NutiKaitse 2017

Nutikoolitus

Koolitusmaterjal koolitajale

Sisukord

Sissejuhatus

Käesolev materjal on mõeldud kasutamiseks sisekoolituse koolitajatele koolituse „Nutikoolitus edasijõudnutele“ läbiviimisel. Siia võiks enne välja printimist lisada omi märkmeid. Nagu lektori materjalid ikka, on seegi mõeldud koolitajale, mitte kuulajatele jagamiseks.

Enne koolitust tuleks end õpilase materjali ja slaididega kurssi viia, soovitav oleks siin käsitletud asjad ka nutiseadmes järele proovida. Kui pole käsitletavate äppidega varem kokku puutunud, siis tuleks ka neid lähemalt uurida.

Pealkirjad on jäetud õpilase materjaliga samaks, sisuks on mõtted, millest lisaks ja mida rõhutades võiks antud teemas rääkida. Siintoodud soovitusi ei maksa võtta kui reegleid, kõigesse tasub suhtuda loominguliselt ja tegutseda vastavalt kuulajate tasemele, soovidele ja võimalustele. Koolitus peaks toimuma pigem suunatud diskussiooni, kui loengu vormis.

Edu ja jaksu soovides, koostaja Peep Võrno, IT Koolituskeskuse OÜ.

Millega läbi viia

Vahenditest läheb tarvis:

- Projektor
- Arvuti
- Kellele meeldib sodida, siis vildikad + valge pind
- Demode jaoks mõni nutiseade, soovitavalt tahvel. Eriti hea, kui on selline, mis pole parasjagu muuks kasutusel, siis saab demoda ka algseadete taastamist. Seda ehk siis kõige lõpus ;)

Keerulisem koht on tarkvara, mille abil näidata nutiseadme pilti arvutiekraanil ja projektoris. Kui projektor toetab pildi otseedastust DLNA vms tehnoloogia vahendusel, siis saab enamustest nutiseadmetest saata ekraanil oleva otse projektorisse. Kui niipidi ei õnnestu, siis on abiks äpp + arvutis jooksev *soft*. Paljudel tootjatel on sellised lahendused olemas, Samsungil kannab see näiteks nime SideSync.

Kui konkreetsel mudelil/tootjal säärane võimalus puudub, siis tuleb vaadata universaalsete vahendite poole:

- **Vysor** (http://www.vysor.io/) võimaldab pildi ülekannet läbi USB kaabli
  - Head:
    - Telefoni pole tarvis midagi installida, piisab „USB debugging“ lubamisest
    - Töötab Chrome'i platvormil, seega sobib nii Windows, Linux kui ka Mac
  - Vead:
    - Arendus endiselt beta staadiumis
    - Vajab ühenduseks kaablit
    - Arvutisse peab lisaks Vysor'ile olema installitud ka ADB driverite komplekt
    - Kohati ebastabiilne
- **AllCast -** saadab ja võtab vastu üle AllCast protokolli
  - https://chrome.google.com/webstore/detail/allcast-receiver/hjbljnpdahefgnopeohlaeohgkiidnoe/related
  - https://play.google.com/store/apps/details?id=com.koushikdutta.mirror)
    - Head:
      - Ühendub üle WiFi – kaableid pole vaja
      - Töötab Chrome'i platvormil, seega sobib nii Windows, Linux kui ka Mac

        - Võimaldab suhtlust kõigi AllCast (ChromeCast) protokolli valdavate seadmetega (projektorid, telekad jne)
        - Vajutusi näidatakse ka ekraanil, selle võib soovi korral välja lülitada
    - Vead:
        - Windowsi tulemüür segab, tuleb kas ajutiselt välja lülitada või kohandada reegleid (lubada UDP/TCP pordid 53515)
        - Vajab WiFi seadmete omavahelist nähtavust
        - Logo jääb nutiseadme ekraanile ripendama
        - Arendus beta staadiumis
        - Ei tööta Androidi versioonidega < 5.0 (Lollipop)
- **MirrorOP** (http://www.mirrorop.com) pildi ülekanne USB kaabli või WiFi vahendusel
    - Head:
        - Töötab Windowsi ja Mac'i peal
        - Ühendus üle WiFi või USB
        - Seab ise tulemüüri reeglid paika
        - Väidetavasti töötab ka MiraCast'i seadmetega (telekad, projektorid jms)
    - Vead:
        - Ei tööta Androidi versioonidega < 5.0 (Lollipop)
        - Tasuta versioon töötab 5min, hind 9,99$
- **TeamViewer QuickSupport** (https://www.teamviewer.com) pildi ülekanne interneti vahendusel. Tasub tähele panna, et osadel seadmetel võib olla vajadus installida lisaks TeamViewer QuickSupport äpile ka vastava tootja nimega QS AddOn
    - Head:
        - HTTPS ühendus luuakse TeamVieweri serveri vahendusel (umbes nagu Skype), ei sega piirangud tulemüüris, võib ühenduda ka 3G või 4G vahendusel
        - Arvutisse ei pea ilmtingimata installima, võib käivitada ka niisama

        - Kasutan ise ;)
    - Vead:
        - Ei tööta kehva internetiühenduse korral
        - Tasuta (demo) versiooni maksimaalne sessiooni pikkus on 1h

NB! Demode läbiviimisel jälgida, et oma paroole kogemata kõigile ei näitaks!

Alustuseks

Kuna tegu on sisekoolitusega, siis on inimesed ilmselt omavahel tuttavad, seega tutvumisringi teha pole vist suuremat mõtet. Küll aga tasuks alustuseks lasta igaühel pisut rääkida oma kogemustest nutiseadmete- ja üldse digimaailmaga.

1. Nutiseadmed

1.1. Ülevaade

Hea võimalus jätkata diskussiooni ja klass suhtlema saada.

Rääkida, milliseid üldse on, milliseid ise on saanud kasutada. Uuridal klassilt sama.

Mis meeldib-ei meeldi diskussioon. Liiale ei tasu muidugi minna, sest aeg tiksub ;).

1.2. Mõisted

Pisuke teadmiste kontroll diskussiooni sees, saab ettekujutuse kuulajate tasemest. Asjust, mida kõik, võib üle libiseda. Kui ilmneb, et tase on madalamapoolne, siis võib tagapool tulevaid keerulisemaid teemasid lihtsamalt võtta ja vastupidi. Oluline on pidada turvalist kasutamist keskse teemana.

1.2.1. Andmekasutus

Rõhuasetus võiks olla andmekasutuse ja telefoniarve seostel. Mõtteid-soovitusi, mida teha, et üle rahakoti ei paisuks.

1.2.2. Bluetooth

Põhipoint – BT on mõeldud kaablijupi asendajaks – kaugele ei peagi ulatuma. Ilma paaritamata ei tööta.

1.2.3. GPS (Global Positioning System)

Siinkohal võiks muu sees juttu teha ka turvalisusest – kas on mõtet lasta oma asukohta igale poole kirja panna.

1.2.4. Infrapuna

1.2.5. Lennurežiim (*Airplane mode*)

Muu hulgas mainida seda ka aku säästmise või öiste helinate vältimise nipina. Telefon on ju sees – äratuskell töötab, kõned-sõnumid ei saabu ja aku on hommikul värskem.

1.2.6. Mitmepuutelisus (*multitouch*)

1.2.7. Mobiilne kuumkoht (*Mobile Hotspot*)

Muu seas mainida ühiskasutusest tekkivaid suurenenud andmemahte ja turvariske.

1.2.8. Mobiilside (mobiilne andmeside, 3G, 4G)

1.2.9. NFC (Near Field Communication)

Ehk näiteid, kuidas NFC töötab, kui on selle võimeline seade olemas. Lisaks mainida ka, et lukustatud telefon turvakaalutlustel NFC'd pidi saada ei ole

1.2.10. Puutetundlik ekraan (*touchscreen*)

Mainida puutetundlikke abivahendeid – kindad, pastakaotsad jms. Rõhutada, et märjana ei tööta – ka veekindel nutiseade võib merehädas olles kasutuks osutuda!

1.2.11. Rändlus (*roaming*)

Viidata piirialadel (nt Narvas) varitsevatele "lahketele" naaberriikide operaatoritele ja vajadusele kasutada käsitsi võrgu valimist, et kulukasse võõrasse võrku sattumist vältida.

EL-s on alates 2013. aastast asutud, loodava ühtse digitaalse turu raames, piirama sideoperaatorite poolt "leiutatud" rändlustasude määrasid. Eesmärk on 15. juuniks 2017 rändlustasudest vabanemine.

Alates 30. aprillist 2016 kehtivad kõigile EL-s tegutsevatele sideoperaatoritele rändlustasude piirhinnad, mida koduvõrgus võetavatele tasudele tohib lisada kui klient kasutab teenust välismaal (sh väljaspool EL riike) viibides.

Rändlustasude piirhinnad on (20.04.2016 alates) järgmised:

- Kõned (tegemine ja vastamine): koduvõrgu tasu + 0,05€/min
- SMS: koduvõrgu tasu + 0,02€/sõnum
- Andmeside: koduvõrgu tasu + 0,05€/MB

Rändlustasu lisamine ei ole operaatorile kohustuslik. Mõned operaatorid on rändlustasude lisamist omaalgatuslikult juba piiranud. Tasub operaatorite poolt pakutavaid hindu ja teenuste sisu võrrelda.

Vt ka (ing.k): https://ec.europa.eu/digital-single-market/roaming

1.2.12. Salvestusruum (*storage*)

Tähele panna, kas kuulajad teevad ikka vahet mälul (RAM) ja salvestusruumil, vajadusel seletada.

1.2.13. WiFi

Kui seltskond tundub aru saavat, siis ehk rääkida siinkohal ka WEP'i ja WPA/WPA2 erinevusest ja miks WEP on saadanast.

1.3. Nutiseadmete liigitus

Rohkem selline silmaringi ja kodulugemise teema

1.3.1. Operatsioonisüsteemi järgi

Kuulajad peaksid aru saama, et igal OS-il on omad rakendused ja kohad, kust neid leiab. Selgitada, et alati pole kõiki äppe kõigile platvormidele olemas.

1.3.2. Suuruse järgi

Kuidas võiks kutsuda eesti keeles *phablet*it?

1.4. Statistika ja trendid

Hulk kodulugemist huvilistele, arutelu võimalus.

1.5. Millised Androidi äpid on Eestis kõige populaarsemad?

Suhteliselt subjektiivne nimekiri kokku pandud erinevate andmekogude põhjal. Võib proovida kokku panna „klassi TOP'i“. Kirjeldused pärit äppide juurest.

1.5.1. Facebook

1.5.2. Pangaäpid

1.5.3. ERR

1.5.4. Travel äpp

Reisijale abiks asi, kui sihtriigis ikka internetti leidub.

1.5.5. TV3 Play

1.5.6. Pargi.ee

1.5.7. Viber

1.5.8. Elektriäpp

1.5.9. RMK

1.5.10. Elisa Raamat

1.5.11. mElu

1.5.12. NETI

1.5.13. Taxify

1.5.14. Tele2 Eesti

1.5.15. Smardi äpp

1.5.16. Eesti rakendused

Seda ehk eraldi esile tuua, keskne koht kõigi Eesti äppide leidmiseks

1.6. Mida kasulikku saab nutiseadmega teha?

Mida keegi teeb, mis on lahedamad või erilisemad kasutusalad.

1.6.1. Grupitöö vahendid

Mis on grupitöö ja miks peaks sinna kaasama digivahendeid, kuidas vanasti sai?

1.6.2. Microsoft Exchange Activesync

Kui organisatsioon kasutab Exchange'i, siis muule jutule lisaks võiks siinkohal arutada, kuidas nutiseadmetest rohkem abi võiks olla. Kindlasti tuleks rääkida ka Exchangest, kui tihtipeale ainsast valmis seatud võimalusest „jalutama läinud“ telefoni sisu kustutada ja sellest, et kasutaja saab Outlook Web Accessi abil seda ise teha.

Kui on sobilikult seadistatud Exchange ja nutiseade, mille sisu võib hävitada, siis oleks seda kasulik demonstreerida.

Rõhutada võiks ka ohtu, mis saab siis, kui administraator seadme valikuga eksib. Backup on alati oluline!

1.6.3. Muud kontod

Kuidas saab päris hästi hakkama ilma Exchangeta, Google'i näitel

1.6.4. Veel grupitöö vahendeid

Mida veel selleks otstarbeks leidub. Diskussiooni koht – milline grupitöö digitaalne abivahend tundub parim.

1.6.5. Asukoha määramine

Alustada võiks aruteluga teemal, mida halba võiks teha see, kui terve ilm kellegi hetkeasukohta teab. Kas ja miks peaks seda võõraste silmade eest varjama. Mida head on asukoha määramises, kuidas see töötab. Kindlasti mainida ka turvalisuse küsimust ja turvalise kasutamise nüansse

1.7. Kasulikke äppe

Võiks võtta siit saidilt hetkeseisu ja võrrelda seda trükituga
http://www.appbrain.com/stats

Banco de Brasil on hea näide sellest, kuis kõrge reiting ei tähenda eriti midagi, äppide reitingutesse tasub alati reservatsiooniga suhtuda. Parimaks nõuandjaks on teised kasutajad, ehk siis uurida mida mujal internetis asjast kirjutatakse. Kui ei kiideta, siis pole veel häda miskit. Laitusi tuleks rohkem tähele panna – inimestele meeldib ikka negatiivset emotsiooni jagada.

Kui on teisi eelistusi, siis miks ka mitte neist rääkida, küsida ka klassi arvamust. Kindlasti tuleks üle vaadata käsitletavate äppide load ja võiks arutleda nende otstarbekuse üle.

Käsitletavaid äppe võiks enne loengu pidamist järele proovida. Ei pea siinsetest kinni pidama, kui organisatsioonis näiteks muid kasutatakse.

- **SwiftKey Keyboard**
- **Gesture Search**
- **Polaris Office**
- **Google'i tõlge**
- **QR Droid Private – siin võiks ühtlasi rääkida ka avalikes kohtade olevate QR koodide taga olevatest potentsiaalsetest ohtudest ja kuidas neist hoiduda**
- **MAPS.ME**
- **Waze**
- **(Google) Sky Map**
- **Podkicker Podcast Player**
- **GPS Test**

1.8. Pilveteenused

Kes ja kas ja milliseid pilveteenuseid kasutab. Rõhutada vajadust veenduda teenuse pakkuja usaldusväärsuses, enne turvatundlike andmete pilve paigutamist. Võiks arutada muude valikukriteeriumite üle, k.a. majasisese pilveteenuse püstipanek, selle head ja vead.

1.8.1. ZoneCloud

Kohalik teenusepakkuja, pikk ajalugu.

1.8.2. Google Drive

1.8.3. OneDrive (endine SkyDrive)

Võiks siinkohal pisut ka Office 365'st rääkida, kui see teema tuttav on

1.8.4. DropBox

1.8.5. Box

2. Turvalisus

Rõhutada, et turvalisus ei ole lõplik tulemus, et kui on tehtud 1, 2, 3, … 13 asja siis ongi turvaline. See on pidev protsess. Maailm muutub, vanad ohud aeguvad ja ilmneb uusi.

Siin teemas rääkida ja tuua näiteid kindlasti ka turvalisuse ja käideldavuse ehk kasutuskõlblikkuse igavesest vastuolust.

Pole olemas väheolulisi andmeid, kõike võib õnnestuda kurjasti kasutada.

Tasuks läbi vaadata see uuring, saab mõtteid juurde:

http://www.vaatamaailma.ee/wp-content/uploads/veeb-Nutiseadmete-kasutajate-turvateadlikkuse-ja-turvalise-k%C3%A4itumise-uuring_ARUANNE-2014.pdf

2.1. Kui unustasid oma nutiseadme ühistransporti…

Rõhutada, et turvamata seadme kaotamisel on risk kaotada rohkem raha, kui seade ise väärt.

Võib leiutada muidki sääraseid „mis siis kui…“ tüüpi stsenaariume ja neid üheskoos lahata:

- „kui telefoniarvelt on näha kummalised kuluread“
- “kui soovin telefoni kinkida/müüa“
- „kui laps sai telefonile/tahvlile küüned taha“
- „kust võiks abi saada kui“ jms.

2.1.1. Seadme lukustamine

Kas ja miks lukustada – mugavus vs turvalisus.

Millised lukustusviisid on olemas, nende head ja vead.

Rõhutada, et hädaabi numbreid saab valida ka lukus seadmega.

- **Libistamine** – turvalisus puudub.
- **Muster** – keskmine turvalisus. Näpuga veetud rada võib näha olla.
- **PIN kood** – hea turvalisus.

PIN koodi häkkimise robot:

http://www.forbes.com/sites/andygreenberg/2013/07/22/pin-punching-robot-can-crack-your-phones-security-code-in-less-than-24-hours/#2715e4857a0b26e8116558a8 (kui aeg lubab võiks seda videot näidata)

- **Parool** – kõrge turvalisus. Nippe, kuidas võiks parooli meeles pidada. Kindlasti mitte ära rääkida oma süsteemi (selline ju on? ;), ega lasta ka klassist seda viga

kellelgi teha. Proovida kamba peale miskit leiutada. Selgitada mitmetes kohtades sama parooli kasutamise ohte.

Kui aeg lubab mängida selle saidiga: https://howsecureismypassword.net/ Kindlasti rõhutades, et säärasesse kohta oma päris paroole sisestada mingil juhul ei tohi.

- **Sõrmejälg** – kõrge turvalisus. Rõhutada sõrmejälje „varastamise“ võimalust kas seadmelt või muudelt esemetelt või sootuks magajalt.

Peale „jalutamas käinud“ seadme tagasi saamist tasuks tõsiselt kaaluda tehase seadete taastamist, sest pole teada, millist nuhkvara ja kuidas võib olla seadmesse peidetud.

2.1.2. Sisu krüpteerimine

Jällegi turvalisuse ja käideldavuse vastuolu – krüpteerimine kaitseb andmeid võõra silma eest, aga suurendab andmetest ilma jäämise riski krüptovõtme kaotamise läbi.

2.1.3. Kaugjuhtimine

Veelkord kahe otsaga vorst – turvaline on hoida GPS ja andmeside välja lülitatuna, aga see muudab võimatuks telefoni leidmise ja ka sisu kustutamise. Jääb loota, et varas ühendab seadme häkkimisvahendite installiks moel või teisel internetti ja siis ... ;)

Diskussioon – võib olla ei tasuks selles kontekstis kadunud telefoni SIM kaarti liiga ruttu sulgeda?

2.2. Sissemurdmise vältimine

Pea 90% digitaalsetest sissemurdmistest viiakse tänases maailmas läbi vana head Trooja hobuse nippi kasutades. Võiks tuua näiteid või siis diskuteerida, kuidas saab ka turvateadlikku kasutajat meelitada „hobust tuppa vedama“.

2.2.1. Tarkvara värskendamine

Alati peaks tarkvara värskendused installima. Tõsisema turvaaugu esinemisel on sissemurdmine tublisti kergem!

2.2.2. (Mitte)rootimine

Rootimist ei soovita! Räägime vaid selle negatiivsetest külgedest, netis levivatest troojalase installi soovitavatest väärjuhenditest, automaatse värskendamisvõimaluse kadumisest jne

2.2.3. 0-päeva rünne

Mis on ja kuidas vältida. Rõhutada, et kui mitte avada tundmatust allikast pärit dokumente (ka. MMS-id) või veebilinke, mitte installida tunnustatud poodide väliseid äppe, seadet mitte rootida, siis võib end peaaegu kindlana tunda. Ainus, mis 0-päeva ründe ohu vastu tegelikult aitab, on turvavärskendus, mis augu sulgeb – tõsi, siis pole enam 0-päev...

2.2.4. Viirused & Co.

- **Nakatamine** – enne diskuteerida, kuidas võiks pahalane seadmesse pääseda.
- **Eesmärgi saavutamine** – millised võiksid veel olla nutiseadmesse pääsenud pahavara eesmärgid.
- **Levik** – Millised võiksid olla levimeetodid?

Tõenäolisem on nutiseadmel olla „viirusekandja“, kui tegelikult viiruse poolt rünnatud saada. Ettevaatust sellegipoolest ja anti-viirust ei maksaks unustada!

Kui ilmnes, et seade on „viirusekandja“, siis on asi ohutu ja piisab vaid pahade failide kustutamisest. Kui on leitud seadmest „töötav“ viirus, siis parim eemaldamise viis on algseadete taastamine, sest viirus võib end (turvaaugu abiga) sisse seada süsteemi kaustadesse, kuhu tööprogramme s.h. anti-viirust ei lastagi. Pärast mitte unustada turvapaikade paigaldamist!

2.3. Et salasilm ei seletaks...

Seletada ära vahemehe ründe (*Man In the Middle*) olemus ja kui ei käi kuulajatele üle jõu, ka mõned selle teostamise viisid.

2.3.1. Turvalised ja turvamata protokollid

Seletada lahti turvatud protokolli olemus ja miks ei tohi kahtlase sertifikaadi korral ühendusega jätkata. Siinkohal on sobilik needa administraatoreid, kes kasutavad *selfsigned* serte ja juhendavad kasutajaid veateatest mitte hoolima! Selline praktika võib olla väga kaugele ulatuvate ohtlike tagajärgedega, kuna uinutab kasutajate valvsust.

Rõhutada, et üle turvamata protokolli tundlike andmete edastamine on suur risk. Protokollid dikteerib serveri pool, kasutaja ei saa midagi muud teha, kui kasutamisest loobuda.

2.3.2. VPN

Lühidalt seletada, mis on VPN ja millistest komponentidest see koosneb, et kasutaja on vaid „helistaja“ rollis, andmed saab ta oma võrgu administraatorilt.

2.3.3. Login väliste vahenditega

Selgitada võimalust tünga saada *fake* login aknaga, kust nimed/salasõnad kokku korjatakse. Sisuliselt *Man In the Middle* tõugu rünne. Kodumaiste teenuste puhul eelistada ID-kaarti, muudel juhtudel tuleks teha konto teenusepakkuja juurde.

2.4. Äppide turvalisus

Selgitada põgusalt „liivakasti“ kontseptsiooni.

2.4.1. Seadmega kaasa pandud äpid

Pisuke arutelu, kellele millised eelpaigaldatud äpid tunduvad vajalikud ja millised vähem vajalikud.

2.4.2. Äppide paigaldamine

Võimalusel näidata ka mõne äpi installi.

2.4.3. Äpi juurdepääs seadmele

Selgitada võiks läbi „liivakasti“ ja sinna kaasa antavate „mänguasjade“. Millised võivad olla ohud, kui äpp saab ligi kontaktandmetele ja/või failisüsteemile. Alati ei pea liigsete ressursside küsimine pahatahtlik, võib olla ka arendaja laiskus ja/või ebakompetentsus. Võib kasutada ka muid näiteid peale taskulampide.

2.4.4. Loata ja luba vajavad ressursid

Vaadata enamkasutatavaid ressursse ja seda, kas nende jaoks on luba vaja. Võiks diskuteerida lubade vajalikkuse üle.

2.4.5. Äppide eemaldamine

Võimalusel näidata eemaldamist, mainida tasuliste äppide eelistatavat uninstalli läbi Play poe.

2.4.6. Tehase äppide peatamine

Seletada kontseptsiooni „vähem äppe – vähem teoreetilisi turvaauke“, samuti äpi peatamisega kaasnevat võitu mälu kasutuses ja aku tööajas. Drastilisi muutusi tavaliselt ei kaasne. Rõhutada vajadust taas kasutusse võtmisel turvapaikade installi vajadust. Soovitada äppe peatada ükshaaval ja jälgida tulemust, et ei „tulistaks endale jalga“.

2.4.7. Valik äppide vahel

Võiks koos vaadata, kuidas on hetkeseis:

- http://www.appbrain.com/stats/number-of-android-apps

Selgitada, miks võiks olla sarnaseks otstarbeks mitu äppi, millal vaikimisi äpp valida ja millal võib-olla mitte. Kuidas siiski kasutada „mitte vaikimisi“ äppe. Näidata, kuidas vaikimisi valik maha võetakse.

2.4.8. Äpid väljastpoolt Google'i poodi

Rõhutada säärase lähenemise riske ja erakorralisust. Meenutada vajadust peale installi keeld taastada.

2.5. Tahvelarvuti turvalisus

Tahvli turvalisuse eripärad. Mainida uuringut ja sellest johtuvat, et tahvleid kasutatakse pigem mitme peale.

2.5.1. Mitu kasutajakontot

Võimalusel demonstreerida kasutajakontode tegemist ja erinevate kasutajatena sisse-välja logimist, külaliskontot ka. Kui aeg võimaldab, siis näidata ka äppide installi ja mis juhtub, kui kasutaja eemaldatakse.

2.5.2. Kui kasutajakontod pole võimalikud

Võiks valida mõne sobiliku äpi ja selle võimalusi demonstreerida, sealjuures rõhutades, et see ei ole „maailma parim äpp“, kasutajad peaksid ise omad valikud tegema lähtudes konkreetsetest eelistustest ja vajadustest.

2.5.3. Nutiseade lapse käes

Rõhutada, et väärtuslikke ja isiklikke andmeid sisaldavat seadet lastele mängimiseks anda ei tohi! Samas on see küllalt levinud, aga äärmiselt ohtlik, praktika. Võiks diskuteerida teemal, kas pereringis on saladusi, milline info võib olla liiga isiklik ka pereringis jagamiseks. Laste omavahelise nääklemise küberkiusamiseks kasvamise risk nii peres, kui laiemas ringis.

2.6. Nutiseadmete turvaline kasutamine

2.6.1. Piilujate vältimine

Rõhutada, et silmad on kõikjal. Ettevaatust paroolide sisestamisel – mis on parooli nähtavuse keelamise head ja vead.

2.6.2. Varundamine ehk backup

Selgitada, kuidas ja millist infot nutiseadmest saab hoida näiteks oma Google'i konto juures, millist peaks varundama pilveteenusesse või arvutisse.

2.6.3. Seadme lähtestamine

Tuua näiteid, mis põhjusel võib olla lähtestamine vajalik või lausa kohustuslik. Mainida kontrollimise vajadust võõrandamisel, et kas ikka sai tühjaks. Võõrandamisel mitte unustada seadmesse andmetega mälukaarti. Rõhutada tarkvaravärskenduste installi vajalikkust peale lähtestamist. Kui on kasutada sobilik seade, võiks ka lähtestamist ja värskenduste installi demonstreerida. Mainida ka lähtestamise võimalust ilma seadet tegelikult käivitamata – ükski parool vms ei takista vargal seadet kasutusse võtmast, aga andmetele ta ligi ei saa.

2.7. Nutiturvalisuse 5 kuldreeglit

Võiks diskuteerida, milliseid reegleid pakuksid kuulajad lisaks, kui reegleid oleks näiteks 10. Sobilik koht käia sealjuures läbi eelnenud osast turvalisust puudutavad punktid ja mahutada neid siintoodud punktide alla.

2.7.1. Kasutan oma nutitelefonil ja tahvelarvutil ekraanilukku

2.7.2. Mõtlen enne kui ligipääsuinfot või paroole jagan

Rõhutada parooli teistega jagamise äärmist ohtlikkust ja sellise teo ebameeldivat tavalisust. Tuua näiteid erand-erand-erandjuhtudest, kus muudmoodi lihtsalt ei saa.

Kindlasti veelkord rääkida seadmete ühiskasutusest tulenevatest riskidest, rõhutades sama parooli mujal kasutamise keeldu.

2.7.3. Paigaldan rakendused ametlikust poest

Korrata-meenutada tingimusi, millal võiks lubada installi mujalt. Näitlikustada, kuidas saab troojalane sellise piiranguta seadmesse.

2.7.4. Uuendan nutiseadme tarkvara

Kui aeg lubab, võiks diskuteerida, et mida teha välismaal – roaming kallis jne. Kuidas olla siis eriti ettevaatlik.

2.7.5. Kasutan sisselogimiseks ja digiallkirja andmiseks Mobiil-ID võimalusi

Võimalusel demonstreerida.

Rääkida, et SIM kaardi ja Mobiil-ID PIN koodid on täiesti erinevad asjad. Mainida PIN1-2 ja PUK koodi muutmise kasulikkust peale kaardi saamist. Samuti tuleks ära mainida, et M-ID töötab üle SMSide – välismaal palju kasutades võib arvele mõju avaldada.

Eraldi tuleks välja tuua, et M-ID ei ole nutiseadme teenus. See töötab pea kõigi mobiiltelefonidega, mis on suutelised SMSi saatma ja vastu võtma.

3. Nutikaitse 2017

Projekti „NutiKaitse 2017“ eesmärk on muuta Eesti turvalisema infoühiskonnaga riigiks, aidates nii ellu viia Infoühiskonna arengukava 2020 katusvisiooni: Eestis kasutavad avalik ja erasektor maksimaalselt info- ja kommunikatsioonitehnoloogia (IKT) võimalusi, et nutikate lahenduste abil tõsta inimeste elukvaliteeti ja tööhõivet, tagada Eesti kultuuriruumi elujõulisus ning suurendada majanduse tootlikkust.

2017. aasta lõpuks soovime, et:

- 70% nutiseadmete kasutajatest kasutab oma seadmeid teadlikult turvaliselt;
- vähemalt 300 000 inimest Eestis kasutab nutiseadmetes Mobiil-ID'd elektrooniliseks isikutuvastuseks ja digitaalseks allkirjastamiseks;
- järgmise põlvkonna elektroonilise isikutuvastuse alternatiivid ja Mobiil-ID edasiarendus on välja töötatud, et pakkuda suuremat kasutusmugavust ja täiendavat turvalisust.

NutiKaitse 2017 projektiga on oodatud liituma nii mobiilirakenduste arendajad, IT-spetsialistid kui ka ettevõtted, kes nutikaitsest hoolivad. Projekti koordineerib Vaata Maailma Sihtasutus.