi on loonud Eesti NATO Ühing, kaasates mitmeid küberturvalisuse eksperte. https://1drv.ms/w/s!AuRLzcD9FVl7ywlqPX-J4ewoLgIy
- Lorenz, Birgy (2017) "A Digital Safety Model for Understanding Teenage Internet User's Concerns", Tallinna Ülikool (doktoritöö: Digitaalse ohutuse mudel mõistmaks teismelise internetikasutaja vajadusi) http://www.etera.ee/zoom/30536/view?page=1&p=separate&view=0,0,2067,2834
- DigiTurvis analysis on 2014 aastal Tallinna Ülikooli teadlaste poolt läbi viidud uuring Eesti õppekavades, milles sooviti teada saada millisel määral küberkaitse ja digitaalse ohutuse teemasid õpetatakse. http://1drv.ms/1N7KmtZ

Uuringus osalenute taust

Uuringus osales 2078 inimest, kellest 1097 olid mees- ja 990 naissoost. Vanuse grupiti jagunesid vastanud järgmiselt: 47,24% - 10-15 aastased; 25,8% - 16-20 aastased; 26,96% - 21 ja vanemad. Hariduse ja töötamise järgi jagunesid vastajad: 44,75% põhikooli õpilased, 24,01% - gümnaasiumiõpilased, 15,36% - õpivad kutsekoolis või ülikoolis. Vastajatest ¼ töötavad (sh 6% IT alal ja 5% hariduses) ja lapsevanemaid oli kokku 16,34%. Asukoha põhjal liigitatuna elasid 35,93% vastajaid suures linnas, 37,85% väikeses linnas ja 26,22% maal. Üle 90% vastajatest kõnelevad emakeelena eesti keelt 6,76% vene keelt, 1,58% inglise keelt.

Uuringus vastajate osalus on kaldu põhikooli ja gümnaasiumiõpilaste suunas, vastajad kõnelevad eesti keelt emakeelena või oskavad seda hästi, täiskasvanud vastajad on pigem haritud ja tehnika-teadlikud kasutajad (eriti meessoost täiskasvanud vastajad). Uuringust saadud tulemused annavad meile teada trende noore hulgas, kuidas ühes või teises olukorras võiks eeldada käitumist, täiskasvanute osas üldistavad järeldusi kogu elanikkonna peale teha ei tohiks, kuid kuna tegemist on pigem targa vastajaga, siis näeme täna pigem paremat olukorda, kui on tegelikkus.

Uuringu tulemused

Uuringu tulemusi ja soovitusi antakse järgmistes kategooriates: enesehinnang oma digikasutuse valdkonna oskustele ja milliseid olemasolevaid lahendusi on oskuste parendamiseks kasutatud; harjumused ja oskused digitaalse ohutuse ja küberkaitse teemades: privaatsus ja turvalisus, tehniline taiplikkus, kriitiline mõtlemine ja sotsiaalne manipulatsioon, käitumine ja hoiakud riigi tegevuse suhtes eriolukorras; ootused koolitusteks.

1. Enesehinnang ja pädevuste kasvatamine

1.1. Hinnang digipädevusele

Palusime vastajatel hinnata oma pädevusi kaheksal teemal, mis tulenevad EU digitaalse kompetentsi raamistikust (DigiCOMP). Teemad on küll üldised, kuid annavad arusaama trendidest, millistes küsimustes vastajad tunnevad ennast pigem hästi ja milles tunnevad, et oskused puuduvad üldse.

Milliseks hindate oma digitaalseid ja küberhügieeni alaseid oskuseid täna?

	Headeks või väga headeks	Puuduvad
Teabe haldamine sh. kriitiline sisuanalüüs	46,14%	9,82%
Suhtlemine digikeskkonnas sh. otsesuhtlus	69,96%	4,36%
Sisuloome sh. programmeerimine	19,41%	27,12%
Probleemilahendus digivahenditega ja -keskkondades	41,4%	9,92%
Seadme kaitsmine (rakendate ohutus- ja turvameetmeid)	50,12%	7,76%
Isikuandmete kaitsmine (privaatsus, veebipettus)	65,12%	5,22%
Tervise kaitsmine (väldite tehnoloogia kasutusest tulenevaid terviseriske)	43,32%	9,25%
Keskkonnakaitse (teadvustata digitehnoloogia mõju keskkonnale)	37,43%	12,27%

Teabe haldamine sh. kriitiline sisuanalüüsi pädevuses hindavad naissoost vastajad oma digitaalse pädevuse oskuseid keskmiselt 5% madalamaks, kui meessoost vastajad. Oskused kasvavad vanusega. Mitmed täiskasvanud vastajad andsid teada, et vajadusel võivad nad isegi teisi õpetada, eriti need, kelle IT taust seda võimaldaks. Lapsevanemad pidasid ennast kõikidest täiskasvanutest pädevaimateks. Suhtlemises digikeskkonnas sh. otsesuhtluses hindavad mehed ja naised oma oskuseid vallas võrdselt, keskmiselt 70% vastajaid arvab, et ta on selles oskuslik või väga oskuslik. Paistab silma, et noored, kes on alles alustanud gümnaasiumi õpinguid (olles nooremad, st. 14 aastased) tunnevad, et nad vajavad enam abi. Isikuandmete kaitsmine (privaatsus, veebipettus) näitab vähest kõrgemat enesehinnangut meessoost vastajate puhul ja vähest madalamat enesehinnangut põhikooli õpilaste puhul, kuid tundub, et selle valdkonna probleemide lahendamine on kõikidel gruppidel põhjendamatult kõrge - 60% vastajatest peab ennast selles pädevaks või väga pädevaks.

- Tehnilistest oskustest nt. Sisuloome sh. Programmeerimises hindavad meessoost vastajad oma oskuseid kõrgemalt, ka täiskasvanud vastajatel tundub olevat selles vallas enam oskuseid, arvatavasti seepärast, et vastajate hulgas oli palju IT ja haridusvaldkonna töötajaid ja üliõpilasi, kes vastavat taset hoidsid.
- Meessoost vastajad hindavad ennast probleemide lahendajana digikeskkonnas naistest 20% kõrgemalt, aga selle põhjenduseks on jällegi see, et naissoost vastajad olid pigem tavakasutajad, mitte näiteks IT juhid. Üldiselt täiskasvanud hindavad ennast 10-15% kõrgemalt kui gümnaasiumi või põhikooli õpilased.
- Seadme kaitsmiseks nt. rakendate ohutuse ja turvameetmeid näitab 20% kõrgemat enesehinnangut meessoost vastajatel, keskmiselt 5-10% on täiskasvanute enesehinnang kõrgem kui gümnaasiumi või kui põhikooli vastajatel.
- Oma tervise kaitsmine ehk oskus vältida tehnoloogia kasutusest tulenevaid terviseriske vastajate hulgas suuri erisusi ei näinud - 45% vastajatest peab ennast sellel alal teadlikuks, hakkama saamise tunne kasvab vanusega.

1.2. Abi leidmine ja harimise võimalused

Uurisime, kelle poole pöördutakse erinevates olukordades abi saamiseks. Küsimuste grupi eesmärgiks oli teada saada, keda peetakse endast targemaks ja millistest allikatest harivat infot leitakse, kui palju on koolitusi saadud koolist või tööandja käest. Saadud teadmisi saab kasutada teavitustöö parendamisel.

- Vastusele, kellelt saadakse vastavas valdkonnas abi, kerkisid esile: sõber, pereliikmed, IT-taustaga tuttav, klassi-, kooli- või töökaaslane. ⅓ võib abi saamiseks pöörduda ka õpetaja/lektori poole, ⅕ püüab abi leida ka interneti tuttavatelt (sotsiaalmeedia, e-mail). 33,9% meessoost ja 38,5% naissoost vastajatest on abi saanud just oma sõpradelt ja tuttavatelt. Sotsiaalmeedia kanalil jagatavast info kohta nenditakse, et pigem sealt abi ei saa. Näiteks 10-15 aastased (44,7%) ei ole sotsiaalmeedias jagatavast infost abi saanud. 13,8% 10-15 aastaseid väidab ennast oskavat ennast ise aidata; sama väidavad 23,7% 16-20 aastaseid ja 30% üle 21 aastaseid. Kahjuks 50% 10-15 aastastest, 35,6% 16-20 aastastest ja 21% täiskasvanutest pole näiteks kuulnudki, kuidas oma sotsiaalmeedia profiili turvalisemaks seadistada.
- Küberhügieeni alaste oskuste parendamiseks on palju väärtuslikku abi saadud onlain-meedia veebilehtedelt (37,81%), suhtlus inimestega päriselus (36,08%), koolist/koolituselt (34,93%), erinevad muud veebilehed (27,50%), abitekstid nt. sotsiaalmeedias privaatsusest (20,94%), sotsiaalmeedias jagatavast infost (17,07%), suunatud eestikeelsed abilehed (Targalt Internetis/Veebikonstaabel jne) (12,7%), TV/raadio (12,79%), Interneti teenusepakkuja (11,64%).
    - Meedia (raadio, tv, pabermeedia) kohta arvatakse, et digitaalse ohutuse alast teavet ei ole piisavalt jagatud (infot on piisavalt saanud ainult 10-15% vastajatest). Online meediast saadavat infot peab 47% täiskasvanutest ja 29% 10-15 aastastest aga piisavaks. Online meedia jõuab kiiremini kohale suurlinna elanikule (10%). Interneti, mobiilside pakkujate ja pankate teavitustöö on jõudnud kuni 10-15% vastajaskonnani.

    - Spetsialiseerunud abiteenused ja lehed (Lasteabi, Targalt Internetis, Veebikonstaabel) on jõudnud 9-14% vastajate teadvusesse; samas 59,4% 10-15 aastatest, 61,9% 16-20 aastastest ja 55,1% täiskasvanutest sh. 51,2% lapsevanematest pole saanud nendest teenustest abi. Võimalik on, et teenuseid lihtsalt pole kunagi olnud vaja kasutada, sest teiste küsimuste vastustest tuleb välja, et antud kanalite maine ei ole halb. Erinevad muud veebilehtede kasutegur oskuste parandamisele kasvab kogemusega, selgub, et internetis noorematele vastajatele eakohased materjale nt. 50,2% 10-15 aastaseid pole saanud abi muudelt veebilehtedelt, samas kui 41% lapsevanematest on saanud palju abi.
- Küberohutuse alase koolitusega on palju kokku puutunud tänu koolidele: 38% 10-15 aastaseid; 35% 16-20 aastaseid ja täiskasvanud töökohas/koolis 29,4%. Lapsevanematest on saanud koolitust 25,8%. Huvitaval kombel on saadud enam koolitust väikelinnades, hajakülas jt. Samas annavad vastajad teada, et koolitused pole olnud piisavad nt. 60% põhikooli õpilastest ja 66,7% gümnaasiumiõpilast väidab, et ei ole piisavalt saanud koolitusi. Ühtegi koolitust pole saanud 20% 10-15 aastaseid, 12% 16-20 aastaseid ja 32% täiskasvanuid. 37,6% vanematest väidab, et nad pole kordagi saanud vastavat koolitust
- Töötavate inimeste käest küsisime, et kas küberturbe koolitusi on saadud äkki tööandja käest, kahjuks alla 10% vastajaid on seda saanud piisavalt, üle 70% pole aga saanud üldse. Samas 26% lapsevanematest väidab, et just töö juurest on saadud koolitusi, mis annab märku, et osad tööandjad on siiski pakkunud temaatilisi koolitusi oma lapsevanematest töötajatele. Koolitusi on pakkunud tööandjad pigem suurlinnades töötavatele vastajatele.

2. Harjumused ja oskused digitaalse ohutuse ning küberkaitse teemades

Vastava uurimisbloki eesmärgiks oli teada saada inimeste tegelikud harjumused ja oskused lahendada erinevad väljakutsed. Vaatluse all olid kasutatavad keskkonnad, parooli ja nutiseadme turvalisemat kasutust puudutavad küsimused ja teised juhtumid.

2.1. Keskkonnad, seadmed ja nende kaitse

Enamust vastajatest andis teada, et nende e-post asub 94,44% juhul Google, 24,39% Microsofti, 14,9% Online.ee, 13,03% Mail.ee, 3,64% Mail.ru juures. Sotsiaalmeedia lemmikutest kasutatakse enim YouTube (83,18%), Facebook (81,31%), Instagram (63,39%), Snapchat (54,48%), Google+ (25,8%), Twitter (24,72%). Ning otsesuhtluseks kasutatakse 82,75% Facebook messengeri, 28,32% Skype, 14,57% Google+, 13,7% Whatsapp, 11,16% Viberit.

Parool on käesolevas maailmas A ja O, millest me ei saa üle ega ümber. Enamus koolitused algavad ning lõppevad sõnadega, et “õige ja hea parool oleks..”, mis on tegelikkuses enamus koolitatavaid ära tüüdanud. Kahjuks peame ka siinkohal nentima, et kuigi ollakse teavitustööga suudetud viia inimesed nii kaugele, et paroolid on pigem keerulised, kui

lihtsad, siis paroolide pikkus ja erineva parooli kasutamine erinevas keskkonnas on ikkagi asi, mis tekitab inimestele pigem väljakutseid. Muidugi on vastajad antud uuringus pigem õpilased, kuid ega täiskasvanudki selles olukorras ennast palju paremast valgusest ei näidanud. Samamoodi on oluline, et kui on kasutusel palju erinevaid keskkondasid, siis tuleb hakata mõtlema parematele mnemotehnikatele või turvalisematele paroolihoiustamise võimalustele.

Millised neist väidetest on Teie parooli loomise/kasutamise harjumustele sarnased?

	10-15 aastased	16-20 aastased	täiskasvanud	Keskmine
Üks lihtne parool enamikus keskkondades	15,8%	15,5%	9,2%	14,04%
Üks keeruline parool enamikus keskkondades	64,5%	62,4%	34,8%	56%
Kuni 6 erinevat parooli erinevates keskkondades	31,1%	33,3%	41,8%	34,64%
Enamikus keskkondades on erinev parool	48,7%	38,3%	50,5%	46,93%
Igas keskkonnas on erinev parool	33,9%	22,4%	39,2%	32,44%
Parool on pikem kui 14 märk	31,1%	35,2%	32,1%	32,49%
Paroolis on numbrid ja tähed	87,1%	95,9%	96,4%	91,8%
Paroolis on erimärgid	35,3%	43,8%	46,6%	40,59%
Paroolid on salvestatud arvutisse/brauserisse	25,6%	34,4%	34,3%	30,24%
Hoiustate parooli avatud failis, ühes e-mailis (krüpteeringut ei ole)	12,2%	8,5%	3.3%	8,91%
Kasutate parooli hoiustamise teenust/äppi/krüpteerimist (nt. PasswordSafe)	15,8%	11,1%	24,5%	17,01%
Kasutate tihti parooli meeldetuletamise teenust	11,9%	12%	13,2%	12,36%
Kontod on seotud ühe teenusepakkujaga nt (Google) ja ei vaja eraldi parooli	40,3%	45,5%	27,4%	38,19%
Olete alati seadistanud mitmeastmelise autentimise kui võimalik (logite sisse nii parooli kui nt. Telefoniga)	54,4%	50,6%	58,6%	54,52%

Naissoost vastajatel on 5% tõenäosusega kasutusel üks lihtne parool enamikus keskkondades kui meessoost vastajatel. Iga parool on erinev 26% naissoost ja 38,1%

meessoost vastajal. Kui täiskasvanutest 9,2% omab ainult ühte parooli, siis põhikooliõpilastest on see nii 15,8%. Õpilaste (nii põhikooli kui gümnaasiumi) harjumused näitavad, et usaldatakse pigem ühte keerulist parooli, kui erinevaid paroole erinevates kohtades. Parool on pikem kui 14 märki 37% meessoost vastajal ja 27,4% naissoost vastajal, erimärke kasutavad naissoost vastajad meessoost vastajatest vähem. Põhikooli õpilased pigem eelistavad lühikesi paroole, kus puuduvad erimärgid. 25,7% naissoost ja 34,2% meessoost vastajatest salvestab paroolid brauserisse. Paroolide hoidmist äppis/programmis või krüpteerimist kasutavad alla 21,8% meessoost ja 11,5% naissoost vastajatest. Paroolide salvestamine brauserisse ja äpp-lahenduste kasutamine kasvab vanuse ja vajadusega kasutada erinevaid keskkondasid. Kui enamus täiskasvanud ei ole oma digi-elu veel ühe teenusepakkujaga sidunud, siis seda teinud 16-20 aastased, kelle eelistatud lahenduseks on Google pakutavad *one-sign-on* lahendused koos Facebooki lisavõimalustega.

Nutiseadme ekraani lukustamise viisidest on eelistatud: PIN kood (61,91%), Sõrmejälje tuvastus(46,81%), Parool (34,16%), Näpumuster (34,12%). Biomeetrilised ja asukohast tingitud turvalahendused pigem ei ole kasutuses.

- 61,2% meessoost vastajatest väidab, et on alati seadistanud mitme-astmelise autentimise kui võimalik (logite sisse nii parooli kui nt. Telefoniga), ja ainult 47,1% naissoost vastajatest.
- Kui mingil ajahetkel puudub internetiühendus, siis on telefoni omanikul oma seadmega ligipääs piltidele (86,92%), dokumentidele (65,50%), E-kirjadele (26,69%). 13,51% aga nendib, et ligipääs puudub enamikele asjadele, sest oma asju hoitakse pilveteenustes.
- Kui nutiseade kaob, siis 41,4% saab oma seadme muuta teiste jaoks eemalt kasutamatuks, kahjuks 34,45% ei tea kas ta saab ja 15,48% ei oska seda sisse lülitada. Nutiseadme kadumisel korral on sisse lülitanud eemalt seadme lukustamise 53% meessoost vastajaid ja ainult 29% naissoost vastajaid. 63,4% naissoost vastajaid väidab, et ta ei ole seda teinud sh. 22% ei oska seda teha (enamus vastajad on muidugi põhikooliõpilaste hulgast). Kõige vähem ongi sellele mõelnud 10-15 aastased vastajad, sest 58,9% täiskasvanud vastajatest on eemalt seadme lukustamise siiski sisse lülitanud.

Järgmiseks vaatasime kolme juhtumit - mida teed olukorras, kui on vaja maha müüa arvuti; milline on suhtumine piraatlusesse ja mida teha olukorras, kui sõbra arvuti on lukustatud lunavaraga. Juhtumid annavad parema arusaama tegelikest tehnilistest ja seaduslikest valikutest.

Juhtum 1: Soovite müüa maha oma arvuti. Mida teete seadmes olevate andmetega?

Kustutate ära failid (liiguvad prügikasti)	45.66%
Tühjendate arvuti prügikasti	45.33%
Eemaldate konto ja failid vastavalt kasutajakonto eemaldamise võimalusele	56.25%

Formaadite ära arvuti kõvaketta	44.99%
Kirjutate üle kõvaketta (nullide ja ühtedega)	19.74%
Müüte kõvaketta arvutist eraldi	4.98%
Ei müü kõvaketast, eemaldate selle seadmest ja panete riiulile seisma/teise isiklikku masinasse	36.56%
Hävitate ise või lasete kõvaketta hävitada	14.42%
Midagi ei tee, failid päranduvad järgmisele omanikule	1.72%

Vastused annavad teada, et inimesed ei ole väga mõelnud andmete hoidmise peale seadme müügi korral. Samuti, need kes vastasid, et teoreetiliselt oskaksid kõvaketta ära formaatida või selle arvutist välja võtta, siis kas nad tegelikkuses ka nii teevad, seda me ei tea. Reaalsus on, et kasutatud arvuteid kui nutiseadmeid müüakse ning tihti saavad uued omanikud kaasa ka vana omaniku vara – või kui ka failid on kustutatud, siis on võimalik neid ikkagi taastada, kui kellelgi peaks kuri kavatsus olema.

Juhtum 2: Prantsusmaal blokeeritakse kasutaja internetti ligipääs, kui avastatakse, et ta laadib alla piraatfilme (peale kolmandat vahelejäämist). Mida Te arvate sellest?

See peabki nii olema - hea mõte!	30,33%
Piraatfailide allalaadimist peaks lubama erijuhtudel	39,53%
Sellist asja ei tohiks olla - halb mõte!	45,76%
Midagi ei arva	38,01%
Prantsusmaal võib see nii olla, Eestis kindlasti mitte	42,93%

Blokeerimise poolt on 26,6% 10-15 aastatest, 29,1% 16-20 aastastest ja 38,9% täiskasvanutest ja 46,6% lapsevanematest. Erijuhtudel piraatluse lubamist pooldavad kõige enam 16-20 aastased vastajad (47,4%). Piraatluse pärast interneti teenuse sulgemist teenusepakkuja poolt peavad ebameeldivaks teoks 45,1% 10-15 aastastest, 40,9% 16-20 aastastest ja 51,6% täiskasvanutest. Samamoodi peavad natuke alla pooled vastavat juhtumist Prantsusmaa probleemiks, mis Eestist ei puuduta – Eestis sellist asja ei tohiks kunagi juhtuda!

Juhtum 3: Sõbra arvuti on nakatunud lunavaraga. Varukoopiat arvutis olevatest failidest pole. On vaja kätte saada vajalikud failid. Failide avamise eest küsitakse 100 eurot, 7 päeva pärast tõuseb hind 200 euro peale. Mida soovitate sõbrale?

Maksta nõutud summa	14,13%
Viivitada ja loota, et hiljem tuleb maksta vähem	11,26%

Palgata häkkeri, kes avaks failid	35,12%
Asuda läbi rääkima ja tingida hinda alla	24,19%
Kaevata veebikonstaablile/politseile	75,38%
Püüda kurikaelad üle kavaldada, lubades saata sama viiruse 10nele sõbrale edasi, kui failid avatakse	15,34%
Mitte midagi teha	17,1%
Arvuti ära visata ja eluga edasi minna	22,95%
Otsida üles, kes see kratt on ja teda ise hakata muude viirustega pommitama	19,08%
Teeks veel midagi muud	33,88%

Enamus vastajad pöörduksid loomulikult veebikonstaabli poole, aga päri huvitav on hoopis järgmised valikud, et vastajatest on altid palkama häkkerit näiteks 36,6% 10-15 aastastest 36,8% 16-20 aastastest ja 30,8% täiskasvanutest. Hinda alla hakkavad tingima pigem naised (5% meessoost vastajatest enam) ja 26,1-27,6% 10-20 aastastest ja 15,9% täiskasvanutest. Kui vaatasime vastajate hulgast pädevamaid vastajaid (need, kes andsid teada, et nad teavad midagi seadmete turvalisusest ja probleemi lahendusest), siis ka nende vastused jagunesid kaheks - arvuti ära viskamine vs. häkkeri palkamine. Kasutajad, kes hindavad end pädevalt probleemilahenduses ei ole nõus tasuma lunaraha nagu ka kõik teised vastajad. 18,1% 16-20 aastastest oleks aga valmis maksma nõutud summa. Kuna maailmas jagunevad ka eksperdid kaheks - osad soovitavad maksta ja teised soovitavad olla tulevikus targem, pakkumata lahendusi, siis see on üks keeruline teema, millele oleks vaja enam ka Eestis tähelepanu pöörata.

2.2. Kriitiline mõtlemine ja manipuleeritud sisu tuvastamine

Siinses osas uurisime, millised on vastajate jaoks olulisemad allikad info saamisel ja kuidas saadud info mõjutab otsuseid.

Kõige olulisemaks infokanaliks maailmaga on Internetti ühendatud nutiseade (nutitelefon, tahvelarvuti) (86,44%) ja Internetti ühendatud laua- või sülearvuti (71,63%); 64,83% saab uut infot suhtlusest teiste inimestega (naabrid, kooli või töökaaslased, tuttavad, sugulased) ja 59,94% vaatab ka televiisorit. Otsingumootoritest on igapäevaselt kasutuses Google (96,12%).

- Tahvelarvuti, nutiseade on põhiline infoallikas nooremale generatsioonile. Arvuti tähtsus infoallikana kasvab vanusega nt. 58% 10-15 aastased; 75% 16-20 aastased ja 91% 21 ja vanemad vastajad. Televiisorit vaatavad kas kõige nooremad vastajad või täiskasvanud vastajad nt. 21+ (60%); Suures linnas elavad inimesed vaatavad natuke vähem televiisorit kui väiksemates kohtades elavad vastajad: IT valdkonnas õpivad ja töötavad inimesed vaatavad televiisorit kõige vähem (40%). Raadio jõuab kuni 20-25% vastanutest (kõige vähem suurlinnas, kõige enam hajakülas). Õpilasteni

jõuab raadio üle poole vähem, kui jõuab täiskasvanuteni. Silmast-silma suhtlemises jõuab info naissoost vastajate vahel 20% enam kohale kui meessoost; kõige vähem vahetavad infot omavahel 10-15 aastased. Otsimootoritest kasutatavaim on Google, mis on täiskasvanud kasutajal igapäevane töövahend. Õpilaste hulgas on Google kasutusel vastavalt vajadusele (enamasti koolis) ja täiskasvanutest 20% vähem.

Kui näete internetis või loete meediast pealkirja “Suured lekked paljastasid: just need on eestlaste kõige populaarsemad paroolid”. Tutvute artikliga, et teada saada, kas Teie kasutatud parool on loetelus. Mis saab edasi?

Kui te leiaks parooli, siis ei vahetaks ühtegi oma parooli välja	6.23%
Kui leiaksite oma kasutatule sarnase parooli, siis vahetate selle välja	50.89%
Kui leiaksite oma parooli, siis vahetate enamiku oma paroolidest välja	25.49%
Kui leiaksite oma parooli, siis vahetaksite kõik paroolid erinevaks	29.08%
Ei leidnud parooli ja ei tee midagi	34.79%
Ei leidnud parooli, aga muudate mõne oma parooli turvalisemaks	27.79%
Ei leidnud parooli, aga käite enamiku oma paroole igaks juhuks üle	21.80%
Ei leidnud parooli, kuid muudate kõik oma paroolid erinevaks	8.29%

Reaalsus on seega, et kui enda parooli ei näe, siis uudis üldiselt ei kõneta. Samas enamus sisestaks oma emaili ja „enda parooli laadse parooli“ siiski kontrolliks antud keskkonda, kui seda pakutaks, mis on jällegi turvarisk.

Järgmiseks uurisime nelja juhtumit mõjutamise kohta. A. Loete salajasest foorumist, et eurot planeeritakse devalveerida. Muud allikad seda ei kinnita, kuid foorumikülastajad vannuvad, et nemad on oma raha juba dollariks vahetanud. B. Tuttav jagab sinuga Facebooki postitust, milles räägitakse, et Eesti riiki ähvardab hädaoht. Väidetakse, et eelmise nädala plahvatus lennujaamas ei olnud juhuslik. C. Sõber teavitab, et astus ühendusse, mis tegeleb maailmapoliitikaga läbi alternatiivsete kanalite. Võimalus on saada tegelikku infot otse USA ja Venemaa agentuuridelt. D. Vaatate televiisorist seriaali. Äkki ilmuvad ekraanile nahkmantlites mehed, kes räägivad võimu ülevõtmisest.

- Kui tegemist on rahaga, siis inimesed tunnevad asja vastu huvi. Kui EUR läheks uudise ainetel devalveerimisele, siis 78,44% loeks läbi ka teised uudised, ja 48.35% konsulteeriks sõbraga, et saada kinnitust. Naissoost vastajad eelistavad olla enam proaktiivsed ja infot otsida, lugeda, sõpradelt küsida kui ka politseid teavitada. Nooremad õpilased küsivad enam nõu kui täiskasvanud, täiskasvanud seevastu lähevad kohe teistest kanalitest lisainfot otsima. Tõenäosus on suurem, et raha tormaks vahetama meessoost vastaja, kes on 10-15 aastane (16,1% nooremast vanusegrupist läheks vahetaks osa raha ja 8,6% vahetaks kogu oma raha ära), samamoodi noorem meessoost

vastaja jagaks ka infot erinevates kanalites edasi, samal ajal oleks ta kõige altim teavitama politseid. Olukorra vastu apaatsem on pigem täiskasvanud vastaja, kes pigem jätaks reageerimata.

- Olukorras, kus jagatakse uudist, milles on info toimunud potensiaalse terrorismiakti kohta, siis see tekitab huvi otsida uudis üles ja lugeda kommentaare. 46,23% otsustab kommentaaride pealt, mida edasi teha ehk uuritakse kommenteerivate inimeste meeleolu ja soovitatud tegutsemisjuhiseid. Kõigepealt asuvad tegutsema naissoost vastajad - uurivad viimaseid uudiseid ja kommentaare (81,1%), lisainfot küsima (56,1%) ja meessoost vastajad on ka aktiivsed, aga vähem kui naissoost - lisainfot uurivad (68,5%) ja sotsiaalmeediast (46,1%); pigem on uurijaks noored 10-15 aastased 54,6% vs täiskasvanud 41,3%. Sõbralt küsivad nõu meessoost vastajad 29,1% ja naissoost 40,7%; Ei tee midagi 41,2% meessoost vastajat ja 33,7% naissoost. Samas noored 10-15 aastased on jällegi aktiivsemad (⅔ hakkaks midagi tegema) vs täiskasvanud, kellest pooled midagi ikkagi ette võtaks. Paberajakirjanduse valiku vastu tundsid huvi pigem täiskasvanud vastajad, et sealt lisainfot vaadata.
- Kui tegemist on kutsega liituda salajase organisatsiooniga, siis enamus vastajaid muretseb pigem sõbra pärast, et ta on ennast kuhugi sisse mässinud. Huvi kogukonnaga koheselt liituda on pigem noorematel vastajatel, jällegi pigem meessoost. Enne liitumist on soov saada kokku (et saada enam infot) 27,7% 10-15 aastastel ja 32,3% 16-20 aastastel ning 10,9% täiskasvanud vastajatest. Enamus tunneb sõbra pärast siiralt muret ja saab aru, et selline pakkumine on pigem kahtlane 67,3% 10-15 aastastest; 74,4% 16-20 aastastest ja 82,5% täiskasvanutest. Sõpra „maa peale“ tuua püüavad pigem täiskasvanud vastajad, aga kõige noorematest pooled vähemalt püüavad. Samuti lähevad täiskasvanud vastajad teema kohta lisa uurima, kuigi sõbrale sellest midagi ei maini. Politsei teavitamise peale mõtleb 37,4% 10-15 aastast vastajat, teised pigem vähem. 1/3 vastajaid laseks juhtumil lihtsalt olla ja nad ei teeks midagi.
- Kui nähakse aga ise telekanali kaudu „riigi ülevõtmist“ pealt, siis arvatakse pigem, et see on nali (eriti vanemad vastajad), järgmisena avatakse uus kanal, et teada kontrollida. Uuritakse lisainfot internetist; osad küsivad nõu internetist oma avalikul seinal, helistavad ka sõpradele, ja ka politseisse või kasutavad mõnda muud kanalit (foorumit või otsesuhtlust); telekanalisse helistama vaevuvad vähesed. Üldiselt tänavatele selle juhtumi peale ei mindks (huvi on alla 12%), kuid kui telekanal või raadio paluks abi, siis 21,4% täiskasvanud vastajatest oleks valmis appi minema, samas 43,1% täiskasvanutest ei teeks midagi.

3. Käitumine eriolukorras

Siinses osas uurisime käitumist ja ootuseid info jagamise suhtes eriolukorras, kus info kui ka interneti kättesaadavus on piiratud, saadav info võib olla kallutatud, võib-olla on rakendunud ka muud piirangud liikumise osas. Küsimused on inspireeritud 2007 aastal toimunud tänavarahutustest nimega “Pronksiöö” ja 2014 aastal läbi viidud uuringust samal teemal.

- Kui peaks tekkima olukord, milles oleks vaja rakendada erinevaid piiranguid, siis ebameeldivaks peaks neid ja rahutusi põhjustaks eelkõige info täielik puudumine kui ka liikumispiirangud, kuid sama olulised on info kättesaadavuse piiramine ja vaba interneti ligipääs. Täiskasvanud ja vanemad õpilased toovad välja ka info moonutamise.
- Gene Sharpi kevade teooria Araabia kevade teemadel on kehtiv ka Eestis. Meie tulemuste koha pealt mida ilusam on ilm, seda vähem inimesed huvituvad riigi probleemidest; mida

külmem ja ebameeldivam on ilm, seda enam on nad valmis pigem riigist lahkuma. Probleemidele kogunemisi ja lahendusi otsima hakata reageerivad enneköike noored, sest neil pole eriolukorras võimalik saada adekvaatset infot või midagi teha (koolid on suletud, poed kinni, internet on ebastabiilne jne). Ja mis kõige olulisem, enne minnakse maale vanaema juurde varusid täiendama või vargile, kui rahutusi korraldama või selles osalema (vähemalt täiskasvanute hulgas). Sarnastele tulemustele jõuti ja 2014 aasta uuringus (Lorenz, 2014).

- Olukorras, kus üks riik peaks teist riiki digitaalselt ründama oodatakse rahumeelseid lahendusi nagu “avaldada noot, katkestada poliitiline suhtlemine” või “püüda blokeerida ligipääs internetist sellele maale”. Paljud gümnaasiumi õpilased olid ka seda meelt, et võiks ka digitaalselt vastu hakata “Vastata rünnakuga, kasutades selleks mitteformaalseid ühendusi ja eksperte (sh. häkkereid)” või “Riigil on luba anda mitteformaalsele küberekspertide grupile ohuolukorras enamad õigused, nt. mitteametlik vasturünne”. 64,1% naissoost vastajatest, 53,3% meessoost ja 69,6% lapsevanematest olid jällegi pealtkuulamise poolt. Samamoodi on vaba interneti piiramise poolt enam naissoost vastajad ja vanemad, kui see on vaja korra tagamiseks.
- Vastutavaks sellekohase info ning instruktsioonide jagamisel peeti mõnda vastutavat ministeeriumi (61,76%), Politsei või muu vastutav amet (56,78%), Erinevad eksperdid, kes enamasti sõna võtavad 42,93%, Ise olete vastutav 39,34%, Poliitikud 35,89%, Meediakanalid (TV, raadio, ajalehed paber/online) 34,64%, Sõbrad ja tuttavad 14,32%. Kui vajalikku infot riigis ei saa kätte, siis täiskasvanud peavad enam vastutavaks ametlikke asutusi nagu ministeeriumit, politseid kui ka meediat. Eksperte usaldaksid ka noored, kuid poliitikute reageerimisse antud olukorras pigem vastajate usk puudub, neid ei peeta kas vastutavaks või nende poolne info jagamine ei ole lihtsalt primaarne kanal.

4. Digitaalse ohutuse ja küberkaitse alased koolitused

Uurisime vastajatelt, millistest kohtadest eelistatakse enda harimiseks infot saada, kas see peaks olema teoreetiline või praktiline ning ka äkki isegi kohustuslik.

Infot küberohutuse kohta eelistatakse saada infot järgmistest kanalitest (roheline) ja ei eelistata (punane):

	M	N	10-15	16-20	21+	Lapsevanem	Keskmine
Kool/töö	63,5%	76%	62,6%	73,1%	77,8%	79%	69,24%
Trad.meedia	35,6%	50,2%	33,5%	46,3%	53,7%	54,6%	42,46%
Online meedia	69,6%	66,1%	48,2%	70,2%	80,7%	82,3%	62,43%

Internet pakkuja	51,7%	65,3%	38,7%	57,2%	76%	77,3%	53,28%
Mob. teenusepakkuja	48%	54,2%	37,6%	64,2%	73,5%	76,1%	51,3%
Pank	43,8%	46,9%	28,5%	49,6%	70,6%	68,3%	45,09%
Keskkonna abiteksid	50%	57%	40,9%	55,6%	73,2%	73,7%	53,23%
Lasteabi, Targalt Internetis	40,9%	51,5%	41,7%	42,1%	57,1%	62,8%	45,81%
Veebikonstaabel	49,4%	64,7%	55,1%	56,1%	60%	60,5%	56,58%
Kaitseliit (Küber)	57,8%	61,6%	53,9%	62%	66,5%	65,2%	xxx
Erikoolitus riigi poolt	48,9%	57,9%	45,9%	53,5%	65,6%	65,5%	50,27%
Tasuta e-kursused	48,1%	53%	34,1%	56,1%	73,7%	72,7%	53,04%

Ootus on küberhügieeni parendamiseks, et oleks vaja enam koolitusi: õpilastele (82,42%), täiskasvanutele (78,82%), kõikidele üliõpilastele (ülikool/kutsekool) (76,04%) ja IT valdkonna üliõpilastele (ülikool/kutsekool) (64,99%) ja tööandja poolne koolitus ja kontroll (62,15%); Seada teenusepakkujatele enam vastutust toodete ja teenuste turvalisuse osas (67,18%); luua enam veebikonstaabli ametikohti, kes aitavad inimestel väljakutseid lahendada (61,71%), survestada meediat avaldama vajalikku digipädevust kasvatavat sisu (54,53%), luua seaduseid, mis reguleerivad valdkondi (49,31%), anda kogukonnale enam vastutust ja usaldust väljakutsete lahendamisel (48,73%). Midagi ei pea muutma (19,4%) vastajate meelest.

Ootus olukorra muutmiseks on vaja (proaktiivsed tegevused):

	M	N	10-15	16-20	21+	Lapsevanem
Enam seaduseid	42,1%	57,6%	50,8%	53,7%	42,9%	45,1%
Teenusepakkuja vastutagu enam	71,8%	73,6%	55%	72,4%	84,5%	85,1%
Koolitusi õpilastele	80,2%	85,5%	73,8%	83,7%	97,5%	97,2%

Koolitusi kõikidele üliõpilastele	72%	81%	64,3%	79,1%	84,8%	96%
Koolitusi IT valdkonna üliõpilastele	73,8%	78%	64,7%	80%	89,2%	90,4%
Koolitusi täiskasvanutele	76,7%	81,8%	68,2%	83,7%	93,9%	92,8%
Tööandja koolitus ja kontroll	60,2%	64,9%	51,7%	63,2%	80,7%	81,2%
Ekspertide grupi loomine	62,2%	63,5%	57,3%	64,1%	71,2%	78,3%
Enam veebikonstaableid	54,2%	70,4%	59,4%	63,7%	64,5%	70,1%
Kogukonnale enam vastutuse jagamist	48,7%	49%	44,2%	54,3%	52,1%	52,8%
Meedia survestamine, et nad enam temaatilist sisu avaldaks	52,3%	57,4%	42,6%	60%	70,7%	70,8%
Midagi ei ole vaja teha, kõik on juba hästi	22,6%	15,8%	24,7%	18,4%	7%	10,3%

Küberkaitse teemalised kursused peaksid vastajate meelest eelistatult olema vabatahtlikud, nt. valikainena - gümnaasiumis 63,35% ja põhikoolis 59,46%. Teoreetiliselt ja praktiliselt õpetamiseks on toetus alates 10 aastasest õpilasest alates. Kutsekoolides ja ülikoolides peaks see vastajate meelest jääma kohustuslikuks IT erialadel (toetus üle 68%), kuid pakutama vabatahtlikkuse alusel ka teistele. Ühe erisusena tuuakse välja, et õpe peaks olema kohustuslik kõikidele tulevastele ja olemasolevatele õpetajatele (toetus üle 75%) ja IT õpetajatele (üle 78%). Õpetajatele peaks koolitused olema nii teoreetilised kui praktilised.

Küberkaitse teemaline teavitustöö haridusvallas peaks olema:

- valikainena gümnaasiumis – selle poolt on gümnaasiumis õppivatest õpilastest 76% ja 37,9% on kohustusliku kursuse poolt; täiskasvanute toetus sellele on 74% (66,1% on kohustusliku poolt;
- valikainena põhikoolis on 10-15 aastastest vastajatest 51% ja kohustusliku 39,3%. Põhikoolis õppimise poolt on 69% täiskasvanutest on vabatahtliku ja 64,3% kohustusliku kursuse poolt.

- kursus peaks olema pigem teoreetiline põhikoolis alates 10 eluaastast, alates 14 eluaastast võiks lisada ka praktilisi elemente, gümnaasiumis peaks olema kursus nii teoreetiline kui praktiline.
- ootus on, et gümnaasiumid pakuks küberkaitse kursust vabatahtlikkuse korras, kuid näiteks kui kool on valinud IT ja küberkaitse üheks suunaks, siis oleks loogiline, et see on kohustuslik.
- Õpetajatele peaks olema küberkaitse alane teavitustöö kohustuslik 93% täiskasvanud vastajate meelest, seda peavad oluliseks ka 80% 15-20 aastastest vastajatest ja 63,4% 10-15 aastastest vastajatest. IT õpetajad peaks vastavat haridust saama 97,5% täiskasvanud vastaja meelest. Koolitused õpetajale peaks olema nii praktilised kui teoreetilised.

Ühiskonnas kodanikele peaks olema vabatahtlikud kursused, nii teoreetilised kui praktilised - 63,6% täiskasvanud vastajaid peab oluliseks. Avaliku sektori töötajad peaks saama vastavat haridust 91% täiskasvanud vastaja meelest. Koolitused peaksid olema nii teoreetilised kui praktilised.

Soovitused

Üldised soovitused:

- Korraldada küberkaitse alase eriolukorra kohta ennetavaid koolitusi ja selgitada elanikkonnale, mida teha ja kuidas käituda, et ära hoida potentsiaalseid kallutatud üleskutseid korraldada rahutus. Eriti oluline on see, kui info saamine on tehniliselt raskendatud, siis mis oleks info saamisel alternatiivsed usaldusväärsed allikad nt raadio vms. Ei tasu unustada ära ka meie residente, kes peaksid samamoodi kuskilt infot saama;
- Naissoost vastajate enesehinnang on mitmes erinevas teemas madalam kui meessoost vastajatel (erinevates vanusegruppides), seda saaks kindlasti erinevate meetmetega tõsta, mis oleks suunatud just naissoost elanikkonnale, eriti noortele. Täna kõlab läbi, et digitaalne ohutus tehniliste oskuste valdkonnas kõnetab enam meessoost vastajaid.

Meedia kasutamine teabeallikana:

- Online meedia maine ja kasutegur vastavasisulise teavitustöö tegemisel mõjub pigem täiskasvanud lugejale, kui õpilastele, kes vastavat meediat enamasti lihtsalt ei tarbi;
- Sotsiaalmeedias jagatav ohutuse alane teave kaob üldisesse infomürasse, võib-olla ei ole see parim kanal õpetamiseks/lugejate harimiseks, pigem on ta sobilik oluliste materjalide reklaamiks.

Välja kerkinud teemad:

- Tehnilised: kuidas sisse lülitada mitme-astmeline autentimine; kuidas seadistada nutiseadme kaugelt lukustamine ja jälgimine; kuidas arvutit, nutiseadet turvaliselt puhastada andmetest enne müüki; mis on piraatlusest tulenevaid riskid tegelikult; lunavara korral toimimist. Täna puudub sellekohane info ühiskonnas - kuidas ja mida teha. Ning, et kuritegevuse toetamine või sellele kaasa aitamine (häkkeri palkamisel)

jms. Võidakse sattuda veel suuremasse ohtu, kui lihtsalt nentides, et “varukoopiat ei olnud”, oled failidest ilma.

- Käitumuslikud: Paroolide osas hirmutamine ja shokeerimine toimib ehk enamus läheks oma paroole vahetama, kui nad leiaks uudisest enda paroolile sarnase; Kuna vastajad on agarad Google otsiteenuste ja nutiseadmete kasutajad, tuleks õpetada kasutama ka teisi otsimootoreid, et vältida ühe teenuse osas kallutust. Nutiseade töötab täpselt nii kaua kui on internet ja aku vastu peab, oluline on õpetada otsima infot ka teistest kanalitest, olukorra tarbeks, millest räägime enam järgmises alapunktis “eriolukord”; Tuleks arutada ühiskonnas enam tervise hoidmist ja säilitamist puudutavatel teemadel.

Soovitused koolidele:

- Õpilased ja vanemad vajavad enam digitaalse ohutuse alaseid koolitusi, väga suur hulk vastajaid pole saanud ühtegi koolitust. Ühe võimalusena jätkata kindlasti tööandjate poolt tehtavaid koolitusi lapsevanematele;
    - Kuna õpilaste digiteemaline enesehinnang oli vastajate hulgas madalam kui täiskasvanute oma, siis see võib olla selgituseks 2017 läbiviidud uuringust üles kerkinud väljakutsele – õpilased pöörduvad lihtsate probleemide lahendamiseks pigem täiskasvanu poole, kui oma eakaaslase poole;
    - Luua enam abimaterjale e-keskkondadesse, mis oleks sobilikud ka nooremale lugejaskonnale;
    - Koolitused õpilastele ja vanematele peaksid toimuma võimalusel päriselus, mitte veebi vahendusel ja olema teatud vanusest ka praktilised;
    - õpetada õpilastele erinevate paroolide vajalikkust koos võimalusega kasutada paroolihaldurid, et ei tekiks vajadust kasutama hakata kergeid ja lühikesi üksteisele sarnanevaid paroole. Samuti vähendaks see vajadust olla ühest teenusepakkujast sõltuv või salvestada paroole brauserisse;
- Viia läbi eriolukorra korral käitumise instrueerimised läbi ka koolides 7.-12. Klassis kui ka kutsekoolides ja ülikoolides, kes olid kõige enam valmis antud olukorra lahendamist võtma enda peale, kõiki teisi Eesti elanikke kuulamata, kes oleks jäänud rahulikuks.
    - Kuna erinevate salaseltsingute ja alternatiivsete kanalite vastu tunnevad huvi enamjaolt pigem noored, siis see näitab, et nendega tuleks vastavaid asju ka enam arutada, et arendada kriitilist mõtlemist erinevatest kanalitest tuleva infovoo osas;
    - Gümnaasiumi X klassi õpilased vajavad enam pädevuste tõstmist erinevatel teemadel, et ühiskonnas paremini hakkama saada. Näiteks tuleks enam ajaloo ja kodanikuõpetuse tundides rääkida riigi toimimisest ja riikide vahelistest suhetest ning konfliktide lahendamisest, ilma, et selle pealt algaks kohe kolmas maailmasõda.
- Lastega tegelejatele (õpetajatele, koolitajatele, ringijuhtidele jt.) tuleb pakkuda küberkaitse ja -hügieeni alaseid koolitusi kohustuslikult (täiendkoolitus, õpetajakoolitus).

Soovitused täiskasvanute harimiseks:

- luua täiskasvanutele täiskasvanud õppijatele toetav veebileht. Kui lastele ja lapsevanematele ja õpetajatele on programm „Targalt internetis“, siis täiskasvanutele, kes sinna sihtrühma ei kuulu pole oma keskset veebipesa kuskohast otseselt

„inimkeeles“, mitte „IT keeles“ abi saada, uudiseid lugeda, teste teha ja oma küberhügieeni alastes oskustes veenduda;

- luua koolitusprogramm või e-kursus, mida saab inimene või tööandja kasutada oma töötajate koolitamiseks. Kõige lihtsam on teha ennetustööd inimestega, kes on veel haridussüsteemis – koolis, ülikoolis, kutsekoolis või osalevad koolitustel. On vaja tekitada formaalseid ja mitteformaalseid õppimisvõimalusi täiskasvanutele, kes enam haridussüsteemis ei ole;
- märgata erinevaid sihtrühmi ja vajadusi ühiskonnas (vanemad inimesed, vähese digioskusega inimesed). Kõik ei pea olema küberhügieenis samal tasemele, aga kõikidel peaks olema baastase. Kuna täna puudub arusaam, mis on baastase ja mis on selle järgnevad astmed praktilisel tasemel, siis tuleks kõigepealt luua maatriks ning selle alusel saab hakata juba looma teste ja materjale, kui ka koolitusi;
- kasutamata ressurss on tööandja poolsed koolitused tavalisele töötajale, eriti oluliseks peetakse avaliku sektori pädevust antud vallas.