

# märka last

MTÜ Lastekaitse Liidu ajakiri  
Turvalise interneti päeva erinumber  
2/2016

Nuhkimisest....juriidiliselt

Interneti ohutuse alased  
digipädevused – kelle mure?

**ÜKSKI KÜSIMUS POLE LIIGA  
RUMAL VÕI LIIGA TÜHINE**

PRIVAATSUS JA USALDUS

**KUIDAS TAGADA ENDA KASUTATAVATE  
TEHNOLOOGIATE JA TEENUSTE TURVALISUST?**

**Toimetaja:**

Kerli Kuusk

**Kujundus:**

Katrin Nõu

**Kasutatud pildid:**

[www.shutterstock.com](http://www.shutterstock.com)

**Ajakirja kontakt:**

[ajakiri@lastekaitseliit.ee](mailto:ajakiri@lastekaitseliit.ee)

[ajakiri.lastekaitseliit.ee](http://ajakiri.lastekaitseliit.ee)

**Väljaandja:**

MTÜ Lastekaitse Liit



# SISUKORD

- 10 **Privaatsus ja usaldus**
- 16 **Ameerika salateenistus kuulab pealt ja teeb pilti -  
meie laste teadmised ja hoiakud nutiseadmetega  
seotud ohtudest**
- 22 **Interneti ohutuse alased  
digipädevused – kelle mure?**
- 28 **Projektil Targalt internetis on uuenenud veebileht**
- 32 **Kuidas tagada enda kasutatavate  
tehnoloogiate ja teenuste turvalisust?**
- 38 **Nuhkimisest.....juriidiliselt**
- 44 **Ükski küsimus pole liiga rumal või liiga tühine**
- 50 **[www.vihjeliin.ee](http://www.vihjeliin.ee) – teata internetis levivast laste  
seksuaalset ära kasutamist esitavast materjalist!**
- 54 **Vaata üle oma suhtlusvõrgustike kontode  
privaatsusseaded**

Tule turvalise  
interneti päeva konverentsile

# „Nutikalt netis - Kaitse ennast ja oma sõpra!“

Registreeru  
siin >

09. veebruaril 2016 kell 10.00  
Park Inn by Radisson Meriton Hotellis  
Toompuiestee 27, Tallinn

## Ootame osalema

gümnaasiumi ja  
kutseõppeasutuste õpilasi,  
õpetajaid, õppejuhte ja  
kooli juhtkondi

## Teemad

- Sõprussuhted  
online- keskkonnas
- Vihakõned
- Häbistava sisuga  
pildid ja sõnumid

Oska  
märgata,  
oska aidata!

Konverents on  
**tasuta!**  
Registreerumine kuni  
04. veebruarini

Social  
Engineering ja  
küberkaitse -  
saame selgust!

Vaata konverentsi  
Postimees veebis!

**Kätte on jõudnud ülemaailmselt tähistatav turvalise interneti päev. Eestis on turvalise interneti päeva sõnumiks „Nutikalt netis – kaitse ennast ja oma sõpra“. Sellega kutsume lapsi, noori ja täiskasvanuid internetti ja nutivahendeid turvaliselt ning arendaval viisil kasutama.**

Digipädevuste omandamine on tänapäeva maailmas edukaks hakka- ma saamiseks järjest olulisem. Võtmeroll nende oskuste õpetamisel on koolil ja ka lasteaial. Käesolevast ajakirjast saab teada, millised on laste teadmised ja hoiakud nutiseadme- tega seotud riskide osas. Lisaks saab tutvuda, kuidas näeb digipädevuste õpetamist ette riiklik õppekava ning millised väljakutsed on sellega seoses tänapäeva koolil. Turvalise interneti päeval, 9. veebruaril on kõikidel õpetajatel ja gümnasistidel, aga ka teistel teemast huvitatutel, võimalik uudisteportaali Postimees vahen- dusel jälgida konverentsi „Nutikalt netis - kaitse ennast ja oma sõpra“ otseülekannet.

Üheks digipädevuseks on oskus kaitsta oma privaatsust, isikuandmeid ja digitaalset identiteeti. Kuna internet

on avalik ruum, siis on tähtis hoolikalt läbi mõelda, mida, kuhu ja kellele postitada. Internetti postita- des ja sotsiaalmeedias tegutsedes, tuleb arvestada, et inimesed saavad igasugust sisu endale alla laadida ja levitada. Kui inimene postitab sotsiaalmeedias pilte, kirjeldab enda igapäevaseid tegevusi, ning märgib ära, millises kohas ta parasjagu viibib või millisele üritusele plaanib lähi- tulevikus minna, siis seda kõike on kõigil, ka halbade kavatsustega inimestel, võimalik täiesti seadus- likult vaadata. Seetõttu soovitab Veebikonstaabel käesoleva ajakirja artiklis eraelu kaitseks ligipääsu oma Facebooki või Instagrami profiilidele piirata ning seejuures silmas pida- da ka seda, et võib-olla ei pea kõik sõbranimekirja ja jälgijate hulka kuuluvad inimesed nägema igat infokildu. Projekti Targalt internetis raames on teile selle tarbeks koostatud suhtlusvõrgustike privaatsussätete seadmise juhised, millega soovitan teil käesolevas ajakirjas tutvuda.

Kuigi internet pakub väga palju võimalusi tegutsemiseks, tuleb meeles pidada, et kõik tegevused internetis

siiski lubatud pole. Digikeskkonnas suheldes tuleb järgida seadusi ning moraali- ja väärtuspõhimõtteid. A. Baum kirjutab käesoleva ajakirja artiklis juriidiliselt sõnumisaladusest ja jälitustegevusest.

Lisaks koolile on lapsevanematel väga oluline roll laste suunamisel ja juhendamisel nutiseadmete ning interneti oskuslikumaks ja turvalisemaks kasutamiseks. Lapsevanemana tunne huvi, mida sinu laps internetis teeb, selgita online keskkonnas toimuvat ning julgusta teda küsimuste ja probleemide puhul sinu poole pöörduma. Alati ei pruugi kõikidel lapsevanematel vastused kohe olemas olla, kuid neid saab koos lapsega arutades või spetsialistilt abi küsides leida. Käesolevas numbris saab lugeda, milliste küsimuste ja teemadega seoses interneti kasutamisega on Lasteabitelefoni 116111 poole pöördutud ning millised on nende nõu ja abi andmise kanalid.

Digipädevuste omandamisele aitavad kaasa veel mitmed organisatsioonid ja projektid. Näiteks projekti Targalt internetis eestvedamisel tähistatakse Eestis turvalise interneti päeva

terve nädala jooksul korraldatavate üritustega: konverents „Nutikalt netis – kaitse ennast ja oma sõpra“, meediakampaania „Käitu internetis targalt!“, mitmed teavitustegevused koolides üle Eesti ja temaatilise õpilaskonkursi korraldamine. Peamistest tegevustest leiata ülevaate käesolevast ajakirjast ning veebilehelt [www.targaltinternetis.ee](http://www.targaltinternetis.ee), millel on jaanuarist olemas ka eraldi veebilehed lastele [laps.targaltinternetis.ee](http://laps.targaltinternetis.ee) ning noortele [noor.targaltinternetis.ee](http://noor.targaltinternetis.ee).

## HEAD TURVALISE INTERNETI PÄEVA!



*Kerli Kuusk*

projekti Targalt internetis teavitustöö koordinaator

*Projekti „Targalt internetis“ viivad Euroopa Komisjoni kaasrahastusel ellu MTÜ Lastekaitse Liit, Politsei- ja Piirivalveamet ning Lasteabi telefon 116111.*

**Kutsume kõiki koole, lasteaedasiid ja teisi laste ja noortega tegelevaid organisatsioone turvalise interneti päeva tähistama ning veebruarikuu teisel ja/või kolmandal nädalal oma laste ja noortega nii interneti ja nutiseadmete kasutamise kui ka ohutuse temaatikat käsitlema.**

Selleks oleme teile koostanud teavitusematerjali, millest leiata videoid, teste, artikleid ja kasulikke veebilehti, ning mis on leitav <http://www.targaltinternetis.ee/event/anna-teada-kuidas-tahistasite-oma-koolis-lasteaas-turvalise-interneti-paeva/>.

Ühtlasi palume teada anda, mida vahvat te selle päeva või nädalate raames tegite, vastates paarile küsimusele. Ootame teie lühiülevaadet toimunud üritustest ja tegevustest kuni **22.02.2016**. Kõik osalenud koolid/lasteaiad/noortekeskused/huviringid/organisatsioonid saavad tunnustuse ja tunnustuse ning Vabariigi aastapäeval avaldame nimekirja, kes on Eestis targalt internetis toimetamisel teistele eeskujuks.

Eelmisel aastal jagasime koolidega sarnast üleskutset. Rõõm oli tõdeda, et paljud koolid üle Eesti tähistasid õpilaste ja õpetajatega turvalise interneti päeva, sh mõned koolid tegid seda esimest korda. Näiteks viidi õpilastega läbi temaatilisi ainetunde, korraldati erinevaid kampaaniaid, teadmisi testiti viktoriinides, viidi läbi arutelusid, vaadati filme, kutsuti erinevaid spetsialiste koolidesse oma tööst rääkima, samuti viisid vanemate klasside õpilased läbi temaatilisi teavitustegevusi noorematega jne. **Kahe nädala jooksul osales erinevates tegevustes ligikaudu 9600 õpilast!**

Koolide ja õpetajate nimekiri on leitav: <http://www.targaltinternetis.ee/event/tunnustame-turvalise-interneti-paeva-tahistanud-koole/>.

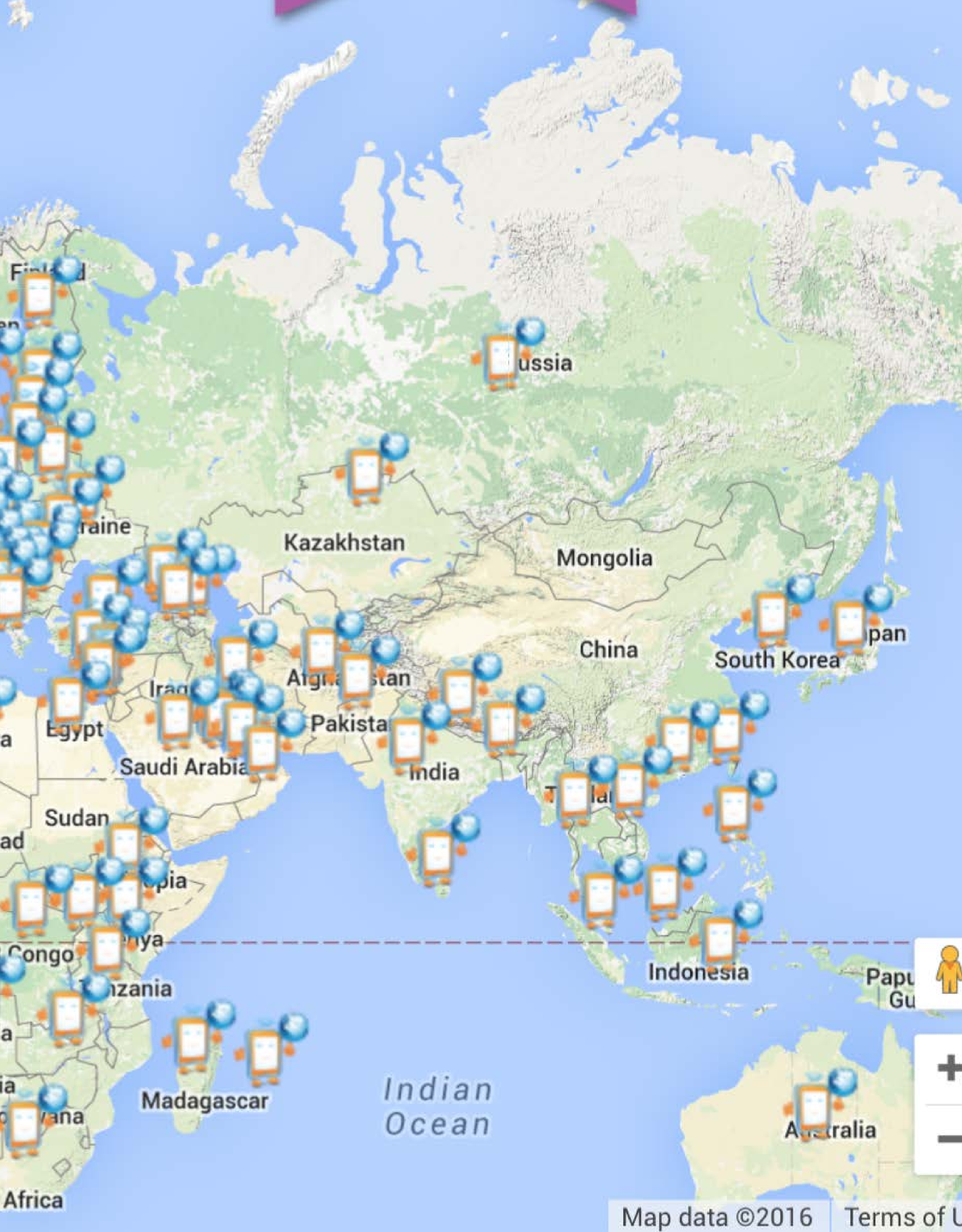
Suur tänu teile. Sellel aastal loodame tähistada turvalise interneti päeva veelgi võimsamalt ning kaasata veelgi enam lapsi ja noori ning miks mitte ka täiskasvanuid.

Kaardil on märgitud kõik maailma riigid, kus turvalise interneti päeva tähistatakse.

Veebilehel [www.saferinternetday.org](http://www.saferinternetday.org) saate tutvuda, mida täpsemalt nendes riikides selle raames tehakse.









# PRIVAATSUS JA USALDUS

*Andero Sepp veebikonstaabel ja Kristi Mäe,*

*Politsei- ja Piirivalveamet*

**Tänapäeval tuntakse üha enam muret oma privaatsuse pärast. Internetikasutajad häirib muu hulgas see, kui võõras inimene jagab kellegi sotsiaalse meedia kanalisse üles laetud fotot või teksti ilma, et oleks autorilt ja omanikult nõusolekut saanud. Selline teabe jagamine on üks sotsiaalse meedia eripäradest ja funktsioonidest.**

Teadlased on sotsiaalse meedia võidukäigu ühiskonda nimetanud massiliseks isekirjutajate ühiskonnaks, kus igaühel on õigus esineda või sõna võtta – see on elementaarne sõnavabadus ühelt poolt. Aga teiselt poolt loob see ka kollektiivse informatsiooni keskkonna, kus kõik saavad jagada ja arvamastust avaldada üksteise kohta. Privaatsuse piirid, samuti autorluse piirid, turvalisuse piirid on hägustunud.

Internetti postitades, sealhulgas sotsiaalses meedias tegutsedes, tuleb arvestada, et inimesed saavad igasugust sisu endale alla laadida ja levitada. Selline informatsiooni jagamise võimalus on üks sotsiaalmeedia alustalaid. Ja sellega tuleb arvestada, kui sotsiaalmeedia sfääri oma sõna ja informatsioonivabadust realiseerima minnakse. Kuid kõik tegevused siiski internetis lubatud ei ole. Nii nagu erinevates kommuunides meie

igapäevases elus, on ka Interneti kommuunis käitumiseks ja tegutsemiseks omad reeglid. Nii nagu me tänaval liikudes vaatame ette ja muretseme oma turvalisuse eest, nii tuleb seda teha ka Interneti keskkonnas.

## **UNUSTAMINE JA LOHAKUS MAKSAVAD KÄTTE**

Kõige tavalisemad vahejuhtumid on seotud erinevate interneti kontode või nutiseadmete lahti unustamisega, mille tõttu keegi saab seda kontot kasutama hakata. Meenub juhtum, kus noormehe Facebooki postitati lakooniline tekst: „Homme lähen kooli ja lasen kõik maha.“ Selgus, et poiss oli jätnud peo ajal oma nutitelefoni järelevalveta ning ta ei saanud postitusest teada enne, kui politsei tuli teda kinni pidama.

Nutitelefoni on tänapäeval seotud ka kõikvõimalikud veebikontod.

Lihtsamad juhtumid on seotud koolis või töökohas lukustamata arvuti ja välja logimata Facebooki kontoga, kuhu midagi rumalat postitakse.

**Lahti unustatud kontot võib võrrelda naaberkorteri avatud uksega. Sõltub inimese eetikast ja kasvatuses, kas ta põikab sinna võimalusse lihtsalt sisse uudistama, või otsustab sealt ka midagi napsata. Tavaelus me taunime sellist käitumist.**

Kas ka arvuti taga ja Interneti kogukonnas? Internetis toimime risti vastupidiselt, andmata endale aru, et selline süütuna näiv käitumine võib kaasa tuua kriminaalvastutuse ja kuni kolme-aasta pikkuse vangistuse. On tekkinud arvamus, et Internet on midagi eraldiseisvat, kus nagu igapäevased viisakus ja kombed ei kehti. Et see on koht kus saame end turvaliselt peita ja aliasena teha, mida iganes pähe tuleb, ka selliseid asju, mida tänaval või reaalses maailmas teha ei söandaks.

Kui me jätame lahti oma „veebiukse“, ei pruugi see lõppeda vaid ebameeldiva naljana. Nii mõnigi paha plaanija kasutab lihtsalt ligipääsetavaid või lohakalt avali jäetud kontosid selleks, et need üle võtta ja hankida privaatinfot. Kui konto kaaperdamisest saadakse võrdlemisi kiiresti aru, siis varjatuma meetodi puhul suunatakse e-kirjad automaatselt kaaperdaja e-postile. Lisaks juba kontol leiduvale teabele saab kurjategija ligipääsu ka kõikidele uutele kirjadele, mis saadetakse ohvri e-posti aadressile.

Keerulisemate kontode kaaperdamise meetodite puhul paigaldatakse arvutisse nuhkvara. Olemas on mitmesugust nuhkvara, neist kõige tüüpilisem on „keylogger“. See programm töötab varjatult taustal, salvestades kõik nupuvajutused. Määratud intervalli järel edastab „keylogger“ kogutud andmed kindlale e-postile. Kuna salvestatakse kõik nupuvajutused, saab paigaldaja enda valdusesse ka pahaaimamatu kasutaja paroolid.

Politseid on teavitatud nuhkvara paigaldamisest arvutitesse, autosse ja mobiiltelefoni ning on olnud juhtumeid, kus endine elukaaslane on loginud Facebooki või Skype´i ning järginud eraelulisi vestluseid.

„Keyloggeri„ paigaldamine leiab kasutust näiteks õpilaste ja üksteist mitteusaldavate inimeste seas, kes on vastava nuhkvara kasutamise selgeks teinud erinevaid veebilehti lugedes. Õpilaste eesmärgiks on tavaliselt ligipääs e-kooli. Üks markantsemaid näiteid, mis meenub, on juhtum, kus õpilased said ligipääsu õpetaja e-koolile ja parandasid seal oma hinded. Seda aga märkas õpetaja, kes arvates, et ta on sisestusel eksinud, muutis hinded tagasi. Seepeale läksid noormehed õpetajalt aru pärima, miks nende varasem hinne on asendunud kehvemaga, ning nende pettus tuli avalikuks.

## ISIKLIKUD SUHTED TULEVAD INTERNETTI JÄRELE

Teine levinud „sihtrühm“ on probleemsete lähisuhetega inimesed, kes ei usalda oma kaaslast ning soovivad jälgida ja kontrollida kõike. Ebaseadusliku jälitustegevuse läbiviimine lähisuhtevägivalla juhtumite puhul on küll aeglaselt aga järjekindlalt tõusev trend. Aastas on paar lähisuhtevägivalla juhtumit, kus rakendatakse eraviisilist jälitustegevust.

**Õpilaste eesmärgiks on tavaliselt ligipääs e-kooli. Üks markantsemaid näiteid, mis meenub, on juhtum, kus õpilased said ligipääsu õpetaja e-koolile ja parandasid seal oma hinded. Seda aga märkas õpetaja, kes arvates, et ta on sisestusel eksinud, muutis hinded tagasi. Seepeale läksid noormehed õpetajalt aru pärima, miks nende varasem hinne on asendunud kehvemaga, ning nende pettus tuli avalikuks.**

Sellised inimesed soovivad „keyloggeri“ abil kätte saada paroole, vestlusi ja panka sisenemiseks vajalikke andmeid. Kuid üha sagedamini leiab nuhkvara kasutust ka kättemaksu eesmärgil. Näiteks paigaldas üks mees elukaaslase arvutisse „keyloggeri“ kohe, kui ta pidi tema juurest välja kolima. Mees hankis ebaseaduslikult naise paroolid, logis sisse tema e-posti kontole ning saatis kõikidele kontaktidele sõimukirju.

## **INIMENE ISE TAGAB OMA TURVALISUSE INTERNETIS**

Eelpool öeldu on vajalik mõistmaks, et enda privaatsuse kaitsmiseks ei saa loota ei portaali, IT-osakonna, ega sõprade abile või heale õnnele. Iga inimene peab ise tagama enese veebiturvalisuse. Asutuse poolt antud arvutid ei ole mõeldud teistele kasutamiseks. Koduarvutite puhul tuleb aeg-ajalt üle kontrollida, mis programmid taustal töötavad ja mis tarkvara on kasutusel. Kui kasutame Windows'i operatsioonsüsteemiga arvutit, siis tagab arvuti juurest lahkudes meie turvalisuse nupukombinatsioon WIN + L, mis lukustab arvuti.

**Kui vanemad soovivad tagada tehniliste vahendite abil oma lapse turvalisust, on selleks lubatud alaealise lapse telefoni positsioneerimine. Kui aga on soov jälgida kellegi teise asukohta, siis peab selleks olema selle inimese nõusolek. Samamoodi peab igasugu nuhkvara paigaldamiseks küsima seadme omaniku luba, vastasel juhul rikutakse seadust. Ilma loata ning postkasti omaniku teadmata teise inimese kirjade lugemine võib olla käsitletav sõnumisaladuse rikkumisena (KarS §156).**

Kui rääkida interneti privaatsuse seaduslikest alustest, siis põhiseadusest tulenevat põhiõigust edastatavate sõnumite saladusele kaitseb ka karistusseadustik. Tegu on kuriteoga, kui rikutakse kirjavahetuse ja sidevahendi abil edastatud sõnumi saladust. Soovi korral võib seda ilmselt tõlgendada liialt meelevaldselt ja laiemalt, kui on seaduse eesmärk. Kuid seda täpsustab kohus. Karistusseadustiku järgi saab süüdlaseks olla inimene, kes ise ei olnud sõnumi saaja ega saatja. Peab siiski rõhutama, et rangeid reegleid ja piire ei saa ette kirjutada ning iga juhtum isemoodi.

## UUE AJASTU LAPSED ELAVAD KA INTERNETIS

Kui rääkida lähemalt lapse käitumisest internetist, siis tuleb lähtuda tema vanusest. Lapse internetikasvatuse loogika on sarnane lapse teadmistega iseseisvalt ja ohutult tänaval liigelda. Me ei luba tal linnas üksinda kõndida enne, kui ta teab, mis on lubatud ja mis mitte. Sarnaselt kõikidele tegevustele, on interneti kasutamise puhul olulisel kohal eeskuju. Oluline on lapsega rääkida ja tunda tema tegemiste vastu varakult huvi.

Kui hakata lapse tegemiste vastu huvi tundma alles murde eas, ei pruugi lapsevanema katse olla tulemuslik ega mõjuda omavahelisele suhtlusele hästi. Kui vanema ja lapse vahel valitseb usaldus, tuleb ta probleemiga ise vanema juurde ning vajadust nuhkimise järgi ei ole.

Meeles tuleb pidada seda, et sotsiaalmeedias levitatav info on olemuselt avalik. Kui inimene postitab sotsiaalmeedias pilte, kirjeldab enda igapäevaseid tegevusi, puhkuseplaanid, mõtteid ning märgib ära, millises kohas ta parasjagu viibib või millisele üritusele plaanib lähitulevikus minna, siis seda kõike on kõigil, ka kurikaeladel, võimalik täiesti seaduslikult vaadata. Oma eraelu kaitseks tasub piirata ligipääsu oma Facebooki või Instagrami profiilidele ning seejuures silmas pidada ka seda, et võib-olla ei pea kõik sõbranimekirja ja jälgijate hulka kuuluvad inimesed nägema igat infokildu.

# Ameerika salateenistus kuulab pe teeb pilti - meie laste teadmised ja nutiseadmetega seotud ohtudest

*Rica Williams*

*Vaata Maailma SA kommunikatsioonijuht*





# alt ja a hoiakud



2015. aasta detsembris toimus rahvusvaheline programmeerimist propageeriv kampaania KoodiTund, mille raames mitmed Eesti tuntud inimesed rääkisid oma esimestest kogemustest arvutite ja internetiga. Näitasime seda videot koolitundides lastele, kellele need jutud päris sageli nalja tegid. Lapsi ajas naerma, kui selgus, et Tanel Padar oli 21-aastane, kui ta sõprade abiga esimese arvuti sai. Sest lastel, kellele sama kampaania raames programmeerimise tundi andsime, on enamasti kodus nii arvuti kui ka nutiseade - nutitelefon ja/või tahvelarvuti.

## OLEME INTERNETIS KOGU AEG

**Juba 2014. aasta detsembri andmed näitavad, et põhikooliks (12-14 aastased lapsed) on nutitelefonid ligi 80%-l õpilastest. 6-8-aastastest lastest omas siis isiklikku nutitelefoni 38% ning tahvelarvuteid 21%. Samast uuringust selgus, et 6-14-aastastest lastest 70% saavad oma nutitelefoni kasutada igal ajal ja nii palju, kui soovivad. Seega on nutiseadmed ja internet neile enesestmõistetavad.**

2016. aasta jaanuaris Suurbritannias avaldatud andmete järgi veetsid alla 16-aastased lapsed esimest korda rohkem aega internetis kui telekat vaadates. 5-15aastased lapsed veedavad 3 tundi päeva internetis, kui teleka vaatamisele kulub 2,1 tundi. Sealjuures ei teinud uuring vahet, kas telekast vaadati nõ klassikalist teleaadet või näiteks nutitelekast mõnda internetipõhist teenust (Netflix, järelvaatamised jne). Seega võib eeldada, et ka telekavaatamise statistika on osaliselt interneti poole kaldu. Kõige populaarsemaks oli Ühendkuningriigi laste seas YouTube'i vaatamine. Pooled vastanutest (kokku küsitleti üle 2000 last) vaatavad YouTube'i iga päev ning pea kõik vastajad kasutavad teenust vähemasti aeg-ajalt.

Nutiseadmed ja internet on meie laste eludes igapäevane osa ning nagu mistahes muus eluvaldkonnas, tuleb ka nutiseadmete ja interneti kasutamise osas rääkida ka turvalisusest. Õpetame lapsele varakult, et võõraste inimestega ei tohi kaasa minna, koduks tuleb lukku keerata ning palavat pliiti ei tohi näpuga puutada. Mida aga õpetame lastele nutiseadmete ja interneti kasutamise kohta?

## LAINED MÕJUVAD AJULE HALVASTI

2014. aasta uuringus palusime lastel (6-14-aastased) rääkida oma sõnadega, mida tähendab nende jaoks nutiseadmete turvaline kasutamine. Saadud vastused peegeldavad üsna hästi seda, mida ja kuidas lapsevanemad või õpetajad on neile rääkinud.

Paljuski mainiti erinevaid aspekte, mis näitavad, et mingil määral on lapsed nutiseadmete kasutamisel hirmutatud. Kui teed midagi valesti, siis võib midagi halba juhtuda või siis aspekte, kus nutiseade ise on ohtlik - see on paha silmadele, võib plahvatada jne. Samuti mainiti jälitamist, küberkiusamist ning ohtu kaotada raha.

Toon välja mõned väited, mis on mõtlemapanevad, kuid mis kindlasti ei tähenda, et kõik lapsed nii mõtleksid.

## Nutiseadmete kasutamisel võib midagi halba juhtuda:

- > Ameerika salateenistus kuulab pealt ja teeb pilti;
- > ei tohi midagi peale mängude teha, muidu võib katki minna;
- > Internetis on kahtlased ja veidrased inimesed;
- > mingi halb asi võib tulla, kui sa mängu alla laed;
- > keegi võib sind ähvardada;
- > kui kellelegi ütled oma paroolid, siis on pahasti;
- > häkitakse palju sisse;
- > vastad võõrale kõnele ja läheb 5 eurot.



## Nutiseadmete kasutamine on kahjulik:

- > lained mõjuvad halvasti ajule;
- > postitused ja mängud tekitavad sõltuvust;
- > rikub silmi.

## Seadmega võib midagi juhtuda:

- > koolikotti võidakse lüüa jalaga ja seal sees olev arvuti võib katki minna;
- > laadija võib seest poolt katki minna, aku kuumeneb üle, ekraan võib katki minna;
- > telefonile ei vett minna;
- > ülekoormusega võivad mõned telefonid plahvatada;
- > võivad lõhkeda, nende peale ei tohi asju panna.



Sealjuures vaid 4 last 10st tajus selget riski, et nad ise võivad millegi ohtlikuga kokku puutuda. Ülejäänud kas ei tea midagi kaasneda võivatest ohtudest või ei oska neid kuidagi enda käitumisega seostada ja tunnevad end üsna turvaliselt. Seega näeme, et kuigi ohtusid kirjeldatakse üsna hirmsate, tõsistena, siis reaalselt nutiseadmeid kasutades lapsed nende ohtude peale olulisel määral ei mõtle. Loogiline oleks eeldada, et need lapsed, kes tajuvad riski ja arvavad, et nendega võib ka midagi nutiseadmete kasutamisel juhtuda, teevad rohkem oma nutiseadmete kaitsmiseks, kui need, kes teavad küll, mis ohud neid ümbritsevad, kuid ei arva, et need teda tabada võiks. Kõrget riski tajuvad kasutajad peaks enam kontrollima oma tegemisi ja toiminguid. Tulemused näitasid aga, et väga olulist vahet neil kahel kasutajasegmendil ei ole.

Seega on oluline riskide hindamise oskuste parandamine. Ei piisa hirmutamisest või keeldudest, kui laps ei saa aru, et need probleemid võivad puudutada ka teda ennast või tema perekonda. Seda eriti juhul, kui näiteks laps ja lapsevanem kasutavad sama nutiseadet - näiteks tahvelarvutit.

Ligi 80% lastest küsiks nutiseadmete ohutu ja turvalise kasutamise kohta nõu oma pereliikmetelt - vanematelt, õelt-vennalt. Seega on perering just see koht, kus omavahel rääkida.

Mida rohkem oleme lastele kübermaailmas kaaslaseks, seda rohkem saame ka nende tähelepanu juhtida võimalikele ohtudele ja riskidele. Eesmärk ei ole lapsi käskida, keelata ja hirmutada, vaid õpetada neid riske hindama ning vastavalt riskidele ka käituma.

Kas Sinu laps on sinu käest midagi nutiseadmete turvalisusega seoses küsinud? Kui ei ole, kuid samas kasutab ta internetti ja nutiseadmeid igapäevaselt, siis on üsna ebatõenäoline, et laps ei ole millegi riskantsuga kokku puutunud, ning sellisel juhul tasuks teema kindlasti juba ise tõstatada. Palu lapsel ühel õhtul näidata, mida ta näiteks Minecraftis ehitab, kuidas seal sõpradega suhtleb või kuidas ta YouTube'is endale meeldivaid asju otsib või leiab. Nii on lihtsam vestlust alustada.

Allikas: 26.01.2016 Guardian "Children spending more time online than watching TV for the first time" <http://www.theguardian.com/media/2016/jan/26/children-time-online-watching-tv>

Allikas: Nutiseadmete kasutajate turvateadlikkuse ja turvalise käitumise esinduslik uuring valmis 2014. aasta detsembris Riigi Infosüsteemi Ameti ja Vaata Maailma sihtasutuse tellimusel EL struktuurifondide programmist „Infoühiskonna teadlikkuse tõstmine“ Euroopa Regionaalarengu Fondi rahastusel. Uuringu viis läbi TNS Emor.

### Loe lisaks:

Interneti ja digivahendite turvalisest kasutamisest:  
[www.targaltinternetis.ee](http://www.targaltinternetis.ee)

Üldised nutiturvalisuse soovitused:  
Nutikaitse 2017 projekt  
[www.nutikaitse.ee](http://www.nutikaitse.ee)



# Interneti ohutuse alased digipädevused – kelle mure?

*Birgy Lorenz*


*Tallinna Ülikool, Digitehnoloogiaste instituut,  
Digiturbe labor*

**Eestis on mitmeid dokumente, mis mõjutavad seda, millised peaksid olema koolist saadavad digiturvalisust puudutavad oskused ja teadmised, ning kes selle eest vastutab. Samas lähemal uurimisel selgub, et paberil kirja pandu sisaldab valdkondi, mille eest keegi ei vastuta, samuti leiab teemasid, millest üldse ei räägitagi, aga mõjutavad väga oluliselt inimese edasist elu.**

Näiteks meie 2012. aastal ellu kutsutud ja mitmel korral muudetud Riiklik Õppekava mainib põhikooli osas, et üldine läbiv teema on „kriitiline mõtlemine ja allikate analüüs ning uurimine“ ja „autorikaitse teemad“. Seda mainivad nii **keel ja kirjandus, sotsiaalsed, kunst, informaatika**; gümnaasiumi osas lisanduvad veel **vene keel emakeelena, matemaatika, uurimustöö alused, üldine osa ja läbivad teemad**. Lisaks mainitakse **loodusainetes** elukeskkonna jätkusuutlikkust ja säästvat arengut tehnoloogiamailmas; **keel ja kirjandus** võtab rolli privaatsuse ja avatuse selgitamisel ja **informaatika** virtuaalse identiteedi kaitsel ja parooli osas kui ka väärast tehnikakasutusest tulenevate ohtude väljaselgitamises ja nende vältimises. Gümnaasiumi osas lubab **keel ja kirjandus** tegeleda ka

sotsiaalse manipulatsiooni mõistmise oskuste tugevdamisega ning **sotsiaalsed** panustada IKT mõju hindamisega elule ja arengutrendidele globaalses maailmas. See, mida mainitakse, on väga üldine ja puudutab ainult 2-3 vajalikku teemat. Sellest ei piisa edukaks digikodanikuks kasvamisel.

Õpetajatele ja õpilastele soovitusliku juhendina on HITSA aluseks võtnud ka ISTE standardid, millest saame teada, et õpetaja üheks pädevuseks on osata õpilastel aidata lahendada tegeliku maailma probleeme kasutades IT vahendeid. Enamus e-ohutuse alaseid tegevusi on üles loetletud neljandas, digitaalset kodanikku puudutavas peatükis: õpetaja propageerib turvalist, legaalselt ja eetilist info- ja tehnikakasutust; valib õppetöö läbiviimiseks sobivad eakohased



**Kui vaatame täna tegelikkust, siis mitmetes koolides ei tegele antud teemadega keegi, mõnes koolis on see kõik lükatud informaatika õpetaja mureks, kes kahe kursusega kogu 12-aastase õppetsükli vältel tulekahju kustutab, või siis tegeletakse asjaga kampaania korras ainult turvalise Interneti päeval**

vahendid; tunneb digitaalse maailma etiketti ja omab kultuurilist arusaama maailmast. Praegu on valmimas sarnane standard ka õpilastele, kus on kirjas ingliskeelse ISTE järgi oskused, mis näitavad oskuslikku ja vastutustundlikku tehnikakasutust, kui ka oskust probleemse arvutisüsteemi ja programmiga hakkama saamist. Seda on jällegi vähe, et tegelikkuses tänapäeva maailmas turvaliselt hakkama saada. Ei tahaks ju keegi, et meie programmeerimishuvilised noored saaksid vastu päid ja jalgu luues ebaturvalisi aplikatsioone või tekitades andmelekkeid, sest nendele ei ole kunagi õpetatud, et see võiks olla üks võtmeküsimusi digimaailma arendamisel.

Kui vaatame täna tegelikkust, siis mitmetes koolides ei tegele antud teemadega keegi, mõnes koolis on see kõik lükatud informaatika õpetaja mureks, kes kahe kursusega kogu 12-aastase õppetsükli vältel tulekahju kustutab, või siis tegeletakse asjaga kampaania korras ainult turvalise Interneti päeval. Selline näiline, läbi fännide asjaga tegelemine on meid toonud küll siia, kuid ei vii meid kahjuks edasi.



Kuna ISTE standard on üsna üldine, siis Eestis seotakse standard ära ka DIGICOMP-i EU pädevuste soovitus- tega, mille alusel hakatakse Euroopa Liidus riike omavahel võrdlema. Andmete saamiseks on planeerimisel ka riiklik tasemetöö-uuring, millest peaks selguma tänane seis ja vajadus õppekava uuendamiseks digipäde- vuste osas. Fakt on aga see, et loodav dokument, nagu ka EU soovitused, seavad digiturvalisuse üheks viieks põhivaldkonnaks informatsiooni haldamise, suhtlemise, sisuloome ja probleemilahendamise kõrval. Eesti kodanikult eeldatakse seega **oskuseid oma seadmete teadliku haldamise osas** (paroolidest ja anti-viiruse kasutamisest seadmete uuendamise, rünnaku puhul oskusliku käitumise ja enkrüptimiseni välja); **andmete ja identiteedi halduse osas** (oskus mõista, mida jagada ja mida mitte, privaatsuse kaitsmise alased oskused ja ka mõistmine, kuidas peaks olema korraldatud andmete turvaline hoiustamine kui ka töötlemine); **tervise hoidmises** (küberkiusamise vastu võitlemine, ergonoomika ja balansseerimine interneti ja pärismaa- ilma vahel) ja **keskkonna hoidmises** (energiasäästmisest tehnoloogia mõju keskkonnale hindamise oskuseni).

### Rohkem infot leiab

<http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=6359>.

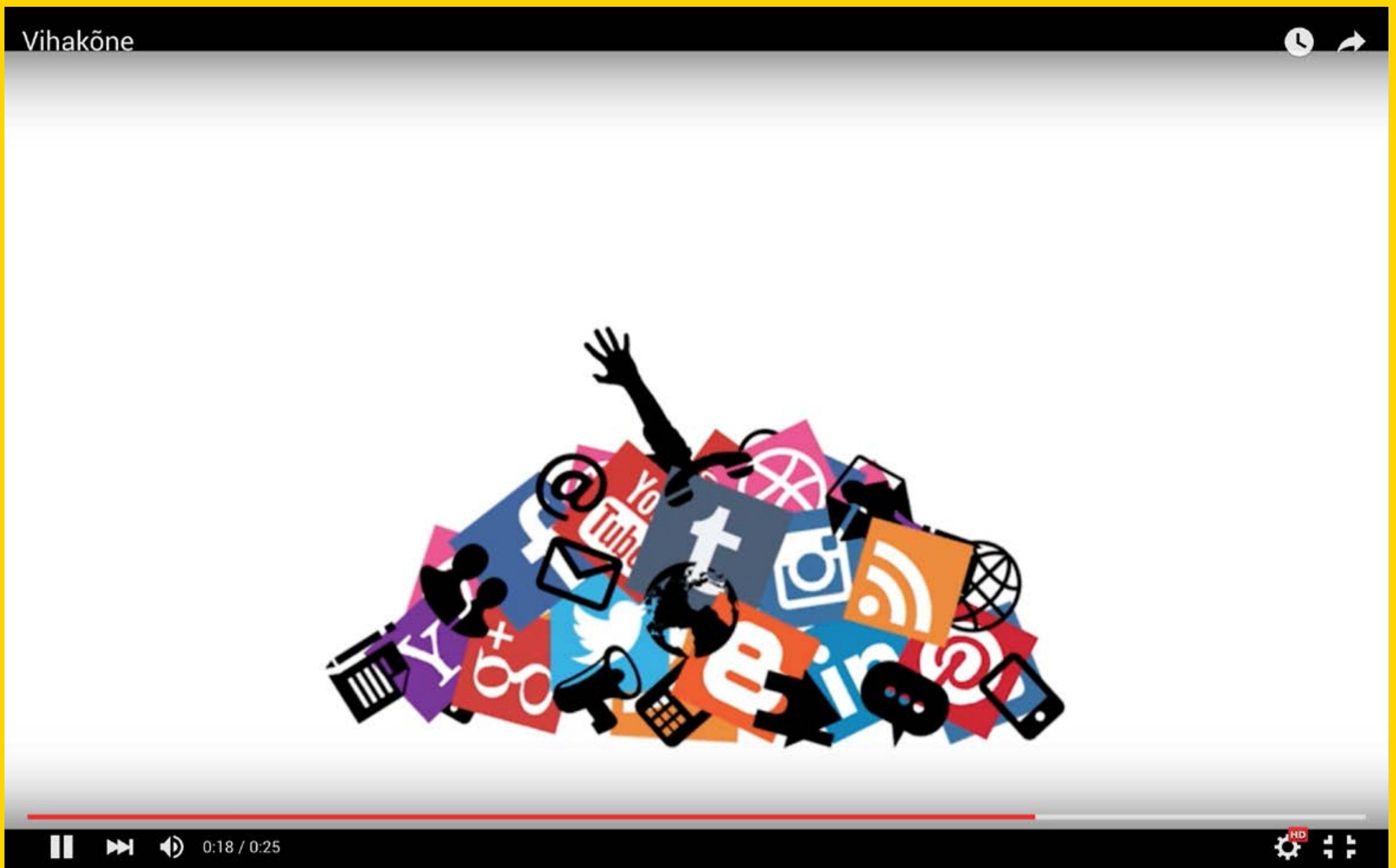
See kõik võib olla natuke ehmatav, sest Eestis on senini tegeletud teemaga üsna üldiselt ja pigem rõhuasetusega, et lapsed ei teeks oma töödes plagiaati ja hindaks teiste loodut ning ülejäänud teemad on jäänud pigem „paremaid aegu ootama“, kui õppekava ei oleks muude teemade osas nii ülepaisutatud. Kuid tegelikkuses on haridussüsteemile ootuseid veelgi. Näiteks Küberjulgeoleku strateegia 2014-2017, mis on kõikide ministriumide ülene, toob välja, et meie kodanikud ei tule edukalt toime nii küberkuritegevuse korral kui ka tuleviku julgeoleku ohtude korral (tavainimest puudutavana peetakse väga oluliseks võimalikku sotsiaalset manipulatsiooni ja ka põhivabaduste piiramist).

Seega digiturvalisuse osas on koolidel üsna suur tee veel minna. Esimese sammuna tuleks tunnistada, et meil puudub koolis selge arusaam, mida valdkond endast kujutab ja et see tuleb meil selgeks teha. Valmis lahendusi ei ole, sest iga kool on eriline – kes on asjaga tegelenud enam, kes vähem, kes on alles eituse faasis. Teiseks oleks vaja kujundada digiturvalisuse valdkonna suhtes positiivne meelestatus, et see on iga meie kooli töötaja vastustus ja mure. Kolmandaks asuda katsetama, luua reeglistikud ja rutiinid.

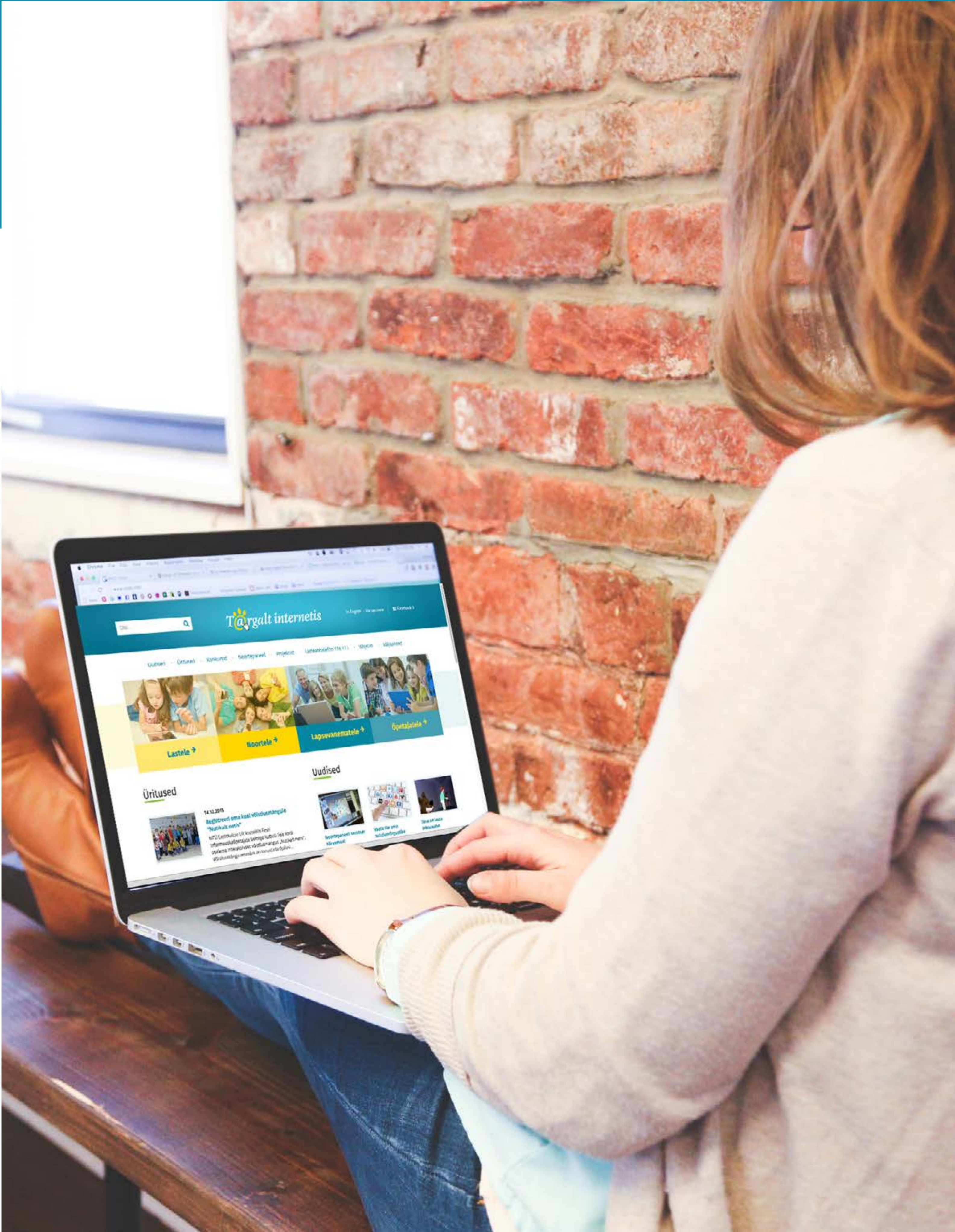
**Viimaks omandada kõrgeim aste: olla teistele eeskujuks, eksperdiks ja nõuandjaks, kes samal ajal ei unusta fakti, et muutuv maailmas muutuvad digimaailma turvalisust puudutavad tegevused pea iga aasta. See ei ole asi, mis kunagi valmis saab, et me saaksime panna linnukese „tehtud!“. Selles osas on ta nagu Ülemiste Vanakese pidev ähvardus, et kui linn valmis saab, siis tuleb ka uputus.**

**EDUKAT E-OHUTUSE ALAST NUPUTAMIST SOOVIDES!**

# Vaata turvalise interneti päeva videot!



## Vihakõne



# Tärgalt internetis

[Lastele](#) → 
 [Noortele](#) → 
 [Lapsevanematele](#) → 
 [Õpetajatele](#) →

## Uudised

- 

14.12.2019  
**Registreeri oma koal võitlusnappide "Näidake meile!"**  
 14.12.2019 Registreeri oma koal võitlusnappide "Näidake meile!"  
 14.12.2019 Registreeri oma koal võitlusnappide "Näidake meile!"  
 14.12.2019 Registreeri oma koal võitlusnappide "Näidake meile!"
- 

14.12.2019 Registreeri oma koal võitlusnappide "Näidake meile!"
- 

14.12.2019 Registreeri oma koal võitlusnappide "Näidake meile!"
- 

14.12.2019 Registreeri oma koal võitlusnappide "Näidake meile!"

# PROJEKTIL TARGALT INTERNETIS ON UUENENUD VEEBILEHT

**Projekt Targalt internetis alustas 2010.aasta septembris ning sama aasta detsembris avati veebileht [www.targaltinternetis.ee](http://www.targaltinternetis.ee). Veebilehe ülesanne on anda informatsiooni projekti tegevustest ning teha kättesaadavaks lastele, noortele, õpetajatele, lapsevanematele ja teistele temaatikast huvitatutele projekti raames loodud teabe- ja õppematerjalid.**

Veebilehte on aastate jooksul külastatud 234 194 korral 133 227 kasutaja poolt. Need arvud näitavad, et veebileht on jõudnud sihtgruppideni ning kasutajad on leidnud sealt enda jaoks huvipakkuvat teavet ja kasulikke materjale. Veebileht on ka rahvusvaheliselt tuntud, seda näitavad külastused pea sajast riigist üle maailma.

Viis aastat on pikk periood ning kaasa toonud muutusi nii digitaalse maailma tehnilises arengus kui ka interneti kasutajate huvides ja eelistustes. Sellest tuleneski vajadus uuendada juba hästi

sissetöötatud veebileht, et vastata enam meie kasutajate ootustele ja vajadustele.

Veebilehe uuendamisel kaasasime kohe alguses meie peamiste sihtrühmade – lapsed, noored, õpetajad, lapsevanemad esindajad, et saada nende arvamus, milline võiks olla uue veebilehe kujundus ja sisu.

Projektimeeskonna soov oli luua eraldi lehed lastele ja noortele, ning seetõttu oli väga oluline, et lapsed ja noored väljendaksid oma arvamusid ja teeksid ettepanekuid, millised on

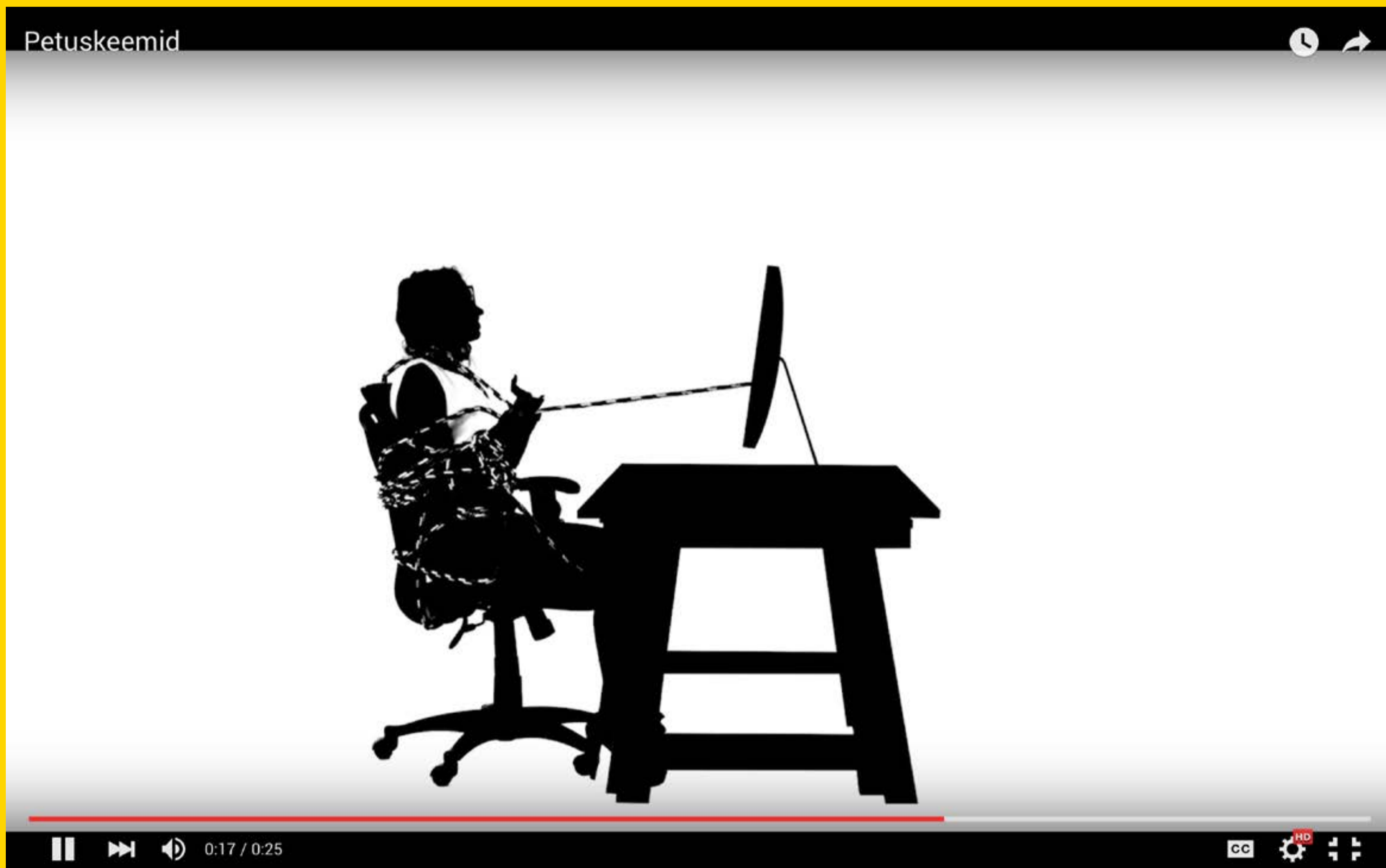
nende jaoks parimad lahendused kujunduse osas ja millistel teemadel ning millisena esitatult nad sooviksid veebilehelt teavet saada. Veebilehe laste ja noorte lehe valmimisse panustasid aktiivselt projekti noorte-paneeli liikmed ning samuti suur tänu Harku-Järve Kooli 3-6-ndate klasside õpilastele, kelle arvamused õpetaja Heily Epro vahedusel meieni jõudsid.

Õpetajatele ja lapsevanematele mõeldud õppe- ja infomaterjalide uuendamise osas toimusid konsultatsioonid projekti koolitajatega, kes andsid sisuka panuse sihtrühmadele pakutavate teemalehtede väljatöötamise.

Veebilehe uue versiooni arendajaks valiti pakkumiskonkursil parimaks osutunud ADM Interactive, kellega edukas koostöös veebilehe uus versioon valmis.

Tutvu projekti  
uuenenud veebilehega  
[www.targaltinternetis.ee](http://www.targaltinternetis.ee)  
ja vaata lastelehte  
<http://laps.targaltinternetis.ee/>  
ning noortelehte  
<http://noor.targaltinternetis.ee/>.

# Vaata turvalise interneti päeva videot!



## Petuskeemid

# Kuidas tagada enda kasutatavate tehnoloogiate ja teenuste turvalisust?

*Birgy Lorenz*

*Tallinna Ülikool, Digitehnoloogiate instituut,  
Digiturbe labor*





**Põnevad trendid tehnoloogias ja turvalisuses muudavad maailma. Oleme tehnoloogia arengus jõudnud samasse ajajärku, kui oli 1950. aastatel autotööstus – funktsionaalsus on olemas, aga kasutaja-mugavusega tuleb veel vaeva näha. Milles me ei ole aga 50ndates aastates, on masslevik ehk siis tänapäeval on igaühe taskus, kotis või töökohas üks või mitu tarka vidinat.**

Targad on ka meie autod, telefonid, lisandseadmed nt. südamestimulaator, mitmed seadmed meie kodudes, Jaapanis WCd jpm. Ühelt poolt on see väga põnev ja innustav - mida kõike me nendega nüüd ära teha ei saa ja teisalt on see päris hirmutav, kui selgub, et meie pole ainsad nende tehnoloogiate võimaluste kasutajad, vaid osa infot, mis on kogutud meie seadme kasutamise käigus, läheb kuhugi interneti musta auku ja kolmandatele osapooltele meie harjumuste uurimiseks.

### **PROBLEEM: KES KOGUB MINU KOHTA SALAJAST VÕI AVALIKKU INFOT JA MILLEKS?**

Täiskasvanuna tundub ohtlik ja kummastav, et miks peaks saama minu autol satelliitlevi kasutades uksi avada (näiteks rendifirma USAs avab ukсед kui oled oma

võtmed pagasnikusse unustanud ja ukse kinni löönud), kuid samal ajal tundub see brilliantse võimalusena, sest inimesed ju ikka unustavad oma võtmeid autosse. Rõõmustavad aga ka pätid ja kaabakad, sest pole olnud paremat võimalust kaaperdada kellegi sõiduvahend või ka sotsiaalmeedia vahendusel lihtsalt sirvida galeriid kellegi kodust ja uutest ostudest ja teada saada, mis ajal teda objektile pole (spordiappid, mis postitavad marsruuti koos kellaaegadega). Oleme ju lugenud viimastel aegadel ka artikleid, kus nii mõnigi on kaotanud töö, kuna on haige asemel veetnud lõbusalt aega SPAs ja vastava info sotsiaalmeediasse ülesse laadinud või et laenuandjad teevad laenuotsuseid analüüsides inimese sotsiaalmeedia käitumist.

## **PROBLEEM: SÕBRAD JA VANEMAD EI MÕISTA ALATI NENDE LÄHEDASTE VAJADUST PRIVAATSUSELE**

Me ise oleme täielikult vastutavad enda käitumise eest, kuid tahtmatult võime sellega luua väljakutseid ka teistele. Minnes mõnele üritusele pildistama, võivad meie piltidele sattuda ka teised, sama toimib ka märgendamise (tagging) kohta. Luba loomulikult keegi ei küsi, sest see tundub ajaraiskamisena. Lohutame end sellega, et kui neile pilt ei meeldi ja nad seda ütlevad, siis võtame selle maha. Kuid me ei mõtle sellele, et mis on internetis liikvel, seda täielikult maha võtta ei saa. Veel hullem olukord on aga noorte lapsevanematega, kes täiesti süüdimatult riputavad terve oma laste elu, alustades ultraheli pildist, internetti üles. Üsna ohjeldamatu postitamine toimub enamasti esimesel kahel aastal – siis tuleb üles panna iga vankrisõit tänaval või õhtune magamajäämise laul. Ei erine selles osas ei noored isad ega emad. Mõne aja möödudes tuleb enam naljakaid ja äpardusi jäädvustavaid pilte, kus lastel ei tule kõik veel välja.

**Selleks ajaks, kui laps jõuab kooli, on tal internetis üsna võimas ajalugu üleval, mis annab head alused sattumaks puberteedieas või isegi varem kiusamise või narrimise ohvriks. Peale selle on arvatavasti mõned paljamad pildid jõudnud ka pedofiilide pildipankadesse.**

## **PROBLEEM: MIDA KÕIKE EI SAA PRINTIDA, SH. RELVI TERRORISTIDELE.**

Põnev asi, mis maailmas on juhtunud, on 3D printimise tehnoloogia võidukäik, mis aitab luua paremaid tooteid ja mõnes mõttes loob ka uusi tööstusharusid nagu organite, majade ja muude esemete printimine. Tooted luuakse kohapeal ja vastavalt kliendi soovile, ei pea ootama kui need asjad kuskil kaugel tehases valmivad. Printimine on hitiks saanud ka sõjatööstuses ja lennunduses. Kui tavakasutajat saab tõesti piirata sellega, et kui ta püüab relva printida, siis printer keeldub sellest või saadab teate KAPOle, et seda on üritatud, siis tegelikult võetakse üsna kergesti kood koost häkkerite poolt, kes teevad

loodud võimalustega ikkagi seda, mida nad soovivad.

Mis oleks lahenduseks? Osta vana auto, keelduda nutiajastust, meditsiini arengutele vastu seista, mitte minna peole, mitte teha endale võrgustikus konto, minna vanematega lihtsalt tülli ja majast enam mitte väljuda, reisimisest rääkimata. Need on kindlasti mõned võimalikud lahendused, aga neid on veel. Esiteks ei saa ärimaailm toimida ilma inimesteta ja see annab meile tegelikkuses hääle ja võimaluse oma teenusepakujatele ja ka tootjatele teada anda meie soovidest ja vajadustest, näiteks et meile on oluline privaatsus ja turvalisus. Samamoodi on meil inimestena õigus luua ja algatada seadusloomet, mille alusel ei või teatud andmeid lihtsalt koguda ega kasutada. On see siis nõue meie andmeside teenusepakujale tagada laste käes olevates vahendites filtreeritud internetti või midagi muud, mis on meile oluline. Ennustan tulevikku, et üha enam hakatakse maailmas tegelema eetilise digikasutuse ja eetiliste teenuste pakkumisega. Üha enam aitab internet ja avalikkus realiseerida inimeste tegelikke soovide ehk siis keskkonnad muutuvad, arenevad, kuna ka infoühiskond areneb.

**Seega soovituseks kaasaegses maailmas hakkama saamiseks on nautida kõike, mida pakutakse, aga teha seda mõistlikult.**

Kui osta kasutusse seade, tarbida teenuseid, jagada endast maailmale infot, siis teha seda teadlikult, ning selgitada välja, mis on toote/teenuse vourused ja varjuküljed ning mitte lasta ennast peibutada näiteks helkivast valgest kaanest või ümmargusest logost. Kui kahtled, siis ei ole midagi katki ka selles, kui lihtsalt Segwayga rullitamise asemel jalutada või päriselus sõpradega kohtuda ja küsida „kuidas sul läheb?“ Kuid fakt on see, et ka seisev nutividin vajab tänapäeval uuendamist ja kaasajastamist, sest muidu võtab selle aukliku seadme kasutusse keegi teine, kellel kindlasti ei ole sellega häid kavatsusi.

**Mõistliku vidinakasutust soovides!**

# *Nuhkimisest....juriidiliselt*

*Anu Baum,*

*PPA, TLÜ õigusteaduse magistrant*



*Sain teada, et mehel võib olla armuke ja sain teada ka selle isiku nime. Mehel on facebooki konto, mida peamiselt suhtlemiseks kasutatakse. Facebook on installitud mehe nutitelefoni ja sama kontoga facebook on vaikimisi käimas ka meie ühises lauaarvutis, parool on salvestatud. Hiljuti, kui mees läks eraldi ruumi telefoniga oletatavasti oma armukese-ga facebooki kaudu suhtlema, vaatasin nende vestlust lauaarvutist pealt.*

**Selliseid ja sarnaseid postitusi on viimasel ajal aina rohkem näha erinevates portaalides ja foorumites. Muidugi on mõistetav selle poole mure, kes kahtlustab, et teda petetakse, et kõik ei ole nn korras. Uudishimu on suur, ning hing ei anna rahu – seitsmes meel ütleb, et midagi on valesti, aga fakte oleks vaja.**

Täpselt sama moodi on mõistetav lapsevanema mure oma lapse pärast – me ju näeme, et meie lapsed on kuskil online maailmas, aga mida nad seal teevad ning kes on nende sõbrad – seda me tihti ei tea. Teismeline ei taha ka ise rääkida, tal on oma privaatsus ning ealistest isaärasustest lähtuvalt on seda parem, mida vähem vanemad teavad – nad ei tea nii ehk nii midagi.

Eesti Vabariigi Põhiseaduse II peatükis on sätestatud isikute põhiõigused ja – vabadused. Põhiseaduses §26 sätestab, et igaühel on õigus perekonna- ja eraelu puutumatusel ning §43, et: „Igaühel on õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele. Erandeid võib kohtu loal teha kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks seadusega sätestatud juhtudel ja korras.“

Nagu me näeme, kaitseb Põhiseaduse §43 isikute sõnumisaladust, ning samas on loetletud ka erandid, mille puhul on lubatud sõnumisaladust rikkuda. Kui me nüüd uuesti loeme §43 sätestatud erandeid, siis me ei näe siin eranditena a`la saamaks teada, kellega teine pool suhtleb ja millest nad omavahel räägivad. Samuti ei ole erandiks Põhiseaduse mõttes vanemliku kontrolli teostamise vajadus kui õigustus sõnumisaladuse rikkumiseks.

Selleks, et kaitsta isikute eraelu ning sõnumisaladust tõhusamalt, on riik näinud ette kriminaalõiguslikud kaitsemeetmed. Nii on karistus- seadustikus sätestatud süütegudena ning kriminaalkorras karistatavate tegudena nii eriviisiline jälitustegevus, eesmärgiga koguda andmeid, kui ka sõnumisaladuse rikkumine.

**Karistusseadustiku §137 sätestab kriminaalkorras karistava teona eraviisilise jälitustegevuse isiku poolt, kellel puudub selleks seaduslik õigus, eesmärgiga koguda tema kohta andmeid. Inimeste jälgimine hõlmab tema korduvat või pikemaajalist varjatud visuaalset vaatlemist kas vahetult või tehniliste vahendite abil, sõnumite salajast pealtkuulamist või läbivaatamist, sõltumata sõnumite edastamise, läbivaatamise või pealtkuulamise viisist ning asjade või inimeste kohta andmeid sisaldavate andmekogude salajast läbivaatamist.**

Antud näite puhul, so eraisiku FB kontol toimuva sõnumivahetuse jälgimine, on meil tegemist tehnilise vahendi abil edastatavate sõnumite läbivaatamise või pealtkuulamisega, olenevalt siis sellest, kas sõnumeid vaadatakse reaajas või loetakse neid hiljem.

Tuleb kindlasti märkida, et eraviisilise jälitustegevuse puhul on oluliseks koosseisuliseks tunnuseks andmete kogumise eesmärk. Andmeteks loetakse isikuandmeid, mis ise loomustavad inimese perekonda, päritolu, aga ka sidemeid ning tema varalisi kohustusi. Seega – tahtes teada, kellega meie teinepool suhtleb, on tegemist andmetega, mis puudutavad jälitatava (või nuhitava, nagu seda pigem igapäevakeeles nimetame) sidemeid. Oluline on pöörata ka tähelepanu asjaolule, et koosseisulise tunnuseks on oluline, et andmeid kogutaks nende hilisema kasutamise/ töötlemise eesmärgil.

Mis omakorda võib tekitada küsimuse, et kui näitena toodud juhtumi puhul küll jälgitakse teisepoole suhtlust, kuid neid andmeid ei salvestata või koguta muul moel, ning otseselt

ei ole eesmärgiks neid kusagil hiljem kasutada, siis pole tegemist era-  
viisilise jälitustegevusega.

Põhimõtteliselt on selline lähenemine õige, kuid – nagu me juba ka eelpool mainisime, on lisaks veel eraldi kaitstud sõnumisaladus, mille rikkumine on kriminaalkorras karistatav Karistus-  
seadustiku §156 järgi.

**Kuigi sõnumisaladuse rikkumine, so KarS §156, on kergem süütegu, kui eelmainitud ebaseaduslik jälitustegevus - sõnumisaladuse rikkumine on karistatav rahalise karistusega, samas kui ebaseaduslik jälitustegevuse maksimaalne karistusmäär on kuni kolme-aastane vangitus, on siiski tegemist kriminaalkorras karistavata teoga.**

Sõnumisaladuse rikkumise puhul on oluline pöörata eraldi rõhku asjaolule, kas sõnumi saatja on pidanud sõnumit kaitsmisväärseks. Kui tuua näide nn tavapostist, siis lahtiselt saadetud postkaardi puhul ei saa me rääkida sõnumisaladuse rikkumisest ka juhul, kui seda loevad kolmandad isikud, sest sõnumi saatja ei ole pidanud seda vajalikuks varjata mingilgi moel sõnumi sisu.

Mis puudutab elektroonset kirjava-  
hetus ja sõnumite vahetust, siis meil tuleks eeldada, et isik ei ole teinud postitust avalikus kõigile ligipääsetavas interneti keskkonnas ja ruumis (nt Delfi kommentaariruum, avalik foorum), vaid on adresseerinud selle ühele konkreetsele isikule, ning see isik, kes sõnumi sai, ei ole pärast sõnumi saamist avaldanud seda kolmandatele isikutele, siis tuleb lugeda selline sõnum kaitstuks sõnumisaladusega.

Samas tekib meil loomulikult küsimus, et millisel juhul lugeda, et ka sõnumi saaja kaitseb sõnumit, soovides, et sõnum jääks saladuseks. Kui kasutame taas tavakirja ja postkaardi loogikat, siis ilmselt arvutiekraanile lahtiselt jäetud e-kiri/sõnum, ei ole



enam sõnumisaladusega kaitstud, täpselt samuti nagu laule lahtiselt jäetud postkaart või tavakiri ei ole enam sõnumikaitse objektiks. Samuti ei saa sõnumisaladuse rikkumisena käsitleda olukorda, kus kolmas isik näeb sõnumit juhuslikult nt möödudes arvutist hetkel, kui sõnumisaaja (või kirjutaja) parajasti sõnumit/e-kirja loeb või kirjutab. Seda peamiselt seetõttu, et isikult, kes juhuslikult sellisel hetkel arvuti juurde satub, puudub tahtlus seda sõnumit näha.

Asjad lähevad keerulisemaks juhtumite puhul, kui sõnum nõ ei vedele meie vaateväljas ning me peaksime tegema mingeid tegevusi selleks, et selle sõnumini pääseda. Tihti kohtab elus juhtumeid, kus oma teo õigustuseks kellegi e-kirjade/sõnumite lugemiseks, tuuakse välja, et teati parooli nendele ligipääsemiseks. Kui tegemise e-kirja aadressi mõlemad pooled igapäevaselt jagavad ja/või on teine pool just selleks paroolid andnud, et tema kirju loetaks, siis võime ilmselt eeldada, et konto omanik ei pea vajalikuks oma e-kirju/sõnumeid teise isiku eest kaitsta, võiks isegi öelda, et ta on andnud teisele isikule volituse ja loa oma e-kirju lugeda.

**Küll aga ei saa sellist luba a priori lugeda olemasolevaks juhtumite puhul, kui nt ühiselt kasutatavas arvutis on paroolid salvestatud, kuid ei ole otsesõnu omavahelist kokkulepet ja/või luba teise kontol käimiseks. Sellisel juhul tuleks meil siiski lähtuda seisukohast, et e-kirjad/sõnumid on nende valdaja poolt kaitstud.**

Tuues võrdluse nn reaalse maailmaga – kui meie naaber jätab oma korteri võtmed mingil põhjusel meie juurde, ei anna see veel meile õigust minna naabri korterisse lihtsalt niisama huvi pärast kolama tema kappides ja isiklikes asjades. See, et arvutit kasutakse ühiselt, ei ole piisav argument – ka tavakirjad tulevad perekonna puhul tavaliselt ühte postkasti, kuid igaüks avab tema nimele tulnud ümbriku ikka ise, kui ei ole just kirja avamiseks luba saanud.

Foorumitest on tihtipeale näha ka postitusi, kus avaldatakse soovi saada informatsiooni selle kohta, kuidas saada rohkem informatsiooni mitmesuguste tehniliste vahendite kohta, mis võimaldavad salvestada teise isiku poolt arvutis tehtavat sh võimaldamaks salvestada erinevatele kontodele ligipääsu paroolle. Seda siis juhtudel, kui teine isik on pidanud vajalikuks kaitsta oma kontosid, ning pole nuhkija suureks meelehärmiks neid isegi arvutisse salvestanud.

**Oluline on alati enne sellise tehnilise ja/või tarkvaralise vahendi arvutisse paigaldamist pidada meeles, et lisaks eraelu ja sõnumisaladuse karistatavusele, on kriminaalkorras karistatav ka arvutisüsteemile ebaseaduslikult juurdepääsu hankimine kaitsevahendi kõrvaldamise või vältimise teel. Kuigi sõna „arvutisüsteem“ tekitab meis ehk mulje, et jutt käib tõesti millestki suurest a'la ettevõtte arvutipark koos serverite ning kõige sinna juurde kuuluvaga, siis arvutisüsteemiks kriminaalõiguse mõttes on laiem nõ tavamõttest, ning arvutisüsteemiks loetakse seadet või seadmete gruppi, millest vähemalt üks täidab automaatse andmetöötamise funktsiooni.**

Seega on arvutisüsteemideks kriminaalõiguslikus mõttes, mitte ainult arvutid ja laptopid, vaid mõiste on palju laiem, hõlmates ka nutitelefone, tahvelarvuteid, kaasaegseid mängukonsoole, nutiteleviisoreid, sõidukite pardakompuutreid jne ehk sisuliselt enamikku meid igapäevaselt ümbritsevatest elektroonilistest vahenditest.

Juhul, kui kasutatav tehniline seade on mitmete isikute ühiskasutuses ning sellises seadmes soovitakse nii enda kui teiste tegevusi salvestavaid vahendeid kasutada, tuleb sellest informeerida kõiki seadet kasutavaid isikuid. Argument, et seade on minu oma, ja ma teen sellega, mida ma tahan, ning paigaldan sellele, mida vajalikuks pean, ei ole piisav, kui see seade või tehniline lahendus on ohuks teiste kasutajate privaatsusele.

Kokkuvõtvalt – enne, kui uudishimu saab lõplikult võitu, tasub sügavalt järele mõelda, kas sellise tegevuse so teise isiku sõnumite lugemine, tema kontode ja/või e-kirjavahetuse kontrollimine ning keyloggerite ning

muude põnevate tehniliste vahendite kasutamine tehnilistest seadmetes, ilma isiku teadmata, on ikka väärt neid õiguslikke tagajärgi, mis sellise tegevusega kaasneda võivad. Rääkimata tagajärgedest, kuidas sellised tegevused mõjutavad inimeste vahelisi suhteid, seda siis nii paarisuhtes olevate isikute omavahelistest suhetes, kui ka lapse ja vanema usalduslikke suhte aspektist vaadatuna.

**Üldiselt, hoolimata infotehnoloogia võidukäigust ning kasutamise aktiivsusest, ei ole endiselt keelatud inimeste vaheline otsene verbaalne suhtlemine – proovi, tulemused võivad sind ennastki üllatada.**

# Ükski küsimus pole rumal või liiga tühi

*„Ei tea, kas see on õige koht kuhu pöörduda?“, „Mul on mure...“  
„Soovin kellegagi rääkida...“, „Ma ei tea, mida teha...“, „Kas te saate mind aidata...“*

*Mari-Liis Mänd*

*Projektijuht, Arstlik Perenõuandla OÜ*

*Lasteabitelefoni 116111*

Ükski küsimus pole liiga rumal või liiga tühine, et mitte lasteabitelefoni 116111 poole pöörduda. Lasteabitelefoni 116 111 on nõuandetelefon, kuhu võib helistada igaüks, kes soovib saada nõuannet lastega seotud teemadel või teatada abivajavast lapsest. Lasteabitelefoni eesmärgiks ongi aidata, kuulata, jagada nõuannet ja informatsiooni, vajadusel suunata küsija abisaamiseks edasi. Lasteabitelefoni on oodatud helistama nii lapsed ise, kui ka täiskasvanud, teemadel, mis on seotud lastega ja lapsi puudutavates küsimustes. Sekkumine ei ole kaebamine, helistamisega saab aidata.



***e liiga  
ine***



**Kiired arengud tänases elu-tempos panevad suured ootused nii lastele kui ka lapsevanematele. Ka lapsevanemad vajavad nõuannet, kuidas tänases kiiresti muutavas ühiskonnas olla hea lapsevanem. Kuidas olla toeks lapsele või noorele, kelle valikute võimalused on järjest avaramad ning kiiresti muutu- vad: interneti tuttavad suhtlus- portaalides, erinevad naudinguid pakuvad mõnuained, mitte- traditsioonilised intiimsuhted ja paljud teised näited.**

See eeldab ka vanematelt teadlik- kust, informeeritust, kasvamist koos lapsega. Ning kui ei suudeta omava- hel piisavalt suhelda, üksteist mõis- ta ning usaldada, on arusaamatused kerged tulema. Kui oma sisimas ei tahetagi teisele poolele haiget teha, võib oma soovide arusaadavaks tegemine olla keeruline, kui teine pool ei ole selleks valmis. Kuid vane- mad ei tohiks unustada, ükskõik kui keeruline olukord ka poleks, nemad on täiskasvanud ning peavad võtma vastutuse olukorra lahendamise osas.

Kui suhted lapsega kipuvad käest minema, võiksid vanemad mõtiskle- da, mis võib olla selle põhjuseks. Palju- nad teavad oma lapse tegemistest ja sõpradest tegelikult, millal viimati ise lapsega koos midagi tehti ja talle tõeliselt aega pühendati. Lapse või noorega tasub olla aus, rääkida talle enda tunnetest, rõõmudest ja hirmud- est. Ühtlasi tunda siirast huvi lapse tunnete ja mõtete vastu. Suhe on alati kahepoolne ning laps ootab vanemalt tuge ning turvatunnet. Kui talle on antud võimalus seda mõista, saavad ka omavahelised suhted loode- tavasti paremaks.

Vahel on lastel või noortel lihtsalt teadmatus, mida oleks kõige parem mingis olukorras teha. On näiteks tülli mindud, kas sõbra, kaaslase või vanemaga ning ei osata olukorda kuidagi lahendada. Tuntakse ennast juhtunu pärast halvasti, samas ei julgeta või ei osata ise situatsiooni kuidagi lahendada. Kellelki nõuannet küsida aga pole või ei tea, kuhu täpselt peaks helistama, teatama. Vahel pole soovi oma asjadest enda lähedaste- le rääkida. Tahetakse, et oleks keegi, keda ei tunne, aga kes oleks valmis kuulama, kaasamõtleva, vestleva,

aitama. Lasteabitelefoni nõustajaga olukorda arutades saab selgust, kuidas oleks kõige parem toimida, mida teha ning saada juurde ka enesekindlust, millest võib puudust olla. Mõnikord ehk polegi endal probleemi, vaid tahaks aidata hoopis sõpra või kedagi teist, kedagi, kes ise ei saa või ei oska abi küsida. Näiteks kiusamiste puhul, kas koolis, huviringis, internetis. Ka nügimine ja norimine on kiusamine ning kellelgi pole põhjust seda taluda. Samuti ignoreerimine ja tõrjumine. On suhteliselt levinud olukorrad, kus kõik nagu näevad ja teavad, et mingi kiusamine toimub, kuid ei julgeta sekkuda, kuna kardetakse iseenda pärast. Kardetakse eba-populaarsust ja et kiusamise ohvriks võidakse hoopis ise sattuda. Samas tuleb meeles pidada, et kiusamisest mitte teatamine on omamoodi sellele kaasaaitamine ning sellest rääkimine pole kunagi kaebamine. Kui oma koolis või lähikonnas pole usaldusväärset inimest, võib julgelt lasteabitelefoni poole pöörduda.

**Interneti tihe kasutamine on viinud palju suhtlemist internetti, mis annab juurde palju võimalusi, kuid millega võivad kaasneda ka ohud, millest tuleb olla teadlik.**

**Seepärast on hea, kui nii lapsed ja ka vanemad on teadlikud heast ja turvalisest interneti kasutamisest ning oskavad olla tähelepanelikud.**

**Et ei satuks isiklikku infot levitama kohtades või inimestele, kes seda võivad kuritarvitada, ja soovimatuid postitusi ja pilte jagama, mis võivad kahjustada ja häbistada. Et ei suheldaks isikutega, keda ei tunta ja kes võivad olla pahatahtlikud. Kui selliseid asju juhtub, ei tohiks lapsi oma probleemidega üksi jätta, sest need võivad ilma sekkumiseta põhjustada lastele palju valu ja hirmu.**

Projekti „Targalt internetis“ raames tähistatakse veebruaris turvalise interneti interneti päeva ning lasteabi-telefoni eestvedamisel on valmimas kolm uut videoklippi, millega soovitakse juhtida tähelepanu targale käitumisele internetis. Teemad on valitud ohtude põhjal, millega võidakse tihedamini netis kokku puutuda – vihakõne, petuskeemid, ahistamine. Teemad, mis võivad puudutada igapäev, kui ei olda piisavalt teadlikud. Klippe näidatakse nädala jooksul aktiivselt erinevates internetiportaalides nagu FB, Instagram, e-kool. Samuti kinodes enne filme suurtel erkaanidel ja reklaamtahvlitel, kaubanduskeskuste digiekraanidel. Bänneritena lisanduvad väliekraanidest bussiootepaviljonid ning valgusvitriinid, veebibännerid delfi.ee erinevates väljaannetes, postimehes.ee portaalis. Interneti oskusliku kasutamise kajastamiseks ilmuvad valdkonna spetsialistide teemaartiklid nii üleriigilistes ajalehtedes kui ka maakonna lehtedes, et sõnum saaks võimalikult laialdaselt kajastamist üle Eesti. Intervjuud meediakanalitele annavad lisavõimaluse tutvustada nii Targalt internetis projekti üldisemalt, kui ka turvalise interneti interneti päeva fookuses olevaid teemasid.



# ***Võta lasteabitelefoniiga ühendust:***

- > kiusamised,
- > suhete probleemid,
- > vägivald,
- > enesevigastamine,
- > arusaamatused laste ja vanemate vahel,
- > hooletusse jätmine,
- > väärkohtlemine,
- > raskused lapse kasvatamisel,
- > internetiga seotud küsimused või probleemid,
- > lastega abivajavad pered,
- > kodutu või kerjav laps

# ***Lasteabitelefoniiga saab ühendust võtta:***

- > telefon **116111** üle-Eestiliselt 24/7, helistamine on tasuta ja anonüümne
- > [www.lasteabi.ee](http://www.lasteabi.ee) online nõustamine „Küsi nõu“
- > e-post: [info@lasteabi.ee](mailto:info@lasteabi.ee)
- > nutiseadmest otsisõnaga „Lasteabi“
- > Skype: **Lasteabi\_116111**
- > FB: „Et ükski laps ei jääks abita kui ta seda vajab!“



[www.vihjeliin.ee](http://www.vihjeliin.ee) – teata internetis  
levivast laste seksuaalset ärakasutamist  
esitavast materjalist!

*Malle Hallimäe,*

*vihjeliini projektijuht, Lastekaitse Liit*

## **Internet pakub meile kõigile uusi ja kasulikke võimalusi, kuid kahjuks on enam kui kahe miljardi interneti kasutaja hulgas inimesi, kelle tegevus võrgus rikub laste õigusi ja on lastele ohtlik. Nii näiteks kasutatakse ülemaailmset arvutivõrku laste seksuaalset ärakasutamist esitava materjali hoiustamiseks ja levitamiseks.**

Vihjeliin on MTÜ Lastekaitse Liit poolt pakutav veebipõhine tasuta teenus [www.vihjeliin.ee](http://www.vihjeliin.ee), mis võimaldab internetikasutajal anda teavet sellest, kui ta märkab veebis keskkonda, mis sisaldab laste seksuaalset enesemääramisõigust rikkuvat materjali - Eesti Vabariigi seaduste kohaselt on keelatud sellise teose (pildi, video jne) valmistamine ja levitamine, mis kujutab nooremat kui kaheksateistaastast pornograafilises või nooremat kui neljateistaastast pornograafilises või erootilises situatsioonis. Vihjeliini töö eesmärk on kaasa aidata taoliste materjalide eemaldamisele internetist.

Laste seksuaalset ärakasutamist sisaldavad materjalid, nende levitamine, tarbimine ja tootmine rikub ohvriks langenud lapse õigusi, au, väarikust ja kehalist puutumatus. Sageli on internetis levitatava lapsi seksuaalses/erootilises kontekstis esitatava materjali eesmärk juhtida laste vastu ebatervet seksuaalset

huvi tundvaid inimesi ühendust võtma suletud kogukondadega, mille liikmed kasutavad laste seksuaalset enesemääramisõigust rikkuvaid materjale oma haiglasliku kire ja fantaasia rahuldamiseks. Seejuures esineb risk, et taoline käitumine võib jõuda fantaasiast reaalsusesse ja laste otsese füüsilise ärakasutamiseni. Vihjeliini laiemaks eesmärgiks on ennetada selliste kuritegude toimepanemist.

Teabe saab edastada anonüümselt ilma teavitaja isikuandmeid lisamata. Vihjeliinile tulnud teave käideldakse vastava koolituse saanud Lastekaitse Liidu töötaja poolt. Vihjeliin kontrollib vaid avalikel veebilehtedel olevat materjali. Isikute vahelises suhtlusvõrgustikus või sisselogimist eeldavas keskkonnas asuvat materjali ei kontrollita ning selline teave edastatakse politseile. Saadud teates sisalduv veebilehe aadress avatakse ja selle sisu hinnatakse vastavalt Eestis kehtivatele seadustele. Kui veebilehe sisu

on ebaseaduslik, siis edastatakse teave sellest Politsei- ja Piirivalveametile. Kui veebilehe haldaja asub väljaspool Eestit, siis edastatakse teave vastava riigi vihjeliinile (kui see riigis tegutseb) ja/või õiguskaitseasutustele.

Vihjeliin alustas tööd 2011. aasta veebruaris. Viie tegutsemise aasta jooksul on vihjeliin saanud 3741 teadet, millest 468 sisaldas teavet laste seksuaalset

ärakasutamist esitava materjali kohta.

Kuna internet ei tunne riigi piire ning ühes riigis loodud ja üles laetud materjal levib üle maailma, siis on laste seksuaalset enesemääramisõigusi rikkuvate materjalide internetist eemaldamiseks vajalik rahvusvaheline koostöö <https://www.youtube.com/watch?v=10JhnGLxXu4>

## Vaata videot!



*Alates 2011.aasta novembrist on Eesti vihjeliin rahvusvahelise võrgustiku INHOPE liige. INHOPE võrgustik asutati 1999.aastal, hetkel ühendab võrgustik 48 vihjeliini 42 riigist.*

*Vihjeliini tegevus on osa projekti „Targalt internetis – SIC EE III“ tegevusest, mida rahastab 50% ulatuses Euroopa Liidu programm Connecting Europe Facility (CEf)*

# Vaata turvalise interneti päeva videot!



## Ahistamine

# Vaata üle oma suhtlusvõrgustike kontode privaatsusseaded

*Kerli Kuusk*

Projekti Targalt internetis  
teavitustöö koordinaator

Sotsiaalsuhtlusvõrgustikud ja osalemine interneti kogukonnas on tänapäeva noortele ja täiskasvanutele väga oluline. Inimesed kasutavad erinevaid suhtlusvõrgustikke, et suhelda oma sõpradega, laadida üles fotosid, jagada linke ja videoid, saada teavet inimeste kohta, kellega ollakse kohtunud või plaanitakse kohtuda jne.

Internet on avalik ruum. Mõtle alati, mida sa suhtlusvõrgustikes teistega jagad, sest mida oled kord internetis teistega jaganud, seda on raske või pea võimatu internetist täielikult eemaldada. Küll saad sa aga suhtlusvõrgustikes määrata, kellega millist infot jagad. MTÜ Lastekaitse Liit on koostanud projekti “Targalt internetis” raames populaarsete keskkondade privaatsussätete seadmise juhised. Enda andmeid läbimõeldult jagades vähendada riski sattuda ebasoovitava olukorda.



**Facebook**

[privaatsusseadete soovitused](#)



**Instagram**

[privaatsusseadete soovitused](#)



**Twitter**

[privaatsusseadete soovitused](#)



**Ask.Fm**

[privaatsusseadete soovitused](#)



**Snapchat**

[privaatsusseadete soovitused](#)



**Tumblr**

[privaatsusseadete soovitused](#)



**WhatsApp**

[privaatsusseadete soovitused](#)

# ÜLDISED SOOVITUSED

## Fotod

Kui soovid enda fotot lisada suhtlusportaali, siis mõtle enne, milline foto on sobilik. Ära riputa üles pilti, mille pärast sul võib häbi olla näiteks oma vanemate ees. Samuti ilma küsimata ära lae internetti fotosid oma sõbrast. Tea, et kõiki pilte on võimalik kopeerida ning sa ei tea kunagi, kuhu su pildid võivad sattuda.

## Profiil

Kui sa täidad profiili, siis tee seda lühidalt. Ära avalda oma isiklike andmeid, neid võidakse sinu suhtes vääralt kasutada.

## Postitused

Mõtle läbi, kellele sa soovid oma postitustes oleva sõnumi, pildi või video edastada ning jaga seda ainult nendega.

## Kommentaarisid

Ära vasta ebameeldivatele või sündusetutele kommentaaridele. Sõpradega vesteldes vasta läbimõeldult. Tea, et igaüks võib teie juttu lugeda.

Lisa oma **sõprade nimekirja** vaid inimesi, keda sa päriselt tunnend. Oluline ei ole, kui palju inimesi sa enda sõprade nimekirja suudad lisada, vaid see, kui palju sul tegelikult on tõelisi sõpru.

## Mõtle enne, kui midagi postitad!

Pea alati meeles, et internet on avalik koht ning kõik su postitused on kättesaadavad!

## Parool

Kasuta turvalist parooli ja ära jaga seda kellegagi.

## Kui vajad abi...

...siis teavita sellest suhtlusvõrgustikus kasutades nt *report* või *teavita* nuppu või pöördu nõu ja abi saamiseks usaldusväärse täiskasvanu, lastea-bitelefoni 116111 või veebikonsta-ablite poole.

## Logi välja!

Peale keskkonna kasutamist logi ennast kindlasti keskkonnast välja.



# Tutvu erinevate Lastekaitse Liidu projektidega

[www.lastekaitseliit.ee](http://www.lastekaitseliit.ee)

[ajakiri.lastekaitseliit.ee](http://ajakiri.lastekaitseliit.ee)

[www.targaltinternetis.ee](http://www.targaltinternetis.ee)

[www.kiusamisestvabaks.ee](http://www.kiusamisestvabaks.ee)

## Uuri ka Lastekaitse Liidu lastelaagrite kohta

[www.lastelaagrid.eu](http://www.lastelaagrid.eu)



**Lastekaitse Liit**  
Estonian Union for Child Welfare

**T**@rgalt internetis





Anna meile tagasidet  
ja soovita teemasid,  
mida võiksime järgmistes  
numbrites kajastada.

[ajakiri@lastekaitseliit.ee](mailto:ajakiri@lastekaitseliit.ee)