TARTU ÜLIKOOL
Sotsiaalteaduste valdkond
Ühiskonnateaduste instituut
Kommunikatsioonijuhtimise õppekava

Diana Poudel

Digipädevusi arendava õpimängu “Häkkerite lahing” loomine

Magistritöö

Juhendaja: Maria Murumaa-Mengel, PhD

Tartu 2019

TÄNUSÕNAD

See töö on olnud põnev rännak tundmatutes vetes ning teel sihtkohta olen saanud tuge ja suunavaid juhiseid paljudelt fantastilistelt inimestelt. Esmalt tahaksin tänada oma juhendajat Maria Murumaa-Mengelit, kes aitas praktilistele ideedele panna ümber akadeemilise rüü ning kelle tagasiside oli alati väga innustav. Suur tänu ka Birgy Lorenzile, kes aitas luua mängule sisu ning esitas kriitilisi küsimusi just siis, kui neid kõige rohkem oli vaja.

Suureks abiks oli ka Eesti lauamängurite kogukond – eesotsas Meelis Looveeri, Aigar Alaveeri ning Kaido Tammega. Tänu neile ei pidanud ma ratast leiutama asuma, vaid sain kohe sõitma asuda.

Kindlasti tänan ka Telia Eesti AS kollektiivi liikmeid, kes andsid tagasisidet ja aitasid mängu testida. Ei saa kindlasti unustada ka 125 Hooandjat, kes projektile õla alla panid ning hoo sisse lükkasid.

Suur aitäh ka neile paarisajale õpilasele, kes mängu katsetasid ja oma mõtteid minuga jagasid. Ja õpetajatele, lapsevanematele ja kõigile teistele, kellega ma viimase aasta jooksul mängu teemadel suhelnud olen.

Pikk pai minu kahele inspiratsiooniallikale, Mirjamile ja Oliverile, kelle seiklustele digimaailma džunglites ma jätkuvalt kaasa elan ning kes kannavad hoolt, et mul lapsevanemana kunagi teemad otsa ei saaks, mida sügavamalt uurida on vaja.

Kõik see ei oleks võimalik, kui mu lastel ei oleks nii fantastilist vanaema, kes alati on nõus lapsed enda tiiva alla võtma, kui nende ema mööda Eesti koole ringi rallib või Tartus tarkust juurde käib hankimas. Ma olen selle toe eest väga tänulik.

Ja lõpetuseks suur tänu Maile, kes aitas mul kaosest korda luua ning kes alati oli taamal olemas, et kaasa elada või vajadusel turgutada.

SISUKORD

SISSEJUHATUS

Käesoleva magistritöö tulemusena valmib hariv lauamäng, mille abil saab lastega lahti rääkida olulised digimaailmaga seotud teemad ja suurendada dialoogi ning seeläbi üksteise mõistmist erinevate tegutsejate ja põlvkondade vahel. Lauamängu sihtrühmaks on eelkõige 1.-6. klassi õpilased ja nende vanemad. Töö eesmärgiks on anda põhjalik ülevaade mängu loomise protsessist, selle erinevatest etappidest ning testimisest.

Põhjus sellise töö teema valimiseks on minu isiklik kogemus: olen IT taustaga lapsevanem, kes annab küberhügieeni teemalisi külalistunde lastele, nende vanematele ja õpetajatele. Viimase paari aasta jooksul olen teinud turvalise interneti koolitusi enam kui paarile tuhandele noorele ja täiskasvanule ligi poolesajas erinevas Eesti koolis ning näen, kui palju tegelikult lapsed soovivad, et lapsevanemad tunneksid huvi nende tegemiste vastu virtuaalmaailmas. Ka lapsevanemad on mures selle pärast, millega nende lapsed internetis tegelevad ja sooviksid oma sõnul teada, kui seal mingeid probleeme on. Ometigi tajun, et eraldav müür kahe põlvkonna vahel on kohati väga tugev ning kumbki pool ei oska seda müüri lõhkuda või sellest üle ronida. Eelmisel kevadel püüdsin seda müüri lammutada raamatuga “Turvaline internet. Digimaailma teejuht”. Raamat sai küll ekspertidelt ja pedagoogidelt palju positiivset tagasiside, kuid kahjuks pole see veel kaasa toonud soovitud laiaulatuslikku muutust ning soovin panustada teadlikkuse tõstmisesse ja dialoogi arendamisse veelgi. Olen täheldanud trendi, et lapsevanemad on väga varmad lastele koolitusi tellima ning koolid kutsuvad mind lapsevanematele küberhügieenist rääkima, kuid täiskasvanutel puudub autonoomne motivatsioon ennast teemadega kurssi viia ning pigem püütakse kedagi teist koolitada ja seeläbi jäädakse ise passiivsesse rolli.

Hiljuti ühes Lääne-Virumaa koolis jäin peale turvalise interneti koolitust viienda klassi lastega rääkima erinevate mängude teemal. Vestlus oli täies hoos, kui järsku üks poiss ütles, et see on nii imelik. Kui palusin täpsustada, mis imelik tundub, sain vastuseks, et ta

pole kunagi ühegi täiskasvanuga varem mängude teemal vestelnud. Ja see poiss pole ainus. Ma olen kuulnud sarnast fraasi kümnetelt lastelt Eesti erinevates paikades. Neil on sügav soov oma tegemistest rääkida, kuid kahjuks on neil mulje, et vanematel pole huvi neid kuulata. Noortel on probleemid petuskeemidega, vägivaldsete videotega, küberkiusamisega, kahtlaste SMS-dega ja palju muu negatiivsega, kuid nad arvavad, et nende veebipõhised mured vanemaid ei huvita ja seetõttu neist teemadest täiskasvanutega sageli ei räägita.

Erinevad põlvkonnad kasutavad internetti erinevalt (Taipale, 2016; Ait, 2017) ning seetõttu võib olla keeruline leida teemasid, mis teisele osapoolele huvi pakuks. See olukord on kurb, kuid samas mõistetav. Vähem kui ühe inimpõlvega on internetist saanud unikaalne ja universaalne tööriist, mis on maailma transformeerinud. Tehnika areneng on olnud nii kiire, et see on toonud endaga kaasa hulganisti väljakutseid.

Järjest suuremad on ootused koolidele ja haridussüsteemile, et need aitaksid noortel toime tulla riskidega digimaailmas ja aitaksid arendada vajalikke digipädevusi (Kalmus, von Felitzen ja Siibak, 2012; OECD, 2015 Kluzer ja Pujol Priego, 2018). Järk-järgult on digipädevuste teemad, oskused ja teadmised jõudnud koolide õppekavadesse (Digipööre..., i.a), paika on saanud õppijate digipädevuse mudel (Õppijate..., 2016) ja teema on üldisemalt pidevalt aktuaalne (Leikop, 2018; Raudla, 2019; Koolid…. , 2019). Teadlikkuse kasvule ja kooli tegevusele suunatud soovitused ja jõupingutused on küll asjakohased, sest need on digipädevuste arendamise raamistuses kindlasti olulised tegutsejad ja struktuurid, kuid arvestama peaks paljude seonduvate probleemidega. Näiteks paljudel õpetajatel napib digivaldkonna-alaseid teadmisi (Leppik, Haaristo ja Mägi, 2017) ning digipädevuste arendamisel on mitmeid teisigi olulisi agente nagu näiteks eakaaslased, vanemad, õed-vennad, sotsiaalmeedia mõjuliidrid jne (Hargittai, 2010; Kalmus jt, 2012; Vinter, 2013). Lisaks tegeletakse formaalhariduses täna eelkõige erinevate digitaalsete töövahendite kasutama õpetamisega, see tähendab, tehnilisemate spetsiifiliste osaoskuste arendamisega, ning vähem tähelepanu saavad komplekssed ja sotsiaalsed oskused ning teadmised nagu netikett, turvalisus, kontekstuaalne privaatsus (Leppik jt, 2017).

Olen suhelnud oma külalistundide käigus kümnete õpetajatega erinevates Eesti koolides ja näen, kuidas õpetajad tunnevad, et ootused neile on liiga kõrged. Valdav enamus

õpetajatest, kellega olen suhelnud, on nõus, et tundidesse peab lõimima digipädevuste õpet, kuid lapsevanem ei saa delegeerida kõike interneti ja nutiseadmetega seonduvat õpetajatele. Ühes Tallinna kesklinna koolis aitasin eelmisel aastal ühel õpetajal lahendada olukorda, kus kolm sõpra olid teinud ühise mängukonto, kuid siis läksid tülli, kui üks poiss oli teinud kontol oleva n-ö kaasomandiga iseseisvalt tehingud. Mängimine toimus kodudes, kuid pinged jõudsid kooli ning õpetaja tundis survet probleem lahendada, samas ta ei saanud üldse aru, milles konflikt seisneb. Seletasin asja kaasomandi näitel ning meie jutuajamise tulemusena otsustasid poisid individuaalsed kontod luua ja n-ö ühisvara ära jagada.

Teine ekstreemne näide oli, kui ühes väikeses maakoolis paluti mul koolitusel süvitsi käsitleda SMS laenude võtmist n-ö mängunänni ostmiseks. Selgus, et vanemate klasside õpilastel on selle teemaga seoses suuri probleeme ning vanemad leidsid, et see peaks kooli roll olema, et sellistest teemadest rääkida. Isiklikult olen ma seda meelt, et lapsed peaksid esmased küberhügieeni alased teadmised kodust saama, sest see on ka koht, kus kasutatakse internetti märgatavalt rohkem.

Olen teinud mitmeid lapsevanematele suunatuid koolitusi ning tundub, et lapsevanemad tahaksid lapsi paremini internetis suunata, kuid puudub ettekujutus, kuidas seda teha. Hetkel on lapsevanemate jaoks küll välja töötatud mõningaid digimaailmas toimimise juhiseid ja abistavaid materjale (nt targaltinternetis.ee, suurimjulgus.ee), kuid nendes keskkondades on väga palju infot ning selle edasiandmine lapsele võib osutuda küllaltki keeruliseks. Netikäitumise teemade käsitlemine ja digimaailma ohud ning võimalused tõstatuvad teemana peredes reeglina n-ö tulekahju kustutamisena, reaktiivselt – kui mõni veebirisk on pereliikme jaoks realiseerunud või kui meedia kajastab intensiivselt mõnda konkreetsemat veebiriski (Kõrvits, 2018; Pau, 2018).

Noorte netikäitumise teemat on uuritud küllaltki palju nii Eestis kui maailmas laiemalt. Näiteks Kristi Vinter (2013) käsitleb oma doktoritöös digitaalse ekraanimeedia tarbimist 5-7 aastaste laste seas ja Birgy Lorenz (2017) lõi oma doktoritöös mudeli, millega saab paremini mõista teismelise internetikasutaja vajadusi. Laste ja noorte netikäitumise teemat uuritakse aktiivselt ka Tartu Ülikooli ühiskonnateaduste instituudis (Kalmus, von Feilitzen ja Siibak, 2012; Siibak ja Tamme, 2013; Kalmus, Blinka ja Ólafsson, 2015; Murumaa-Mengel, 2017). Selle magistritöö kirjutamise ajal ilmusid EU Kids Online

jätku-uuringu tulemused (Sukk ja Soo, 2018), mis annavad hea ülevaate noorte käitumispraktikatest digimaailmas.

Magistritöö tulemusena valmib hariv ja mänguline tööriist „Häkkerite lahing“ lapsevanematele, mis aitab arutada lastega erinevaid teemasid juba enne, kui need tõstatuvad negatiivsete veebikogemuste kaudu ja mis ei sõltu ajahetkel aktualiseerunud meediasündmustest. Luues erinevaid veebiriske- ja võimalusi käsitleva lauamängu, on võimalik arendada mitme eri huvipoole teadlikkust kübermaailma ohtudest ning suurendada laiemalt digipädevusi (eelkõige suunatud lastele, vanematele ning õpetajatele). Teiseks eesmärgiks on kaardistada, kirjeldada ja analüüsida selle mängu välja töötamise protsessi, et tulevikus sarnaseid projekte kavandavad inimesed saaksid ülevaate sarnase iseloomuga ülesannete võimalikest tegutsemisviisidest ja -protsessidest. Kolmandaks ülesandeks, mis käesoleva töö raames püstitatud, on mängu sisu ise - noored ja veebiriskid – mille kohta on võimalik saada tagasisidet strateegiliselt kavandatud koostöös sihtrühmadega. Lühidalt – magistritöö kirjeldab ja analüüsib seda, kuidas luua digipädevusi õpetavat lauamängu, milline peaks olema selle sisu ja kuidas huvipooled selle mängu keskmes olevate teemadega suhestuvad.

Magistritöö püüab anda vastused kolmele peamisele uurimisküsimusele, millest kaks esimest keskenduvad mängu loomisele ning viimane veebiriskide sisulisele tajumisele ja kogemisele:

UK1: Millised teemad peavad olema digipädevusi käsitlevas õpimängus kajastatud, et see aitaks kõige paremini ennetada erinevaid riske, millega noored digimaailmas kokku puutuvad ning annaks noortele vajalikke oskusi digimaailmas tegutsemiseks?

Sellele küsimusele leian vastuse esimeses peatükis, kus analüüsin erinevaid uuringuid ja loon ülevaate teooriast, mis on käesoleva töö kontekstis oluline.

UK2: Milliseid mängudisaini universaalseid elemente ja aspekte saab rakendada interneti-teemalise laumängu loomisel?

- Milline on mänguloome protsess konkreetse lauamängu näitel?

Teisele uurimisküsimusele vastan töö teises peatükis, kus kirjeldan detailselt mänguloome protsessi mängu “Häkkerite lahing“ näitel ning annan ülevaate mängu elementidest ja dünaamikast.

UK3: Kuidas suhestuvad erinevad huvipooled mängus käsitletavate veebiriskidega?

- Milliste teemade puhul võib märgata erinevate huvipoolte kõrgemat ja madalamat teadlikkust?
- Millised teemad ja mängudisaini elemendid aitavad kaasa diskussiooni ning dialoogi tekkimisele?

Sellele uurimusküsimusele vastan kolmandas peatükis, kus on ülevaade mängu testimistest erinevate huvipooltega.

Olen oma töö struktureerinud veidi teistmoodi, kui klassikalise ülesehitusega teadustööd. Seda eelkõige, sest minu töö ei ole lineaarse loomuga (kõigepealt töö teoreetilise materjaliga, seejärel andmekogumine ja analüüs jne), vaid olen läbivalt ja pika aja jooksul tegelenud paralleelselt mitme etapi ning ülesandega, püüdes läheneda sellele projektile võimalikult terviklikult.

Magistritöö esimeses peatükis annan, nagu tavaks, ülevaate olulisematest teoreetilistest ja empiirilistest lähtekohtadest, keskendudes noorte veebikäitumisele ja online-riskidele, nendega toimetulekuks vajaminevatele digipädevustele ning mängudisaini baasteadmistele.

Teises peatükis annan ülevaate lauamängu “Häkkerite lahing” loomise protsessist, püüdes kirjeldada nii konkreetse mängu loomise juures läbi käidud etappe, kuid tuues välja ka teoreetilisema olemusega universaalseid protsesse ja skeeme, mis võivad olla abiks teistele, kes soovivad luua õpimängu.

Kolmandas peatükis kirjeldan mängu testimise ja arendamise käigus toimunud osalusvaatluste, intervjuude ning külalistundide tulemusi ja analüüsin veebiriskide tajumise ning teadlikkuse sisulisi aspekte. Töö lõppeb diskussiooni ja enesereflesiooni peatükiga.

1 TEOREETILISED JA EMPIIRILISED LÄHTEKOHAD

Käesoleva peatüki eesmärgiks on luua teoreetiline raamistik esimese uurimisküsimuse lahendamiseks. Soovin mõista, millised on teaduskirjanduse käsitluses peamised digipädevused ja veebiriskid, kuidas toimub mängude loomine ning mis on need elemendid mängus, mis muudavad mängu mängijate jaoks atraktiivseks.

1.1 Noorte digipädevused

"Te olete hirmunud oma laste pärast, sest nad on põliselanikud maailmas, kus teie olete sisserändajad"

- John Perry Barlow (1996) "Küberruumi iseseisvuse deklaratsioon"

Erinevate tegutsejate oskuste ja teadmiste alase diskussiooni pidamiseks, on oluline ära defineerida, mida me **digipädevuste** all mõistame. Abstraktsel ja üldisel tasemel peetakse digipädevusteks oskusi, mis on seotud **info leidmisega, haldamisega, hindamisega ning vahetamisega** (OECD, 2015). EU Kids Online uuringus (Sukk ja Soo, 2018) hinnatakse digipädevuste osana muu hulgas laste oskust eemaldada inimesi oma kontaktide nimekirjast, salvestada nutiseadmega pilte ning laadida veebipoest rakendusi nutiseadmesse. Enamus lapsi ütleb üsna kindlalt, et saab nende tegevustega hakkama (Sukk ja Soo, 2018), kuid kas need on tõesti piisavad digipädevused? Kui laps oskab pilte teha nutitelefoniga ja mängude jaoks häkke internetist alla laadida, ei tähenda, et tal on olemas koolitööks vajalikud digipädevused (Bennett jt, 2008). Oluline küsimus on siinkohal see, mis täpselt mõjutab noorte digipädevuste arengut. Kas piisab sellest, et nad kasvavad üles ühiskonnas, mis on tehnoloogiast läbi imbunud või on vajalik vanemate ja õpetajate tugi omandamaks vajalikke teadmisi, oskusi, väärtuseid ja hoiakuid.

Marc Prensky (2001a) võttis esimesena akadeemilises maailmas kasutusele mõisted **digitaalne pärismaalane** (*digital native)* ning **digitaalne immigrant** (*digital immigrant*)

ning tema arvamus oli, et keskkonna mõju on esmatähtis ning ta väitis, et uus põlvkond on eelmisest niivõrd erinev, et me peame muutma oma haridussüsteemi, sest praegused viisid enam ei toimi. Tema sõnul on digitaalsed pärismaalased suutelised korraga tegema mitmeid tegevusi, nad on aktiivsed ja lõbusad ning harjunud kohese tagasisidega (Prensky 2001a; 2001b).

Prensky mõtted ja terminid on tänaseks pälvinud palju kriitikat. Hargittai (2010) soovitab pigem kasutada terminit **digitaalsed naiivikud** (*digital naives*), sest tema uuringute põhjal mõjutab noorte digitaalseid pädevusi pigem nende perekondlik taust kui sünniaasta. Kirschner ja De Bruyckere (2017) tegid uuringu, mis viidi läbi kuni 50-aastaste arvutikasutajate seas ning nende tulemused ei näidanud otsest seost digipädevuste ja vanuse vahel. Samuti ei ole nad nõus väitega, et tänapäeva noor suudab korraga mitut asja teha efektiivsemalt kui eelmine põlvkond (Kirschner ja De Bruyckere, 2017) ning selle tulemusega on kooskõlas uuring, mille autoriteks Bennet, Maton ja Kervin (2008).

Viidi läbi uuring (Taipale, 2016), mille eesmärgiks oli välja selgitada kuidas erineb esimese ja teise põlve digitaalsete pärismaalaste ning digitaalsete immigrantide **digitaalse meedia** tarbimine. Tulemused näitasid, et teine põlvkond (ehk noored, kes on sündinud 2000ndate keskpaigas ja hiljem) tarbivad rohkem erinevaid digitaalse meedia vorme ning on kaasatud erinevamatesse tegevustesse, kui teised grupid, kuid autor toob välja, et piir nende digitaalsete põlvkondade vahel on hägune ning seetõttu ei soovita ta sellist liigitust kasutada (Taipale, 2016).

Digipädevuste omandamist võib mõjutada ka nutiseade, mida noored kasutavad. Paremad digioskused on noortel, kes kasutavad rohkem tahvelarvuteid ja arvuteid – nutitelefonide kasutamise aktiivsus digioskuseid ei mõjuta (Akçayır, Dündar ja Akçayır, 2016). Samas teame värsketest uuringutest, et Eesti noored kasutavad järjest rohkem nutitelefone ning palju harvemini kasutatakse lauaarvutit (Sukk ja Soo, 2018) ehk siin võib tekkida oht, et hoolimata suuremast nutiseadme kasutamisest noorte teadmised digimaailmas toimuva kohta ja oskused seal hakkama saada hoopis vähenevad.

Noored ise usuvad, et nad teavad rohkem internetist kui nende vanemad, näiteks Mascheroni ja Ólafssoni (2014) läbi viidud uuringust selgus, et 38% noortest usuvad, et

teavad rohkem kui vanemad internetist ning 58% väitsid, et oskavad nutitelefoni kasutada paremini kui nende vanemad. Samas uuringus vastas 42% noortest, et nad ei oska raporteerida internetis ebasobivast sisust või tegevusest ning ainult 28% 9-12 aastastest tüdrukutest oskab privaatsussätteid muuta (poiste puhul sama näitaja 38%). Sarnased tulemused saadi Eestis EU Kids Online jätku-uuringus, kus 9-12 aastaste laste seas teavad alati, kuidas internetis ebameeldivustega toime tulla 28% ning 13-17 aastaste vastanute seas vastas 47%, et oskab alati ebameeldivustega toime tulla (Sukk ja Soo, 2018).

Euroopa Liidus on loodud **DigComp digipädevuste raamistik** (vt *Tabel 1*), mis peaks olema abivahend ekspertidele ja koolitajatele ning seal on toodud välja viis kompetentside valdkonda, mis on vajalikud, et kasutajad saaksid tehnoloogiat kasutada oma eesmärkide saavutamiseks nii personaalselt kui professionaalselt.

Tabel 1. DigComp digipädevuste raamistik

Info ja andmete mõistmine	Digitaalse info sirvimine, otsimine ja sortimine Info hindamine Info talletamine ja taasesitamine
Kommunikatsioon ja koostöö	Suhtlemine tehniliste vahendite abil Info ja sisu jagamine Kodanikuaktiivsus veebis Koostöö digikanalite kaudu Netikett Digitaalse identiteedi haldamine
Sisuloome	Sisu väljatöötamine Lõimimine ja ümbertöötlemine Autoriõigus ja litsentsid Programmeerimine
Ohutus	Seadmete kaitsmine Isikuandmete kaitsmine Tervise kaitsmine Keskkonna kaitsmine
Probleemilahendus	Tehniliste probleemide lahendamine Vajaduste väljaselgitamine ja neile tehnoloogiliste lahenduste leidmine Innovatsioon ja tehnoloogia loov kasutamine Digipädevuse lünkade välja selgitamine

(Allikas: Kluzer ja Pujol Priego, 2018)

DigComp raamistik on kasutusel ka Eestis, selle põhjal on koolide jaoks loodud õppijate digipädevusmudel (Õppijate…., 2016). Eesmärgiks on lõimida digipädevuste õpe erinevate õppeainetega, kuid hetkel on see protsess veel algusjärgus ning koolide tase digipädevuste õpetamisel on ebaühtlane (Leppik jt, 2017). Üheks suureks takistuseks on õpetajate endi vähesed oskused tehnoloogiarikkas keskkonnas toimetamiseks (Valk, 2013).

Peatüki lõpetuseks pean tõdema, et tegelikult puudub ühene arusaam, et kes ja kuidas noorte digipädevusi kõige rohkem mõjutab. DigComp raamistik (Kluzer ja Pujol Priego, 2018) on väga põhjalik ning kui haridussüsteem suudaks kõik need soovitatud teemad õppekavadesse lõimida, siis võib see kaasa aidata noorte paremate digipädevuste tekkele. Kahjuks hetkel on digipädevuste lõimimine ainekavadesse kaootiline – suurimateks takistavateks teguriteks on digivahendite vähene hulk koolides, õpetajate piiratud aeg, sobiva taristu puudus ning sobivate õppematerjalide puudus (Leppik jt, 2017). Seda viimast kitsaskohta püüab selle magistritöö raames valmiv mäng leevendada pakkudes välja õpetajatele ja lapsevanematele ühe tööriista, mille abil saab vajalikke digipädevusi õpetada.

1.2 Noorte riskikäitumine internetis

"Kasutaja valib alati tantsivad sead turvalisuse asemel"

- Bruce Schneier (Miller, 2009)

Noored alustavad interneti kasutamist väga varajases eas (Vinter, 2013; Macheroni ja Ólafsson, 2014; OECD, 2015), kuid neil puuduvad tihti oskused ja kogemused, et osata toime tulla internetis tekkivate ohtlike olukordadega (Helsper, 2008; Lorenz, Kikkas ja Laanpere, 2012; Sukk ja Soo, 2018). Ohtlike olukordadena võib käsitleda näiteks suhtlemist võõrastega, isikliku info jagamist, kahtlaste eesmärkidega mängudes osalemist, tundmatute failide avamist ja paljut muud (Livingstone, Kirwil, Ponte ja Staksrud, 2014; Sukk ja Soo, 2018).

Nagu eelmises peatükis viidatud, on paljude vanemate ja õpetajate seas levinud arusaam, et lapsed on sündinud juba teatud digipädevustega (Prensky 2001a; Murumaa-Mengel, 2017) ning seetõttu ei piirata suure osa laste internetikasutust ning nende tegemisi ei jälgita igapäevaselt (Álvares jt, 2013). Seetõttu on lapsed aktiivsed iseseisvad tegutsejad

virtuaalmaailmas ning nad peavad leidma ise sobivad strateegiad, kuidas võimalike riskiolukordadega toime tulla. Helsper (2008) uuris, milliseid taktikaid noored kasutavad potentsiaalselt ohtlike olukordadega toimetulekuks ning jõudis tõdemuseni, et kõige levinum on noorte seas n-ö jaanalinnu taktika ehk püüe probleeme mitte näha ja loodetakse, et oht möödub iseenesest. Näiteks seksuaalse sisuga sõnumi saabumisel kustutab algklassilaps sõnumi ja blokeerib sõnumi saatja ning loodab, et selline olukord ei kordu.

EU Kids Online'i Eesti 2018. aasta uuringust selgus, et 27% lastest, kes olid internetis ebameeldivustega kokku puutunud, hoidsid selle enda teada (Sukk ja Soo, 2018). Kindlasti on olukordi, mida laps suudab lahendada iseseisvalt ilma usaldusväärse täiskasvanu abita, kuid see peaks olema teadlik valik ning mitte olema lapse hirmust või teadmatusest tingitud otsus.

Teema mõistmiseks on oluline kaardistada, milliste ohtudega noored kokku puutuvad. Livingstone jt (2014) pakkusid välja neli kategooriat internetiriskide jaoks (vt *Tabel 2*) - **veebisisuga, käitumisega ja suhetega seotud riskid ning muud riskid**. Ta kasutas riskide klassifitseerimiseks 2010. aastal toimunud EU Kids Online esimest üle-euroopalist uuringut, kus lastel paluti vabas vormis vastata küsimusele, mis neid internetis häirib. Sellele küsimusele vastas pea 10 000 last ning vastuste põhjal lõi ta tabelis välja toodud kategooriad. Esinemissagedus näitab, kui palju küsimusele vastanud lapsi seda tüüpi ohte või häirivat sisu välja tõi.

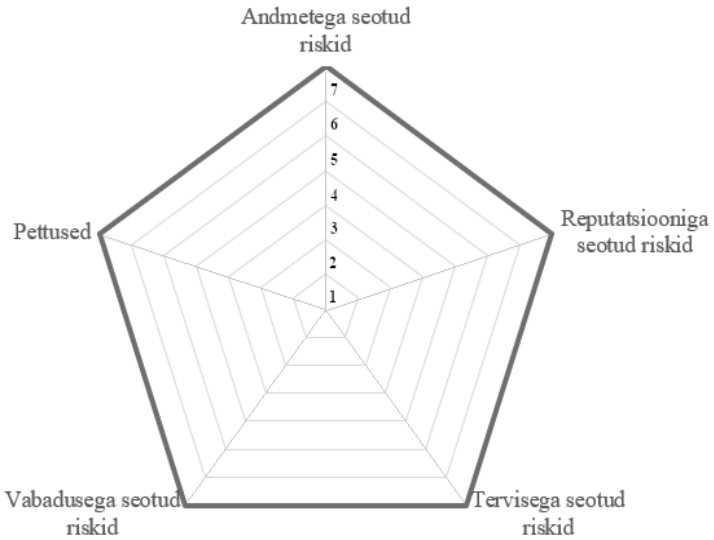
Tabel 2. Ohud ja riskid, millega noored internetis kokku puutuvad

Risk	**Sagedus**	**Kirjeldus**
Sisuga seotud riskid	55,4%	Pornograafiline sisu Vägivaldne sisu Muu (hirmutav, narkootikumid, reklaam, rassistlik, enesetapule õhutav, anoreksiat propageeriv, mina-pilti kahjustav jne)
Käitumisega seotud riskid	19,4%	Õel või agressiivne suhtlus, kiusamine Soovimatu käitumine (ropendamine, vulgaarne käitumine) Häkkimine või andmete väärkasutus Reputatsiooni kahjustamine teiste inimeste poolt Seksuaalne ahistamine Personaalse info jagamine

Risk	Sagedus	Kirjeldus
Suhetega seotud riskid	14,0%	Sobimatud kontaktid üldiselt Võimalikud sobimatud seksuaalsed kontaktid Teise inimese kehastamine Reaalsed kohtumised Ideoloogiline või religioosne ajupesu Teiste inimeste ligipääs sinu andmetele (küpsised)
Muud mainitud riskid	7,7%	Viirused Spämm Skämm jmt
Ülejäänud	3,5%	Riskid, mida ei saa ühegi eeltoodud kategooria alla liigitada

(Allikas: Livingstone jt, 2014)

Birgy Lorenzi (2017) doktoritöös on soovitatud kasutada mudelit, kus riskid on jagatud viieks kategooriaks ning lisaks soovitab ta kasutada seitsmeastmelist skaalat, et täpsemini kaardistada kasutaja teadmised ja oskused iga riskivaldkonna kohta (1-algaja tase; 7-eksperdi tase). Läbi kategooriate ja skaalade saab luua iga kasutaja kohta unikaalse küberhügieeni alaste teadmiste kaardi (vt *Joonis 1*).



Joonis 1. Digitaalse ohutusega seotud riskide kategooriad koos tasemetega (1-algaja; 7-ekspert) (Lorenz, 2017)

Oluline on küsimus, kas ja kuidas vanemad ning õpetajad saavad kaasa aidata sellele, et lapsed omandaks sobivad toimetulekumehhanismid ja -strateegiad erinevates ohuolukordades. Üheks võimaluseks on **vastupidavuse** (ingl *resilience*) loomine andes lapsele vajalikud teadmised ja vahendid erinevates olukordades toime tulekuks (Windle, 2011). Hea **digitaalne kirjaoskus** ning aktiivne **vanemapoolne juhendamine** aitavad lapsi paremini ette valmistada digitaalse maailma riskidega toimetulekuks (Piotrowski ja Valkenburg, 2015; Rodríguez-de-Dios, van Oosten ja Igartua, 2018).

Oluline on mõista, et need riskid ei esine üksikult, vaid näiteks sobimatu kontakt võib viia seksuaalse ahistamiseni või mõista, et paljude petuskeemide eelduseks on see, et inimene jagab oma personaalset infot. Digimaailmas käitumine on küllaltki sarnane liiklemisega tänavatel - vajalik on pidev selgitustöö vaheldumisi praktiliste kogemustega. Mänguline lähenemine aitab teadmisi omandada ning neid kinnistada (Saar, 1997; Koster, 2013; Kiili, de Freitas, Arnab ja Lainema , 2012). Kui liikluslinnak õpetab liikluses käitumist, siis mäng "Häkkerite lahing" aitab lapsi ette valmistuda digimaailma iseseisvaks külastuseks.

1.3 Õpimängude loomine

"Mäng on lapse elu jaoks sama oluline, kui unenägude nägemine magamise ajal."

- Sally Jenkinson (2001) "The Genius of Play"

Videod ja arvutimängud on tänapäeva laste lapsepõlve oluliseks osaks ning see mõjutab nende ootusi ümbritsevale maailmale. Näiteks tunnevad õpetajad järjest suuremat survet võtta klassiruumis kasutusele rohkem mängulisi komponente (Prensky 2001a; 2001b; Furdu, Tomozei ja Köse, 2017). Siinkohal tuleb küll vahet teha mängustamisel (*gamification*), mille sisuks on eelkõige päriselu tegevustele mänguliste kihtide lisamine (Nicholson, 2015) ja tõsimängudel (*serious games*), kus mängule lisatakse hariv komponent ning lõbu ja õppimine peaksid olema tasakaalus (Arnab jt, 2015). Käesoleva töö eesmärgiks on luua tõsimäng, mille abil saaks noortele õpetada vajalikke digipädevusi.

Enam ei saa lapsed õppida päriselu lihtsalt oma vanemaid jälgides (Jenkinson, 2001) ning seetõttu püütakse anda vajalikke oskusi noortele läbi mängude. Kahjuks õpetab enamik

tõsimänge küllaltki kitsa valdkonna teadmisi ning nende loomisel ei ole seatud eesmärgiks üldisemate oskuste arendamine (Romero, Usart ja Ott, 2015). Oluline on mõista, et mäng on lihtsustatud mudel päriselust (Coil, Ettinger ja Eisen, 2017), mis aitab mängijate jaoks mõista ja kinnistada mustreid, mis neid päriselus ümbritsevad (Koster, 2013).

Hea mäng peab olema vaba tegevus, mille juurde last ei sunnita (Saar, 1997; Gordon 2008) ning see peab pakkuma erinevaid kogemusi, et iga osaleja leiaks mängust enda jaoks midagi tähendusrikast ja olulist (Nicholson, 2015; Koster, 2013). See peab pakkuma just mängija võimetele vastavat väljakutset (Kiili, Lainema, de Freitas ja Arnab 2014), sest liiga lihtne mäng on igav ning samas liiga keeruline mäng ei võimalda mängijal leida mustreid ning ta näeb ainult arusaamatut müra (Koster, 2013). Kui mäng on kohustuslik, kaob mängijal motivatsioon (Domínguez jt, 2013) ning seetõttu peaksid mängu elemendid olema loodud nii, et mängijale tekiks autonoomne motivatsioon mängu mängimiseks, mis lähtuks sisemistest väärtushinnangutest (Deci ja Ryan, 2008).

Caillois (2001) on jaganud mängud neljaks kategooriaks ning iga kategooria puhul toob ta välja tegevused, mis rikuvad mängijate jaoks mängust saadava naudingu:

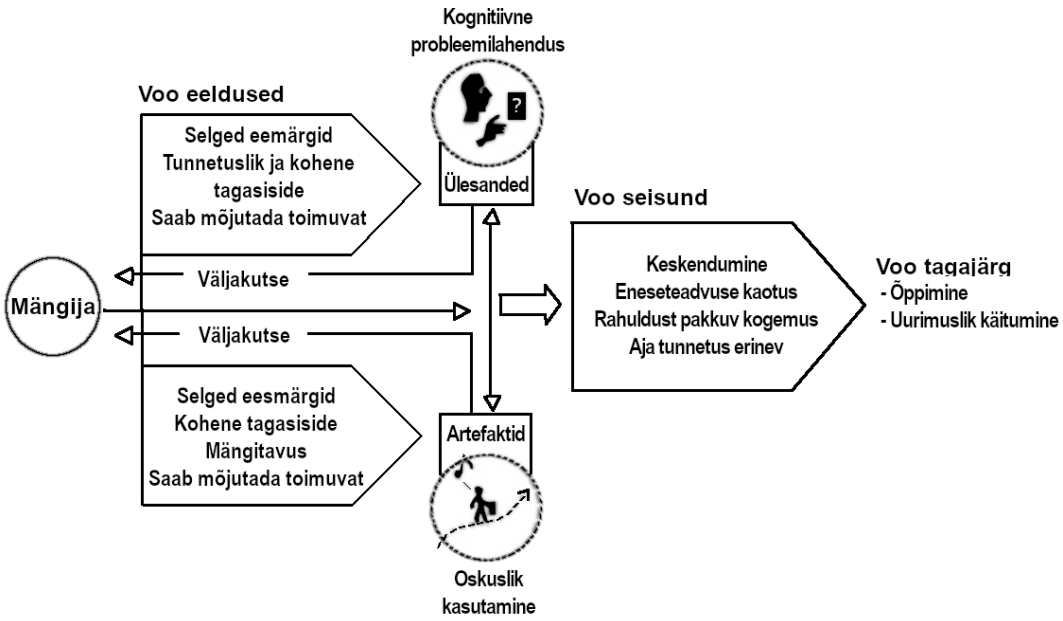
- **AGÔN** (võistlus) - sport, parima välja selgitamine. Mängu rikuvad võim, pettus, vägivald;
- **ALEA** (juhus) - õnnemängud, juhuslikkus määrab võitja. Mängu rikuvad ebausk, astroloogia jne;
- **MIMICRY** (simulatsioon) - maskid, teater, näidendid. Mängu rikuvad võõrastamine, jagatud isiksus;
- **ILINX** (põnevus) - adrenaliini teket soodustavad tegevused (kiikumine, ratsutamine jne). Mängu rikuvad alkohol ja muud mõnuained.

Väga vähesed mängud esindavad puhtalt ühte kategooriat. Lauamängudes on enamjaolt nii *agôn'*it ehk võistlust ning *alea'*d ehk juhuslikkust.

Mängude **põhielemendid** on mehaanika, lugu, esteetika ning tehnoloogia ja hea kasutuskogemuse loomiseks on vaja artefakte ning nendega seotud ülesandeid (Kiili jt, 2012). Mängu **mehaanika** pannakse paika reeglitega, mis määravad ära, kui palju mõjutavad mängu tulemust mängija tehtud valikud ehk strateegia ning kui suur on roll

juhuslikkusel (täringud, segatud kaardid) - mängus peaks mehaanika olema tasakaalus (Koster, 2013). Juhuslikkus aitab luua erinevat mängukogemust igal mängul, kuid mängija peab tunnetama, et tema valikud ja otsused mõjutavad mängu. Mängu **artefaktideks** lauamängu puhul on tegelased, nupud, kaardid, mängulaud, märgised ning muud füüsilised või virtuaalsed vahendid, mille abil saab mängija mõjutada mängu käiku. *Joonisel 2* on näidatud Kiili jt (2012) poolt välja töötatud õpimängude soovituslik voog.

Jooniselt 2 näeme, et läbi artefaktide ja ülesannete esitatakse mängijale mängus erinevaid väljakutseid ning nende lahendamine annab mängijale uusi teadmisi ja võimaluse teemat sügavuti uurida. Väga olulisteks eeldusteks Kiili jt (2012) mudeli juures on selged eesmärgid, kohene tagasiside ja mängija tunnetus, et ta kontrollib mängu kulgu.



Joonis 2 Õpimängu voog (*flow*) (Allikas: Kiili jt, 2012; autori tõlge)

Õpimängu loomisel peavad mängu eesmärgid olema seotud **õpiväljunditega** ning kui eesmärgid on väga kõrged, siis tuleb kasutada väiksemaid vahe-eesmärke (Kiili jt 2014). Mängule pole mõtet liiga keerulist **lugu** juurde mõelda, sest mängijaid huvitab eeskätt mängu juurde asumine ning pigem on motiveeriv see, kui mängu käigus saavad mängijad ise mängu käigus sisu ja lugusid juurde luua (Koster, 2013). Mängu **esteetika** moodustavad mängust saadud sensoorsed aistingud, mida mängija saab läbi disaini,

kunsti, helide ning muude erinevate kunstivormida ja mille tulemuseks on mängust saadav nauding (Niedenthal, 2009).

Arvestades käesoleva magistritöö eesmärke, peab mäng “Häkkerite lahing” olema küllaltki lihtsa mehaanikaga, kus tulemus sõltuks pigem mängijast (tema teadmistest ja valitud strateegiast) kui juhusest. Samas on juhus vajalik, et pakkuda korduvat mängurõõmu. Mängija peab koheselt saama tagasiside soovitud tulemuse (head teadmised) puhul ning mäng peab olema visuaalselt atraktiivne ja mängu artefaktid peavad olema üheselt mõistetavad, kuid ei tohi piirata mängijate tegutsemisvabadust ning loovust.

2 ÕPIMÄNGU "HÄKKERITE LAHING" LOOMINE

Käesolevas peatükis püüan leida vastuse teisele uurimisküsimusele „Milliseid mängudisaini universaalseid elemente ja aspekte saab rakendada interneti-teemalise laumängu loomisel?" vastuse otsimist ning püüan anda vastuse alaküsimusele „Milline on mänguloome protsess konkreetse lauamängu näitel?". Peatükis põimin teoreetilisi teaduslikke lähtekohti oma isiklike kogemuste ja taustateadmistega ning annan detailse ja süstemaatilisel eneserefleksioonil põhineva ülevaate sellest, kuidas õpimängu "Häkkerite lahing" väljatöötamine käis.

2.1 Mängu eesmärk ja soovitud õpiväljundid

Olen läbi viinud turvalise interneti külalistunde paarile tuhandele lapsele ning teinud koolitusi sadadele lapsevanematele ning järjest enam olen veendunud, et on vaja rohkem tööriistu, mis aitaksid lastel ja nende vanematel koos arutada läbi erinevaid olukordi, mis võivad internetis ette tulla. Hetkel võib märgata tugevat dissonantsi selle vahel, kuidas lapsed ja lapsevanemad hindavad omavahelise suhtluse sagedust ja ulatust interneti teemadel (Sukk ja Soo, 2018).

Eelmisel kevadel andsin välja raamatu "Turvaline internet. Digimaailma teejuht" (Poudel, 2018a) lootuses, et selline käsiraamatu formaat aitab vanematel ja õpetajatel paremini mõista digimaailma telgitaguseid, kuid kahjuks avaldus selle raamatu puhul kolmandas isikus mõtlemise efekt, mida Helsper (2008) käsitleb oma artiklis. Kuigi kõik on nõus, et küberhügieen ja vastutustundlik internetis käitumine on teemad, millega peaks tegelema, siis ikkagi eeldatakse, et endal on vajalikud teadmised olemas ning seega raamatut peaks lugema keegi teine. Paljud lapsevanemad ei tunne end interneti teemadel kindlalt (Sukk ja Soo, 2018) ning seetõttu on neil keeruline võtta initsiatiivi diskussiooni algatamiseks.

Otsides erinevaid lahendusi selle suhtlemisprobleemi lahendamiseks jõudsin järeldusele, et mäng võib olla efektiivne vahend antud olukorras. Lauamängud on endiselt laste seas küllaltki populaarsed ning kombineerides meelelahutusliku sisu vajaliku infoga on võimalik luua suurepärane tööriist, mille abil saab õppida nii uusi teadmisi kodus ja koolis.

Seadsin mängu "Häkkerite lahing" eesmärgiks tõsta valmisolekut iseseisvalt internetis tegutsemiseks ning õpetada noortele taktikaid erinevate ohuolukordadega toimetulekuks. Selle eesmärgi täitmiseks on vajalik saavutada järgmised õpiväljundid:

- mängijad on kursis erinevate enamlevinud ohtudega internetis;
- mängijad on kursis enda õiguste ja võimalustega internetis;
- mängijad mõistavad erinevaid erialaseid termineid, mida interneti ja arvutitega tegeledes vaja võib minna;
- mängijad oskavad valida sobivad strateegiad erinevates ohuolukordades, et vältida füüsilist, vaimset või finantsilist kahju.

Lisaks nende õpiväljundite saavutamisele peab mäng vastama järgmistele kriteeriumitele:

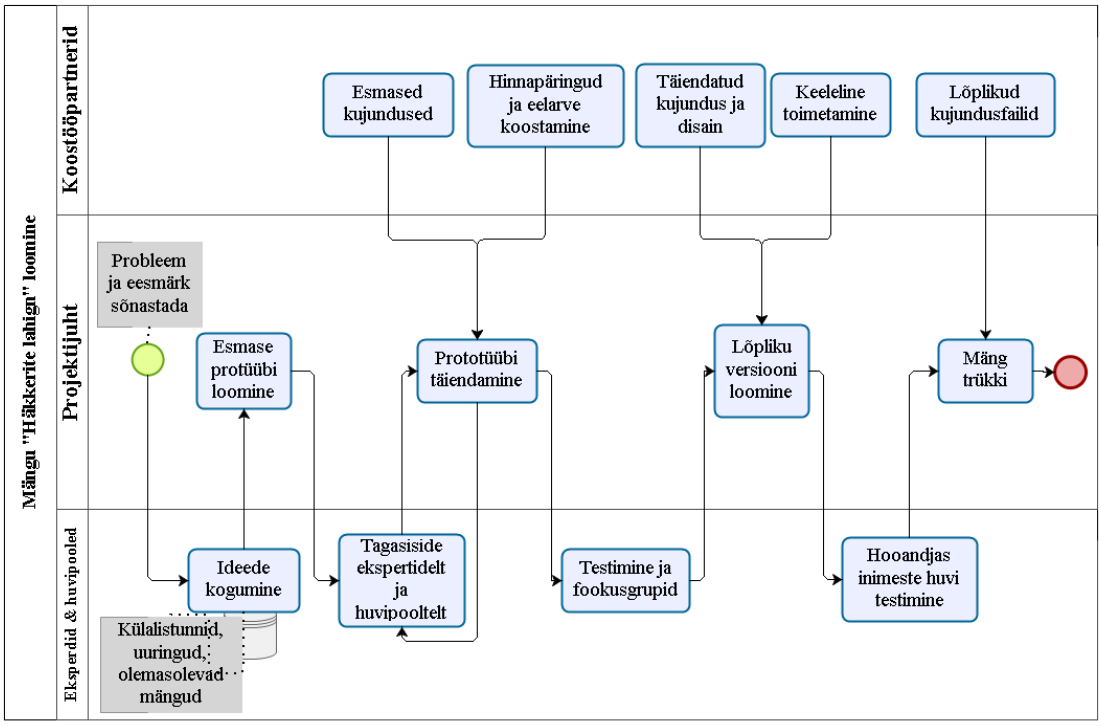
- mängu artefaktid ja ülesanded on seotud internetiga ning moodustavad tervikliku loo;
- mäng on võimalikult mitmekülgne - eesmärgiks on aidata kaasa erinevate 21. sajandi jaoks vajalike oskuste ja kompetentside arendamisele;
- mängu on võimalik mängida nii konkureeriva kui koostöömänguna;
- mängu on võimalik kohandada koolitundide jaoks;
- mäng on põnev ka sellisel juhul, kui vastamisi on erinevate teadmistega mängijad.

Mäng peaks valmima hiljemalt 2019. aasta suveks ning juba järgmisel sügisel on plaanis hakata pakkuma koolidele külalistunde mängu baasil. Selleks ajaks valmivad abimaterjalid, millega õpetajad ja julgemad lapsevanemad saavad soovi korral iseseisvalt külalistunde läbi viia.

2.2 Mängu loomise protsessi ülevaade

Mäng “Häkkerite lahing” oli minu jaoks esmakordne mängu loomise kogemus ning seda valmistades tundsin puudust juhendmaterjalidest, mis aitaksid tööd paremini raamides hoida. Seetõttu püüan käesolevas töös anda võimalikult täpse ülevaate kogu protsessist, et see töö oleks tulevikus abiks neile, kellel plaan ise mõni õpimäng luua.

Protsessi visualiseerimiseks lõin protsessijoonise kasutades *Bizagi Modeler* programmi. *Joonisel 3* on välja toodud kõige olulisemad etapid mängu arendamisel.



Joonis 3 Õpimängu “Häkkerite lahing” loomise protsessi kaardistus (autori koostatud)

Esimese sammuna toimus **ideede kogumine** ning **tutvumine olemasolevate lahendustega**. Kohtusin selles etapis Eesti lauamängude disaineritega Aigar Alaveeri ja Meelis Looveeriga, et täpsemalt luua enda jaoks arusaam projekti skoobist ning vajalikest tegevustest. Tutvusin erinevate mängudega, mille eesmärgiks on internetialaste teadmiste suurendamine (vt *Lisa 1*). Väga kasulikku sisendit sain õpilastelt ja lapsevanematelt oma rohketes külalistundides ja eelnevast tööst digipädevuste-alase koolitaja ja eestkõnelejana (Raudla, 2018; Poudel, 2018b; Lõugas, 2019).

Kui piisaval hulgal sisendit oli kogutud, alustasin **prototüübi loomisega**. Algselt oli plaan luua mängulaud koos riikidega (vt *Joonis 4*), kuid peale paari testimist oli selge, et sellisel tasemel mäng ei täida seatud eesmärki – algklassilaste ja paljude lapsevanemate jaoks oli tegu liiga keerulise mänguga. See oli kindlasti õppetund, et tuleb kohe alguses alustada testimisega sihtrühma seas, sest valdkonna ekspertide arusaam tavakasutajate teadmistest võib olla moonutatud ja liialt optimistlik.

Joonis 4 Esimese ideekavandi materjalid turvalise interneti lauamängu jaoks

Teise ideekavandi puhul püüdsin traditsioonilise mängulaua asemel kasutada hoopis tegelaskaarte. Mängija eesmärk on sel puhul oma hoole all olevaid tegelasi kaitsta internetis olevate riskide eest. Mu esimene ideekavand põhines olemasoleva lauamängu "Discworld"[1] mehaanikal, kuid teine versioon mängust oli täielikult minu isiklik idee, kus kasutasin komponente väga erinevatest lauamängudest. Tegelaskaartide nakatumise idee

[1] "Discworld" on strateegiamäng, mis toimub Terry Pratchetti Kettamaailma raamatutes kirjeldatud fantaasialinnas Ank-Morpork. Iga mängija saab endale salajase tegelaskaarti ning ta peab saavutama just selle tegelaskaarti jaoks olulise eesmärgi. Täpsem info mängu kohta: https://boardgamegeek.com/boardgame/91312/discworld-ankh-morpork

sain “Pandemic”[2] mängust, unikaalsete tegelaskaartide idee oli “Discworld” rollikaartidest inspireeritud ja kaitsekaartide kategooriate osas andis inspiratsiooni “Eesti Mälumäng”[3]. See lisas mängu arendustegevusse märgatavalt keerukust, et leida tasakaal strateegia ja juhuslikkuse vahel. Kui esmane idee oli paigas, testisin mängu mehaanikat alguses üksi ja eeldusega, et kõigil mängijatel on täielikud teadmised ning ainuke asi, mis mängu pikkust mõjutab on juhuslikkus (täring) ning strateegia. *Joonisel 5* on näha üks taoline testimine.

Joonis 5 Mängu teise versiooni mehaanika testimine

Kui mehaanika oli paigas, hakkasin välja mõtlema küsimusi mängu jaoks. Esimesed 50 küsimust tulid minu raamatu „Turvaline internet. Digimaailma teejuht“ (Poudel, 2018a) ning külalistundides kasutatud Kahoot testide põhjal. Edasi läks küsimuste välja mõtlemine järjest keerulisemaks – sain sisendit akadeemilistest allikatest, meediast, erinevatelt veebilehtedelt, kus oli laste ja internetiturvalisuse teemat kajastatud. Lõplikus versioonis on 150 kaitsekaarti koos küsimustega.

[2] “Pandemic” on koostöömäng, kus iga mängija saab spetsiifilise rolli (nt arst, uurija, logistik jne) ning mängijad peavad ühiselt saama kontrolli alla viiruste leviku maailmas. Täpsem info mängu kohta: https://boardgamegeek.com/boardgame/30549/pandemic

[3] Lauamängus “Eesti Mälumäng” peab mängija vastama erineva valdkonna küsimustele õigesti ning võidab see, kes kõige kiiremini vastab õigesti igas valdkonnas vähemalt ühele küsimusele. Kasutatakse valikvastustega küsimuste kaarte ning täringuid. Täpsem info mängu kohta: https://www.rahvaraamat.ee/p/lauamäng-eesti-mälumäng/1010781/et?ean=6416739537597

Kui teatud hulk küsimusi oli välja mõeldud, siis tegin nende põhjal kaitsekaardid, mille abil mängijad saavad oma kasutajaid pahavarast puhastada. Igal kaitsekaardil on küsimus ning kolm vastusevarianti, mille hulgast peab mängija õiged vastused leidma. Kui loodud oli umbes 70 kaitsekaarti, siis alustasin testimisi. Esimesel testimisel püüdsin võimalikult erinevaid testgruppe kaasata. Näiteks mängisime mängu koos õpetajate ja haridustehnoloogidega, kodus koos lastega ning viisin läbi külalistunnid Laagri kooli 2. klassides, kus katsetasin mängu koolitunni formaadis. Lähemalt kirjutan paljude huvipooltega toimunud mängu testimise käigus kogutud sisendis kolmandas peatükis.

Lauamängu puhul on väga oluline roll visuaalil, seetõttu palusin endale appi kursusekaaslase Marja-Liisa Platsi, kes on illustreerinud üle 40 lasteraamatu ning kelle tööd on pälvinud erinevaid auhindu ja tunnustusi. Marja-Liisa rolliks oli mängu kujundus ja põnevate tegelaskaartide joonistamine. Alustasime tegelaskaartide testimisega. Laagri kooli külalistundides toimus esimene suurem katsetamine tegelaskaartide jaoks, et välja selgitada, milliseid tegelasi lapsed oma tiimi tahavad. Väga selgelt joonistus selles etapis muu hulgas välja see, et lapsed eelistavad n-ö aktiivseid tegelasi passiivsetele. Aktiivseteks pean selliseid karaktereid, kes on mõne tegevusega hõivatud, passiivsed tegelased poseerivad tegelaskaardi jaoks pigem portree- või passifoto stiilis. Täpsemalt saab sellest testist lugeda peatükis 3.3 ning *Joonisel 24* (lk 46) on toodud näited erinevatest tegelaskaartidest ning nende populaarsuse kohta laste seas.

Peale iga testimist sai prototüübile sisse viidud täiendused. Õpetajate ning ekspertide sisend oli eelkõige seotud küsimuste ja vastustega ning noorte seas läbi viidud testimiste tulemustena said paika tegelased. Lõplikus mänguversioonis on viis taset küsimustele, sest laste tase on erinev ning väga erineval tasemel küsimused läbisegi tekitasid noorte seas testimisel pahameelt ja tõid kaasa huvi languse mängu osas. Huvitav on see, et jagades küsimused erineva raskusastmega tasemeteks, kasvas noorte huvi keerulisemate küsimuste osas - kõrgemal tasemel mängimine tundus olevat noorte jaoks prestiižsem.

Mäng sobib lastele alates seitsmendast eluaastast ning seda saab mängida üks kuni kuus mängijat. Enam kui kahe mängija puhul moodustatakse tiimid. Üks mäng kestab 15 – 45 minutit, kuid mõne testimise käigus tekkis mängu käigus nii elav vestlus, et mäng ei saanud otsa isegi paari tunniga. Soovi korral saab mängu mängida ka kahe

mängukomplektiga – sellisel juhul saab iga mängija oma käigukorral otsustada, kellele ta täringuga pahavara veeretab ning see tõstab mängu keerukust.

Paralleelselt prototüübi loomisega tegelesin koostööpartnerite otsimisega. Selgus, et Eestis on üksikuid trükikodasid, kes suudavad nii keerulist toodet trükkida täies mahus. Võtsin neilt hinnapakkumised ning võin oma kogemusest 2018-2019 aastal öelda, et , kui tiraažiks plaanida 1500 mängu siis taolise mängu välja andmise maksumus koos kujunduse, keelelise toimetamise jmt on suurusjärgus umbes 10 000 eurot.

Koostööpartneri otsingul erasektorist kaardistasin ettevõtted, kelle tegevusvaldkond kattub võimalikult ulatuslikult projekti skoobiga ning kellel oleks huvi suurendada noorte digipädevusi. Sellisteks ettevõteteks on eelkõige info- ja kommunikatsioonitehnoloogia ettevõtted. Esmalt otsustasin ühendust võtta Telia Eesti AS-ga, kes on viimastel aastatel panustanud noorte küberhügieeni alaste teadmiste kasvu läbi oma projekti #suurimjulgus ning kellega olen varem koostööd teinud. Teliale meeldis idee väga ning leppisime kokku koostööraamistikus, kus Telia aitab finantseerida mängu välja andmist ning mängu pakendile lähevad ka nende brändielemendid.

Täiendava rahastuse sai mäng läbi ühisrahastusplatvormi Hooandja, kus projekt kogus 125 toetajat (Lõbus…., 2019) ning osa kuludest plaanin katta omaosalusena. Mäng on plaanis välja anda hiljemalt augustis 2019. Hooandja keskkonda kasutasin vajaliku investeeringu leidmiseks, kuid see keskkond andis mulle ka võimaluse testida, kas lapsevanemad ja õpetajad on huvitatud sellisest mängulisest tööriistast ning projekti edukas lõppemine andis kindlustunnet juurde, et jätkata mängu välja andmisega. Mäng “Häkkerite lahing” on mu kolmas projekt Hooandjas - varasemalt olen selle abil käivitanud kohaliku robootikaringi (Robootikaring…., 2015), ning eelmine kevad andsin selle abil välja raamatu “Turvaline internet. Digimaailma teejuht” (Turvaline…., 2018). Hooandja keskkond on suurepärane töövahend, millel on ühisrahastuse kaasamiseks vajalik funktsionaalsus, kuid tuleb mõista, et turundustöö jääb enamalt jaolt projektijuhi enda teha. Oluline on kindlasti see, et projekti tutvustavad materjalid oleksid piisavad ning võimalusel visuaalselt atraktiivsed. Samuti aitab projekti õnnestumisele kaasa mitmekülgne auhindade valik.

2.3 Mängu lugu ja artefaktid

Eelmises kahes peatükis andsin ülevaate mänguga seotud protsessist tervikuna. Oluline on mõista, et mängu tootearenduse protsess reaalses elus ei ole lineaarne, vaid pigem korduv tsükkel, kus pidevalt tuleb tagasi pöörduda eelmiste etappide juurde. Käesolevas peatükis annan ülevaate artefaktidest ja mänguelementidest, millest mäng koosneb.

Mängu lühike lugu algab nii: "Internetis käib lõputu lahing heade ja halbade häkkerite vahel. Nad käivad mööda internetti ringi, otsivad nõrkusi süsteemides ja testivad kasutajate teadmisi, kuid nende eesmärk on erinev. Valge kaabuga head häkkerid soovivad muuta internetti turvalisemaks kohaks, kus kõigil oleks hea olla ning selleks nad parandavad turvaauke ja koolitavad kasutajaid. Musta kaabuga pahade häkkerite eesmärgiks on isiklik kasu ning nad ei hooli sellest, et nende tegevus teistele kahju põhjustab. Nüüd on ka sinul, armas mängija, võimalus selles lahingus osaleda. Häid häkkereid on alati juurde vaja ning sinu abi on vaja, et kurjade häkkerite jõud ei saavutaks ülekaalu."

Termin häkker tähistab ajalooliselt inimest, kes tunneb suurt huvi arvutite vastu ning soovib mõista tarkvara ja riistvara toimimist tunduvalt sügavamal tasemel (Yagoda, 2014). Kahjuks on sõna saanud negatiivse tähenduse laiema auditooriumi jaoks ning sõna häkker seostatakse sageli küberkuritegevuse ning halbade kavatsustega. Tegelikult on kriminaalsed häkkerid ehk musta kaabu häkkerid ehk kräkkerid üks väike grupp häkkerite kogukonnast (Yagoda, 2014). Võib öelda, et mängu loo ja pealkirja üks eesmärk on teadvustada noorte ja nende vanemate jaoks, et termin „häkker" on tegelikult neutraalne ning infoühiskonnal on vaja häid ja osavaid häkkereid.

Mängijad (ehk head häkkerid) saavad mängu alguses endale kuus tegelast, keda nad mängu käigus kaitsma peavad. Kui mängitakse võistlevat mängu, siis võidab see mängija, kes oma tegelased kõige enne pahavarast puhastab. Kui mängitakse koostöömängu, siis võistleb tiim paha häkkeri vastu, kes oma rünnakuid teeb täringute abiga ning mängijad võidavad juhul, kui suudavad tegelased ära puhastada enne, kui kaitsekaardid mängulaual otsa saavad. Mäng koosneb 12 tegelaskaardist, 150 kaitsekaardist, kahest n-ö paha häkkeri täringust, 12 numbrižetoonist ning 36 pahavara žetoonist (vt *Joonis 6*).

Joonis 6 Mängu „Häkkerite lahing“ artefaktid (prototüüp)

Tegelaskaartide nurka pannakse mängu alguses numbrižetoonid ning igale tegelaskaardile veeretatakse üks pahavara žetoon. Kaitsekaartidel on ikoonid, mis näitavad, millist pahavara selle kaitsekaardiga eemaldada saab. Järgnevalt tutvustan põhjalikumalt mängus kasutusel olevaid artefakte.

2.3.1 Tegelaskaardid

Tegelaskaartide loomisel olid seatud järgmised eesmärgid:

- tegelaskaardid peavad olema unikaalsed ning iga tegelaskaart peaks kandma endas pikemat lugu, et nad aitaksid kaasa diskussiooni tekkele ning pakuksid mängijatele võimalusi mõelda erinevate olukordade peale, kus tehnoloogiat kasutatakse;
- mängija saab oma tegelaskaardid ise lõpuni meisterdada, mis annab võimaluse igale mängukomplekti omanikule luua unikaalsed tegelased;
- kõik pildid annavad võimaluse aruteluks tehnika ja interneti rolli üle meie igapäevastes tegemistes;
- oluline on vältida soolisi, vanuselisi ja muid stereotüüpe, mis võivad tekkida noortel väga varajases eas (Miller ja Budd, 1999; Sheenan, 2003) ning mis võivad

vähendada näiteks tüdrukutel digipädevuste omandamise soovi (Gürer ja Camp, 2001; Clayton, von Hellens ja Nielsen, 2009). Lisaks võivad stereotüübid tekitada internetis võltsi turvatunnet, sest kurjategijaid ja ahistajatele omistatakse mingeid erilisi omadusi, mis ei ole kooskõlas kuritegude baasil koostatud tegelike kurjategijate profiilidega (Murumaa-Mengel, 2017).

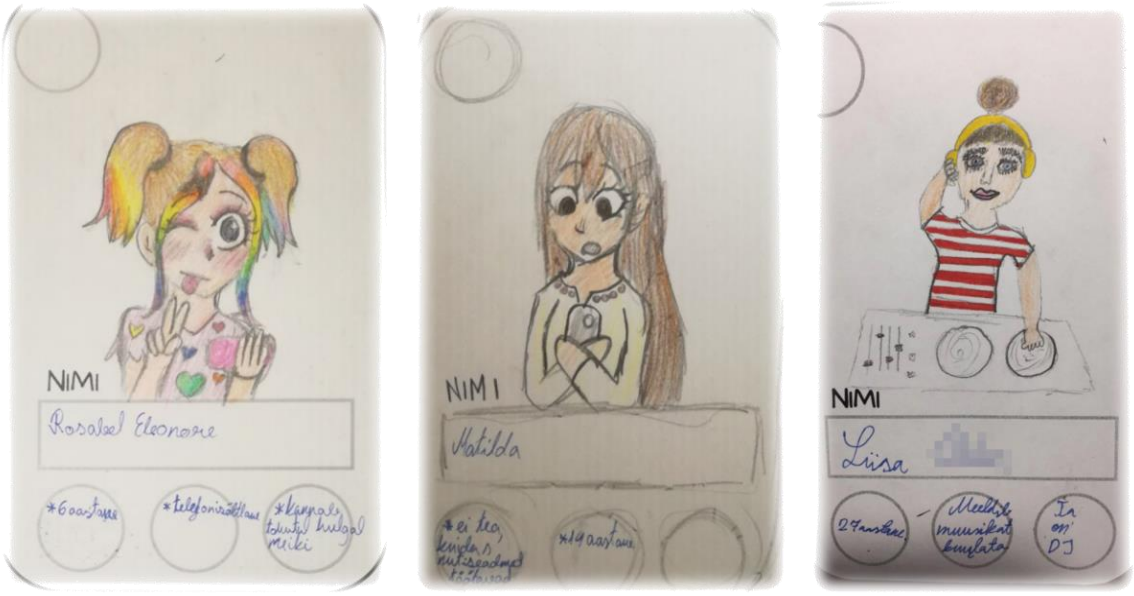
Joonis 7 Näited tegelaskaartidest mängus “Häkkerite lahing”

Näiteks *Joonisel 7* on vasakpoolsel tegelaskaardil vanaema, kes virtuaalmaailmas mängib. See tegelaskaart on laste seas väga populaarne ning tihti on just poiste jaoks esimene valik, kui hakatakse endale tegelaskaarte mängima (vaata põhjalikumat ülevaadet testgruppidest saadud tulemuste kohta peatükist 3). Taustainfona võin öelda, et see tegelaskaart on inspireeritud isiklikust kogemusest – meie peres oli just vanaema see, kes koos lastelastega vahva virtuaalmängude koha leidis, kus saab erinevaid virtuaalreaalsuse mänge mängida. Nüüdseks on vanaema palju paremini kursis, mida virtuaalreaalsus tähendab ning lapsed oma sünnipäevadel leiavad kingikotist kinkekaardid, mis annavad taas põhjuse üheks mõnusaks ühiseks külastuseks VR mängude ruumi.

Keskmine tegelaskaart on saanud inspiratsiooni isiklikest kogemustest. Olen viimased neli aastat seotud olnud Laagri Roboringi tegemistega ning olen kaasjuhendaja tüdrukute tiimile. Olen kuulnud lugusid, kuidas kodus vanemad püüvad suunata tüdrukuid ikkagi n-ö naiselikemate alade poole isegi olukorras, kus tüdruk on robootika proovitunnis

käinud ja ise soovib jätkata. Mitmed uuringud toovad välja soolise tasakaalutuse IKT sektoris (Barker ja Aspray, 2006; Kindsiko, Türk ja Kantšukov, 2015) ning selle tegelase roll ongi viia vanemate ja õpetajateni sõnum, et robootika on täiesti sooneutraalne hobi, kuhu kõik tragid noored on alati oodatud olenemata nende soost.

Parempoolne tegelaskaart on pühendatud kõigile neile noortele, kes tahaksid, et nende vanemad tunneksid rohkem huvi nende mängumaailmades toimuvate seikluste vastu. Mängudel on noorte elus suur osa ning usun, et lapsevanemad võiksid vahepeal mängupuldi kätte võtta ja koos lapsega mõnd mängu mängida virtuaalmaailmas. Sest tegelikult 43% videomängude mängijatest on vanemad kui 36 aastat (Age…., i.a) ning naiste osakaal mängijate seas oli USA-s 2018. aastal 55% (Distribution…., i.a). Tegelaskaardil kujutatud tegelane ei tohiks tegelikult olla nii suur anomaalia meie ühiskonnas, kuigi mul ei õnnestunud leida ühtegi Eesti spetsiifilist uuringut, kus oleks arvutimängurite kohta toodud üldine statistika vanuse ja soo järgi. 2007. aastal tehti küll bakalaureusetöö Tartu Ülikooli Sotsiaalteaduskonnas, kus uuriti Eesti *online*'i mängijaid *World of Warcrafti* näitel ning selles töös on spetsiifilises internetifoorumis (http://www.kalevlased.pri.ee/foorum) tehtud küsitluse tulemused vanuse järgi. Online küsitlusele oli vastanud 238 liiget, kellest 2% vastas, et nad on 30 aastased või vanemad (Seeman, 2007). Aga see on liialt spetsiifiline valim ning see töö on tehtud 12 aastat tagasi, seetõttu ei julge ma nende andmete põhjal mingeid üldistusi teha.



Joonis 8 Laste poolt joonistatud tegelaskaardid

Kõigi 12 tegelaskaardi kujundusi saab vaadata *Lisas 2*. Igasse mängukomplekti tuleb kaks tühja tegelaskaarti, kuhu soovi korral saab ise joonistada tegelasi. Mõned näited laste endi poolt joonistatud tegelastest, mis tehti mängu arendusprotsessi käigus, on *Joonisel 8*.

2.3.2 Halva häkkeriga seotud artefaktid

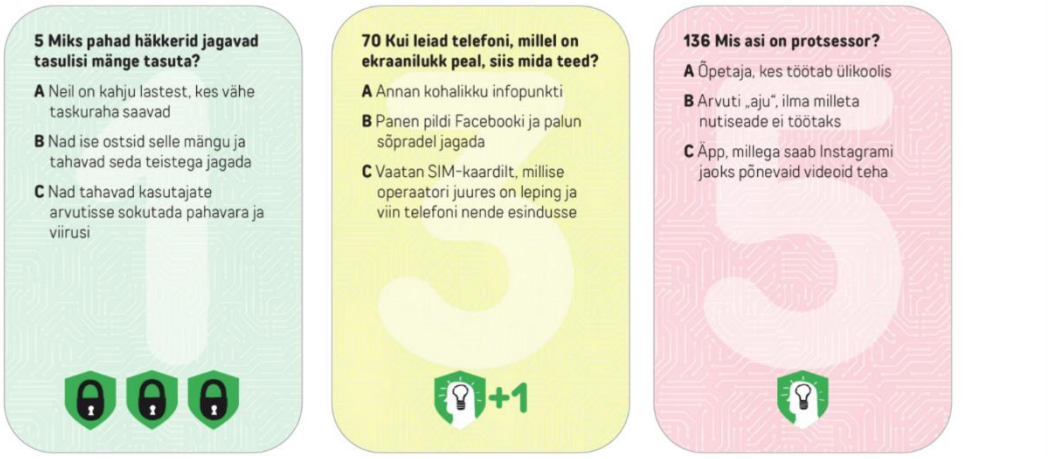
Halva häkkeri rolli täidavad mängus täringud. Mängus on kombineeritud strateegia koos teatava juhuslikkusega (Caillois, 2001). Häkker saab nakatada tegelaskaarti kolme tüüpi pahavaraga, mis on märgitud mängus erinevate žetoonidega (vt *Joonis 9*).

Joonis 9 Pahavara žetoonid, millega häkker tegelasi nakatab

Esimene žetoon sümboliseerib ebaviisakat ja pahatahtlikku käitumist internetis. Teine žetoon näitab kasutaja kehvasid üldteadmisi arvutite ja interneti kohta ning kolmanda märgi tähendus on lukustamata andmed ja seadmed. Olen saanud tagasisidena kommentaare, et tegelikult ei ole päris õige neid kategooriaid pahavaraks nimetada, kuid tuleb mõista, et mäng on reaalse elu väga lihtsustatud mudel (Koster, 2013; Coil jt, 2017) ning seetõttu oli selline lihtsustus vajalik järeleandmine terminoloogilise täpsuse arvelt.

2.3.3 Kaitsekaardid

Tõsimängul peab kindlasti olema hariv komponent (Arnab jt, 2015) ning selle eesmärgi saavutamiseks tegin 150 kaitsekaarti (vt *Joonis 10*) küsimustega, mis on jaotatud viieks tasemeks. Igal kaitsekaardil on küsimus seoses digipädevustega ning teisel küljel vastus koos pikema selgitava tekstiga. Mängu eesmärgiks on panna mängijaid teema üle sügavamalt mõtlema, seega on kaitsekaartide vastuste puhul võimalik, et õigeid vastuseid on üks kuni kolm. Kaitsekaardi saamiseks tuleb leida kõik õiged vastused. Kõik kaitsekaartide küsimused koos vastuste ja selgitavate tekstidega on *Lisas 3*.



Joonis 10 Kaitsekaartide näited koos kaitsekaartidel olevate küsimustega

Iga kaitsekaardi tagaküljel on korrektne vastus (vt *Joonis 11*) ning täiendav selgitus teema kohta. Igal küsimusel võib olla üks kuni kolm õiget vastust ning mängija saab kaitsekaardi endale ainult juhul, kui ta täiesti korrektselt vastab. Testimised näitasid, et selline mitme õige vastuse olemasolu pani mängijad pikemalt mõtlema iga küsimuse üle ning see on kindlasti soovitud tulemus, mis toetab mängu süvenemist ning uute teadmiste omandamist.

Joonis 11 Kaitsekaardi esi- ja tagakülg

Igal kaitsekaardil on ka ikoonid - need näitavad, millise pahavara vastu kaitsekaarti kasutada saab. Lisaks on osadel kaitsekaartidel +1 märk, mis tähendab, et mängija saab käia veel ühe kaitsekaardi sellel käigul. Kaitsekaartide ja pahavara žetoonide puhul on kasutatud vastandumise näitamiseks visuaali – punane taust + must häkker *versus* roheline taust + valge häkker jne. Mängija saab tegelaskaartidelt pahavara eemaldada kaitsekaartidega.

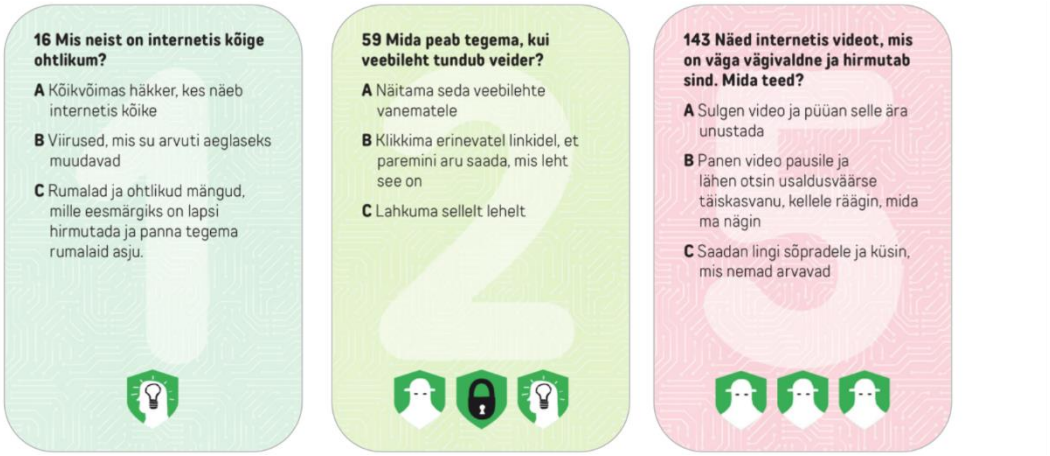
Kaitsekaartide küsimuste loomisel kasutasin erinevaid sisendeid:

- akadeemilised uuringud;
- meedias kajastatud aktuaalsed teemad;
- ekspertide soovitatud teemad;
- isiklikud kogemused külalistundidest.

Kuna mängu eesmärgiks on anda lapsevanematele ja õpetajatele tööriist, mille abil saab läbi arutada kõik põhilised veebiriskid ja küberhügieeniga seotud teemas, siis on minu jaoks oluline, et mängu küsimused kataks kõiki erinevaid kategooriaid. Kaitsekaartide eesmärgiks on katta nii olulisemad digipädevuste valdkonnad kui käsitleda ka erinevaid ohte, millega noored võivad internetis kokku puutuda.

2.3.3.1 Kaitsekaartide analüüs noorte riskikäitumise raamistuses

Livingstone jt (2014) on jaotanud internetis olevad riskid neljaks. Ehkki veebiriskid on oma olemuselt dünaamilised ning juba mõne aastaga võib palju muutuda, saab siiski juba tehtud uuringuid ja analüütilisi jaotuseid kasutada alusena baasteadmiste ja oskuste kaardistuseks. Kõige levinumad olid mainitud uuringu põhjal **sisuga seotud riskid**, mis on seotud näiteks pornograafilise või vägivaldse sisuga, kahtlased reklaamid ja muu veebisisu internetis, mille eesmärk on kuidagi mina-pilti kahjustav. Allpool on toodud mõned kaitsekaardid, mille eesmärgiks on sisuga seotud riskide teadvustamine ning soovitatav käitumine nende riskide realiseerumise korral (vt *Joonis 12*).

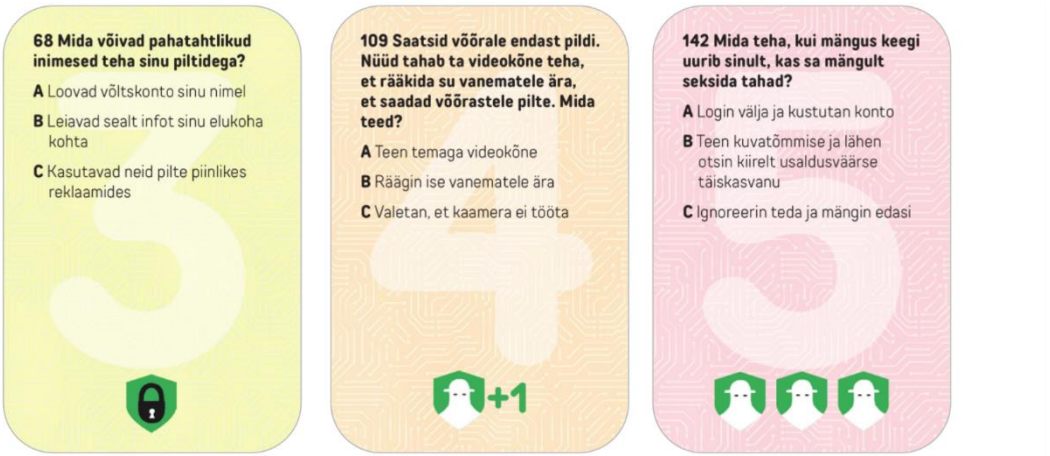


Joonis 12 Sisuga seotud riskide kaitsekaardid

Teisena toovad Livingstone jt (2014) välja **käitumisega seotud riskid**, mille alla kuuluvad erinevad küberkiusamispraktikad, soovimatu käitumine, andmete väärkasutus, seksuaalne ahistamine ja personaalse info jagamine. *Joonis 13* on mõned näited kaitsekaartidest, mis neid teemasid käsitlevad.

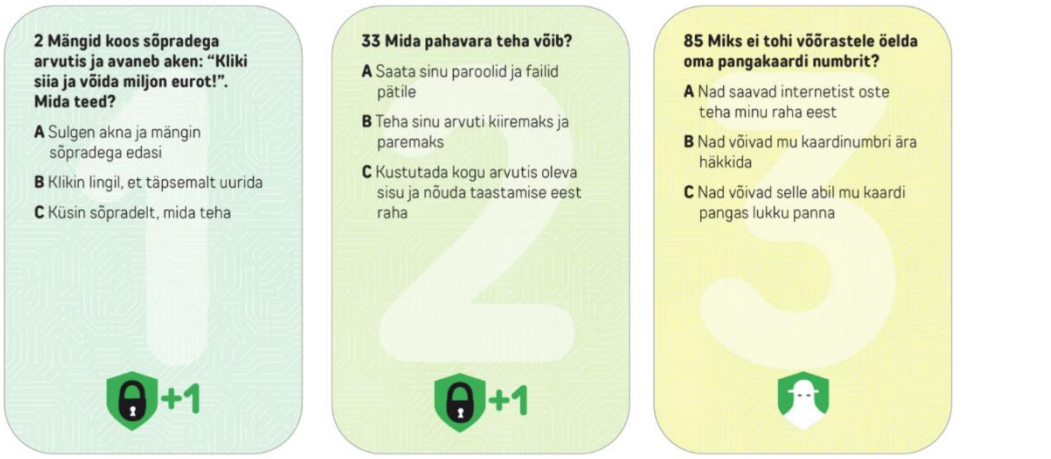
Joonis 13 Käitumisega seotud riskide kaitsekaardid

Järgmisena mainivad Livingstone jt (2014) **suhetega seotud riske** (vt *Joonis 14*), mis aastal 2010 moodustasid 14% kõigist riskidest, mida noored oma vastustes olulisteks pidasid. Isikliku kogemuse baasil julgen väita, et algklassides käivate laste jaoks peaks osakaal sellistel riskidel tegelikult suurem olema, sest järjest populaarsemad on laste seas võrgumängud (Mascheroni ja Ólafsson, 2014), kus edukaks mänguks on vajalik teiste kasutajatega suhtlemine. Mängudes ja mängides ei taju noored väga hästi piiri, kes on võõras ja kes on oma.



Joonis 14 Suhetega seotud riskide kaitsekaardid

Ülejäänud riskid on liigitatud Livingstone jt (2014) poolt kategooria **muud mainitud riskid** alla ning seal on näiteks viirused, rämpspost ehk spämm ja petuskeemid ehk skämmid. Selle riski esinemissagedus on kasvav - EU Kids uue 2018. aasta uuringu põhjal on oma nutiseadme mõne viirusega nakatanud 15% noortest. Samuti on erinevate skämmide hulk suurenenud ja juba esimestes klassides olen näinud kümneid lapsi, kes on hädas erinevate petuskeemidega mängudes. Mõned näited kaitsekaardidest, mis taolisi riske käsitlevad on *Joonisel 15*.



Joonis 15 Pahavara ja petuskeemidega seotud riskide kaitsekaardid

Kuna Livingstone, Kirwil, Ponte ja Staksrudi (2014) poolt välja toodud riskide kvalifikatsioon on leidnud kajastust paljudes akadeemilistes uuringutes, siis oli minu jaoks oluline kontrollida, et küsimused kataksid kindlasti neid teemasid. Praktikuna olen siiski kriitiline nende kategooriate osas, mis on teatud osas alati abstraktsioon ja selgem ning n-ö puhtam kui elu ise. Näiteks igasugused skämmid on seotud väga tihedalt suhtlemisega (nt manipuleerimisründed) ning kui mõtlen erinevatele olukordadele, kus olen koolitaja või lapsevanemana pidanud aitama olukorda lahendada, siis on väga keeruline olnud liigitada neid situatsioone ühe kindla kategooria alla. Seetõttu mulle endale meeldib rohkem Birgy Lorenzi (2017) doktoritöös välja pakutud riskide liigitus, kus riskid on jaotatud **andmetega, reputatsiooniga, tervisega, vabadusega seotud riskideks ning pettusteks**. See liigitus kattub paremini minu enda loodud kategooriatega mängus, kus näiteks andmete kaotus ja lekkega seotud probleemid (luku-ikoon) on ühes kategoorias ning reputatsiooni ja pettustega (valge/musta häkkeri ikoon) seotud olukorrad teises kategoorias.

Huvitavat väljakutset pakkusid **tervisega seotud teemad**. 2018. aastal lisas Maailma Terviseorganisatsioon haiguste nimekirja sõltuvusliku videomänguhäire (Scutti, 2018), kuid tegelikult puudub ühene arusaam, kui kahjulikud või kasulikud võivad erinevad tegevused internetis olla. Internetisõltuvuski on käibefraas, mida igaüks mõistab erinevalt. Salmela-Aro, Upadyaya, Hakkarainen, Lonka ja Alho (2017) jõuavad oma töös järeldusele, et liigne interneti kasutamine on seotud vaimsete häiretega nagu depressioon, üksildus ja madal enesehinnang. Samas Orben ja Przybylski (2019) analüüsisid eelnevalt läbi viidud väiksemaid uuringuid tervikliku koguna, sekundaaranalüüsina (keskendudes Iiri, Ameerika ja Inglismaa noorte seas (N= umbes 20 000) läbi viidud uuringutele) ning jõudsid järeldusele, et internetis veedetud aeg ei mõjuta noorte heaolu märkimisväärselt. Seetõttu oli keeruline luua üheselt vastavaid küsimusi kaitsekaartide jaoks, mis käsitleks tervise ja füüsilise heaolu riske. Mõned sellised kaitsekaardid siiski tegin.

Joonis 16 Tervisega seotud riskide küsimused kaitsekaartidel

Siinkohas võib tekkida küsimus, et kas *Joonisel 16* keskmine kaitsekaart on otseselt tervisega seotud - tegu on pigem ju info usaldusväärsusega? Meedias leiavad käsitlust sageli uudised, kus internetis oleva kontrollimata info mõjul tarbitakse ravimeid või muudetakse toitumisharjumusi sellisel viisil, et see võib ohustada tervist (Rohemäe, 2015). See teema on muidugi keerulisem. Näiteks 10-12 aastaste noorte seas läbi viidud uuring näitas, et noored ei suuda vahet teha erinevatest allikatest tulevate meediasõnumite vahel ning seetõttu pigem ei usuta infot tervislike toitumiskampaaniate osas, mis on näiteks riiklike institutsioonide poolt käivitatud (Dorey ja McCool, 2009).

2.3.3.2 Kaitsekaartide analüüs DigComp raamistuses

Mängu olulisemaiks õpiväljundiks on mängijate kurssi viimine enamlevinud ohtudega internetis, kuid seda pole võimalik teha ilma mängijate üldiste digipädevuste arendamiseta. Väga keeruline on rääkida õngitsuslehtedest, kui kasutaja ei tea täpselt, mis on domeen. Näiteks DigComp juhendmaterjalides on jaotatud inimeste jaoks vajalikud kompetentsid viite valdkonda, millest neljas valdkond on ohutus internetis (Kluzer ja Pujol Priego, 2018), kuid praktikuna julgen väita, et tegelikult iga valdkond on omal moel seotud interneti turvalisusega. Rääkides **info ja andmete mõistmisest**, siis info usaldusväärsuse hindamine ja vajadusel info taasesitamine probleemi korral (vt *Joonis 17*) on kindlasti oskused ja teadmised, mida kasutajal on vaja ohutuks internetis liikumiseks.

Joonis 17 Kaitsekaardid, mis aitavad kaasa DigCompi kompetentsi info ja andmete mõistmine arendamisele

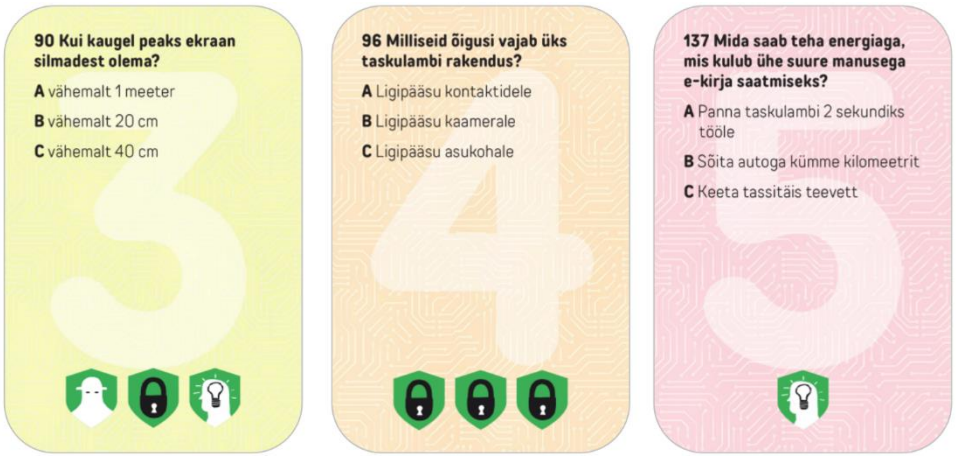
Ka DigCompi teine kompetents **kommunikatsioon ja koostöö** on väga tihedalt seotud turvalise interneti teemadega. Noored hakkavad internetis teiste kasutajatega suhtlema väga varakult ning digitaalne jalajälg internetis tekib enne kui laps kooli läheb (Vinter, 2013). Seetõttu on selle valdkonna teemad mängus kajastatud ning *Joonisel 18* on mõned näited sellistest kaitsekaartidest.

Joonis 18 Kaitsekaardid, mis aitavad kaasa DigCompi kompetentsi kommunikatsioon ja koostöö arendamisele

Ka **sisuloomega** seotud kompetentside puhul on väga tugev seos turvalisusega. Noorte seas on hetkel väga populaarsed keskkonnad TikTok, YouTube ja Instagram, kus jagatakse peamiselt videoid ja pilte (Mascheron ja Ólafsson, 2014; Sukk ja Soo, 2018). Internet annab võimaluse anonüümselt postitada kellegi kohta halvustavaid kommentaare või piinlikke videoid ning see võib viia küberkiusamiseni (Luik, 2018). Näited kaitsekaartidest, mis võiksid selle valdkonna alla kuuluda, on *Joonisel 19*.

Joonis 19 Kaitsekaardid, mis aitavad kaasa DigCompi kompetentsi sisuloome arendamisele

Ohutuse all on DigComp mudelis silmas peetud eelkõige **seadmete, isikuandmete, tervise ning keskkonna kaitsmist**. Siia sobivad suurepäraselt küsimused, mis käsitlevad silmade tervist või ühe e-kirja saatmiseks vajaminevat energiamahtu (vt *Joonis 20*).



Joonis 20 Kaitsekaardid, mis aitavad kaasa DigCompi kompetentsi ohutus arendamisele

Viimane valdkond, mida DigComp käsitleb on **probleemilahendus**. Siin võivad heaks abimaterjaliks olla tegelaskaardid, mille abil saab noortega arutada erinevaid võimalusi, kuidas tehnoloogiat saab igapäevaellu rakendada (vt *Lisa 2*). On ka kaitsekaarte, mis annavad infot vabavara kohta, soovitavad erinevaid programme ja rakendusi ning käsitlevad füüsiliste artefaktide kaitsmist (vt *Joonis 21*).

Joonis 21 Kaitsekaardid, mis aitavad kaasa DigCompi kompetentsi probleemilahendus arendamisele

Kõige keerulisemaks ülesandeks mängu loomisel oli kaitsekaartide välja mõtlemine. 150 küsimuse sõnastamine valikvastustega küsimusteks ning neile vastuste kirjutamine nõnda, et mängu tagasisidestanud eksperdid tekstidega nõus oleks, osutus väga töömahukaks ülesandeks. *Lisas 3* on kirjas kõik kaitsekaartide küsimused, vastused ja selgitavad tekstid. Nüüd sõltub õpetajatest ja lapsevanematest, kui sügavuti teema aruteludega mängu käigus minnakse.

3 EMPIIRILISED UURINGUD:

MÄNGU TESTIMINE JA ARENDAMINE

Käesolevas, kolmandas magistritöö põhipeatükis, annan ülevaate protsessi nendest etappidest, mis seonduvad konkreetsemalt koostööga erinevate huvipooltega ning vastan kolmandale uurimisküsimusele, milleks oli „Kuidas suhestuvad erinevad huvipooled mängus käsitletavate veebiriskidega?“. Mängu loomine on kestnud 10 kuud, mille jooksul kohtusin erinevate ekspertidega, viisin läbi osalusvaatlusi, tegin külalistunde ning kogusin tagasisidet mängu sisule läbi elektrooniliste kanalite. Ülevaade nendest testimistest on leitav *Tabelis 3*.

*Tabel 3***.** Ülevaade mänguga läbi viidud testimistest

Kuupäev	**Testrühm**	**Arv**	**Lühikokkuvõte**
13. detsember 2018	Eksperdid: Birgy Lorenz, Aet Mikli ja Mirell Merirand	3	Tutvustasin mängu esimest prototüüpi ning tegime ühise testmängu. Vt ptk 3.2.
11. ja 13. veebruar 2019	Laagri kooli teised klassid (5 paralleeli)	120	Viisin läbi tunni, kus küsimused olid Powerpoint slaididena. Eesmärk testida küsimuste raskusastet ja laste eelistusi tegelaskaartide osas. Vt ptk 3.3.
22. märts 2019	Testimine perega	6	Testimise eesmärgiks oli teada saada, kuidas mängu dünaamika toimib koduses keskkonnas. Vt ptk 3.4.
25. ja 26. märts	Laagri roboringi nooremad rühmad (4 rühma)	55	Mängu dünaamika ja reeglite testimine. Kas lapsed saavad reeglitest aru ning kas suudavad iseseisvalt mängida. Vt ptk 3.5.
29. märtsil 2019	21. kooli kolmandad klassis	27	Mängu dünaamika ja reeglite testimine. Kas lapsed saavad reeglitest aru ning kas suudavad iseseisvalt mängida. Vt ptk 3.6.
Aprill 2019	Tagasiside ekspertidelt	6	Jagasin ekspertidega kaitsekaartide küsimusi ning palusin tagasiside ja kommentaare. Vt ptk 3.7.

Tavapärase struktuuriga teadustööde raamistuses on see peatükk **metodoloogia** ning **tulemuste** kombinatsioon. Selle asemel, et valida välja mõni konkreetne fookus-grupp, süvaintervjuud, vaatlus või ekspertintervjuud, mille põhjal oma töö see osa kirjutada, püüan ma anda ülevaate paljudest erinevatest väiksematest ja suurematest andmekogumis- ja analüüsimeetoditest tervikuna. See tähendab ühelt poolt detailsuse ja uuringute täpse kirjelduse määra vähendamist, aga loodetavasti annab laiahaardelise ülevaate kõigist nendest meetoditest ja huvipooltest, millest võib mänguarendajal kasu olla.

3.1 Esimesed katsetused - lapsed ideede testijatena

Mängu loomisel kasutasin **Demingi ringi** PDCA (Moen ja Norman, 2006) kohendatud tsüklit **planeeri-tegutse-testi-muuda**, mille käigus testisin mängu väga erinevate huvipooltega ning jooksvalt viisin sisse parandusi.

Esimene mänguversioon oli küllaltki algeline - puudusid tasemed ning kaitsekaardid olid ühepoolsed (ainult küsimused). Tegelaskaartidena kasutasin internetist leitud värvitavaid pilte inimestest. Esimene testimine mängul toimus koos enda pere lastega (viienda klassi noored) ja sõbraga. Esialgne plaan oli teha asi võimalikult lihtsaks – häkkeri rünnak vaheldumisi kaitsekaardi võtmise ja selle kohese käimisega. Põhimõtteliselt kaardimängu „Linnade põletamine“ loogika, kuigi siin oli lisaks õnnele (sobiva ikooniga kaitsekaart) vaja teadmisi, et kaitsekaardil olevale küsimusele õigesti vastata.

Mängijad teadsid vastuseid enamikele küsimustele, kuid mäng hakkas venima. Mängija enda võimalused mängu käiku mõjutada olid üsna väikesed. Pakis olid mõned kaitsekaardid, millel oli rohkem kui üks kaitseikoon, kuid see ei olnud piisav, sest neid kaitsekaarte tuli pakist välja väga harva.

Esialgsete katsete tulemusena jõudsin järeldusele, et mängu mehaanika ja selle elemendid (žetoonid, tegelaskaardid, kaitsekaardid, paha häkkeri täring) toimib, kuid mäng ei ole piisavalt tasakaalus. Sel hetkel oli mäng pigem juhusel põhinev õnnemäng (Caillois, 2001) ning ei pakkunud mängijatele piisavalt intellektuaalset väljakutset, mis võib viia kiire tüdimuseni (Koster, 2013).

Nende testimiste põhjal viisin mängu sisse järgmised muudatused:

- kaitsekaarte ei pea kohe mängima. Võib kuni viis kaitsekaarti kätte koguda ja soovitud ajal välja mängida;
- lisasin kaitsekaarte, millel rohkem kui üks kaitseikoon;
- lõin ikooni +**1**, mis tähendab, et koos selle kaitsekaardiga võib mängida samal käigul ühe täiendava kaitsekaardi.

Mängu tasakaalu testisin üksi mängu läbi mängides - katsetasin kui palju kaitsekaarte on vaja juhul, kui vastatakse kõik õigesti ning kui palju juhul, kui vastatakse 75% või 50% õigesti. Selle testimise tulemused on toodud *Tabelis 4*, kus on välja toodud kaitsekaartide arv, mida läks vaja antud tingimusel mängu võitmiseks.

Tabel 4. Mängu tasakaalu testimine

	100% (kõik vastused õiged)	**75% õigeid vastuseid (iga 4. vastus vale)**	**50% õigeid vastuseid (iga 2. vastus vale)**
1. mäng	17	35	70
2. mäng	23	42	98
3. mäng	13	29	-

Testimise tulemusena selgus, et sisse viidud muudatused aitasid kaasa õnne ja strateegia tasakaalu saavutamisele. Hiljem uuesti lastega testides oli tagasiside juba palju positiivsem ning lapsed ise soovisid mängu uuesti mängida.

3.2 Spetsiifilisem arendus - arutelud ekspertidega

Järgmine testimine toimus juba koos ekspertidega 13. detsembril 2018 ning seal tutvustasin oma prototüüpi **Birgy Lorenzile** (TTÜ küberkaitse magistriõppe lektor), **Aet Miklile** (Püha Johannese kooli haridustehnoloog) ning **Mirell Merirannale** (VHK küberkaitse õpetaja). Antud kohtumise eesmärk oli eelkõige saada sisendit küsimuste osas.

Küsimused põhjustasid mitmeid elavaid diskussioone. Näiteks Birgy Lorenz soovitas kindlasti keeleliselt osad küsimused lihtsamaks teha ning vältida eituse kasutamist pikemates lausetes, sest see muudab muu emakeelega õpilaste jaoks tekstidest aru saamise lihtsamaks. Mirell Merirand pakkus välja, et võiks olla gümnaasiumi jaoks eraldi

küsimused, kus oleks sees näiteks tumeveebi ja *sextinguga* seotud teemad. Ta ütles, et kasutaks sellist mängu meelsasti tunnis, kuid praegused küsimused võivad gümnaasiumiõpilaste jaoks liiga lihtsad olla. Üheks ideeks, mida välja pakuti oli täiendava kaarditüübi lisamine, et lisada strateegiale sügavust ning läbi selle muuta mäng sobivamaks gümnaasiumi tundides kasutamiseks.

Väga elav diskussioon tekkis teatud spetsiifiliste teemade ja küsimuste üle, näiteks kas laps peab vanematele oma parooli ütlema. Minu poolt oli argumendiks see, et lapsevanem vastutab lapse tegevuste üle internetis ning ilma kontrollita ei saa tegelikult vastutada. Lorenz ja Mikli tõid aga näiteid olukordadest, kus lapsel oli probleeme vanematega, kuid tal puudus internetis privaatsuse võimalus ning seetõttu oli väga raske ühendust võtta lasteabi või politseiga vanemate teadmata. Diskussiooni tulemusena jõudsime üksmeelele, et laps võib oma paroole öelda, kuid ta ei ole kohustatud seda tegema ning selle arutelu põhjal täiendasin olemasolevaid kaitsekaarte.

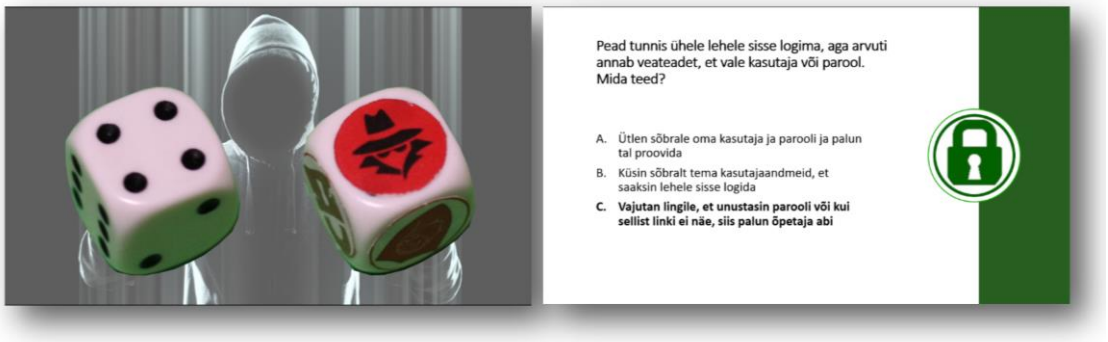
Üheks võimaluseks mängu raskusastme tõstmiseks on, kui ei loeta valikuid ette, vaid mängijad peavad vabas vormis küsimusele vastama. Tekkis küsimus, et kes hindab vastuste õigsust ja sellisel juhul peaks olema pädev mängujuht. Taoline formaat muudaks mängu kasutamise koolis keeruliseks – valikvastustega on võimalik kiirem tempo, sest tund kestab ainult 45 minutit ning see seab ajaliselt suuri piiranguid.

Sellel kohtumisel nägin esmakordselt mängu rolli vestluse algatajana. Mitmed küsimused andsid sisendit pikemale diskussioonile. Muidugi näitasid need vaidlused ka seda, kui keeruline on luua küsimusi koos vastustega, millega kõik eksperdid üksmeelel oleks. Kuna seadus ei reguleeri väga täpselt laste ja vanemate omavahelisi kohustusi ja õigusi küberruumis ning seetõttu on kasutusel päris erinevaid väärtus-raamistikke, mis lähtuvad raamistiku looja subjektiivsetest kogemustest.

Positiivne oli, et kõik osalejad jõudsid järeldusele, et kuna mäng on lihtne, saab seda kasutada mitmetel eri viisidel. Lorenz soovitas mõelda nelja mängijaga mängule, kus häkkeri rünnakut saab suunata kindla mängija vastu. Jõudsime ühisele järeldusele, et reeglid peaksid olema pigem suunavad ja ideid pakkuvad, kuid mitte ranged - see annab võimaluse mängu dünaamikat muuta vastavalt seltskonnale.

3.3 Kaitsekaartide küsimuste ja tegelaskaartide testimine koolitunnis

2019. aasta veebruaris viisin läbi proovitunnid Laagri kooli 2. klassides (viis paralleeli), mille eesmärgiks oli testida küsimuste raskust ning välja selgitada eelistatud tegelaskaardid.



Joonis 22 Powerpoint'i slaidid tunni jaoks

Valmistasin tundideks ette *Powerpoint*'i esitluse (vt *Joonis 22*) ning papist vastusekaardid A, B ja C tähtedega. Klassis moodustasin 5-6 liikmelised tiimid ning iga tiim sai kuus tegelaskaarti, paha häkkeri ikoonid ning vastusekaardid (vt *Joonis 23*) ning mängisime mängu lihtsustatud reeglite järgi. Kogu mäng oli ette valmistatud (küsimuste järjekord, täringuvisete tulemused) ning juhuslikkus tegelikult puudus, kuid õpilaste jaoks see mängurõõmu ei rikkunud.

Joonis 23 Koolitundides läbi viidud testimisel kasutatud mänguelemendid

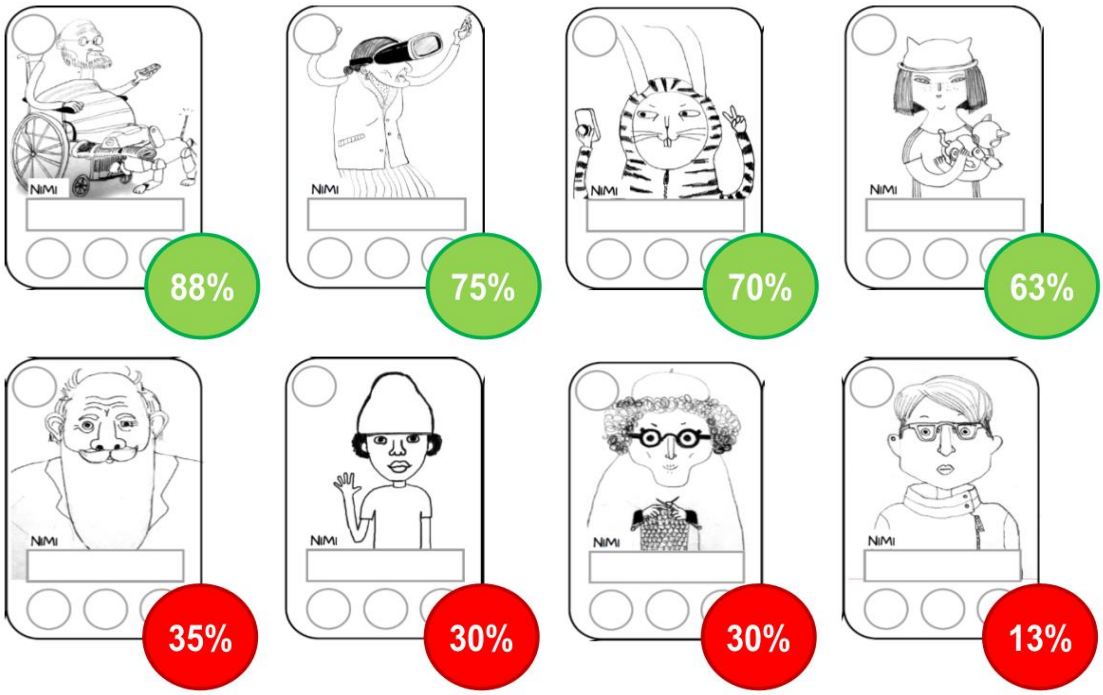
Antud katsetamise käigus selgus, et küsimused on noorte jaoks täiesti mõistetavad ning tiimiga suudeti üldjuhul õiged vastused anda. Mõned küsimused põhjustasid raskusi ning vajasid täiendavat arutelu.

Näiteks küsimusele "mis asi on piksel?" vastas ainult üks tiim õigesti. Kõik ülejäänud pakkusid, et tegu on välgulöögiga, mis on arvuti jaoks ohtlik. Siin küsimuses kasutasin teadlikult sarnaseid sõnatüvesid piksel/pikne, et segadust tekitada, aga ma ei eeldanud, et see nii hästi toimib. Peale vastuste selgumist seletasin lastele piksli tähenduse lahti ja mainisin, et seda ühikut kasutatakse näiteks ekraani suuruse ning pildi kvaliteedi iseloomustamiseks. Ühes klassis uuriti edasi, milline ekraani suurus on kõige parem, mis andis mulle võimaluse teema sügavamaks käsitluseks. Klasside tase oli erinev ja kui ühes 2. klassis vastasid kõik tiimid õigesti seitsmele küsimusele, siis näiteks paralleelklassis vastati õigesti üheteistkümne küsimuse puhul.

Teiseks keeruliseks küsimuseks õpilaste jaoks oli "miks ei tohi võõrastele öelda oma pangakaardi numbrit?". Ainult üks tiim vastas korrektselt, et võidakse oste teha ning pank võib kaardi kinni panna. Ülejäänud valisid kõik ka vale vastuse "nad võivad mu kaardinumbri ära häkkida", mis tegelikult on sisutühi fraas. Siin saime noortega arutada, et mida ikkagi täpselt tähendab häkkimine. Seda fraasi "ära häkkima" kasutatakse minu kogemusel õpilaste poolt väga palju ning see takistab tihti probleemi algpõhjuse tuvastamist. Kui mulle külalistunnis räägitakse, et minu mängukonto "häkiti", siis peale mõningast uurimist selgub, et pigem andis õpilane ise oma konto andmed mõnele tuttavale või on õpilane kasutanud kolmanda osapoole lehte/rakendust, lootuses saada endale mänguraha või mingeid mängus kasutatavaid artefakte. Selgitan seda teemat tihti oma külalistundides nii, et kui ise oma paroolid võõrale anda ja seetõttu konto tühjaks tehakse, siis sellel olukorral pole miskit tegemist häkkimisega, vaid on tegu "lollus hammustab tagumikust" situatsiooniga.

Tagasiside tunnile oli nii õpetaja kui õpilaste poolt väga positiivne ning kuna tunnid toimusid kahel eri päeval, oli võimalik vahepeal tegelaskaartide puhul teha vahetusi - eemaldasin testpakist vähem populaarsed tegelaskaardid ja Marja-Liisa joonistas uued tegelased katsetamiseks. Tegelaskaartide eelistuste hindamiseks sai iga tiim 12 tegelaskaarti ja pidi enne mängu algust nende 12 tegelaskaardi seast valima kuus

kasutajat, keda nad hakkasid mängu käigus kaitsma. Tegin fotod kõigist tehtud valikutest ning arvutasin iga tegelaskaardi kohta, et kui palju teda valiti laste poolt (vt *Joonis 24*).



Joonis 24 Tegelaskaartide populaarsus Laagri kooli 2. klasside õpilaste seas

100% tähendaks *Joonis 24* seda, et tegelane valiti iga kord, kui ta oli valikutes, ning 0% tähistab seda, et tegelaskaarti ei valitud ühelgi korral. Tegelaskaartide puhul kaardistus testimise käigus välja see, et noored eelistavad tegelasi, kes on aktiivsed või kus pildil on lugu. Testimise teiseks päevaks lisandusid tegelaskaartide pakki näiteks ratastoolis vanem mees ning VR prillidega vanem naine ja need on ühed populaarseimad tegelaskaardid olnud läbi kõigi testimiste.

Hiljem kaitsekaarte tasemete järgi liigitades võtsin arvesse erinevatel testimistel saadud tagasisidet ning täiendasin kaitsekaarte terminitega, et kõrgema taseme küsimused oleks paremini mõistetavad.

3.4 Mängu testimine perega

Järgmine testimine toimus ühe perega Kiili vallas nende kodus. Ema tegeleb seal ise arendavate raamatute ja õpimängude loomisega (vt *hop-play.com*) ning peres on kaks tütart - üks läheb sügisel kooli ning teine käib Tallinna kesklinna koolis kolmandas klassis. Lisaks kutsuti testimisõhtule kaks naabripoissi, kes mõlemad kolmanda klassi õpilased. Huvitava asjaoluna selgus kohapeal, et vanem peretütar oli mõned kuud tagasi osalenud minu turvalise interneti külalistunnis, kus me päris palju mängukaartidel olevaid teemasid läbi rääkisime.

Naabripoisse oodates palusin tüdrukutel värvida tegelaskaarte – see osa meeldis neile väga. Tüdrukud püüdsid jätkata värvimist mängu ajal, mis hakkas veidi protsessi segama. Samas testimine on piiratud ajal ning hiljem mängu endale soetades saab rahulikult tegeleda just soovitud tegevusega ning sellist rööprähklemist pole vaja teha.

Mängu mehaanika oli kõigile arusaadav. Kuna see oli viimane testimine, kus mul polnud kaitsekaardid tasemete järgi jaotatud, tekkis vahepeal olukordi, kus küsimused olid veidi rasked, eriti kõige noorema osaleja jaoks. Mängiti kahe tiimiga – õed naabripoiste vastu. Ema ja isa andsid vihjeid ning aitasid keerulisemate kaitsekaarti küsimustega. Mina mängujuhina veeretasin paha häkkeri täringuid ja küsisin küsimusi.

Noored said mängu loogikale kohe pihta ning tüdrukud tabasid üsna kiiresti ka parima strateegia. Poisid nii väga mängu ei süvenenud - nende jaoks tundus põnev pigem rääkida oma kogemusi küsimuste teemadel. Selgus, et mõlemal poisil on olnud hiljuti suured sekeldused sellega, et vanemad oma krediitkaardi andmed nende mobiilikontodele lisasid. Ühe poisi sõnul oli ta paari päevaga suutnud teha 400 eurose arve isale - seda infot kinnitas ka pereema, kellele poisi vanemad olid sellest olukorrast jutustanud.

Diskussiooni oli palju. Näiteks kui pakist tuli välja küsimus “mis on skämm?” siis tekkis pikk diskussioon mängus skämmamiste ning selle eetilisuse suhtes. Poiste meelest on mängus petmine mängu osa ning kui “mängija on nii rumal, et valet usub, siis võib talt asja ära võtta”. Tüdrukutel endil kokkupuudet pettustega mängus ei olnud, kuid ühe tüdruku sõnul oli ta sõbrannal mängus asjad võetud ning sõbranna oli väga kurb olnud.

Peab tõdema, et mäng lõpuni ei jõudnud (võitjat ei selgunud), sest paljude küsimustega tekkis elav arutelu, mis kestis 5-15 minutit. Mingi hetk pidid poisid koju minema ja kuigi tüdrukud olid täiesti valmis edasi mängima, pidin ise lahkuma. Kokkuvõtvalt võib öelda, et mängu elemendid toimisid oodatult. Tegelaskaardid tekitasid elevust panid noori lugusid välja mõtlema. Näiteks kui tegelaskaart seenelisega sai kohe uue pahavara žetooni, kui mängija eelmisel käigul oli tegelaskaardi puhastanud, siis tekkis arutelu, et miks ta kogu aeg viiruseid saab ning üks mängija pakkus välja, et viirus saatis talle karu video ja uudise, et metsas on näljane karu. Tegelane hakkas kartma, et äkki karu lähedal ja vajutas tundmatule lingile.

Hoolimata sellest, et paha häkker jäi seekord alistamata, oli test igati edukas – vanemad ja lapsed suhtlesid väga aktiivselt ning kõigil osavõtjatel oli tugev motivatsioon mängu korrata esimesel võimalusel.

3.5 Mängu testimine Laagri Roboringis

Peale eelmises peatükis kirjeldatud testimist muutsin kaitsekaarte. Jagasin kaitsekaardid kolmeks erinevaks tasemeks ning muutsin veidi kaitsekaartide märgistusi, suurendades kaitsekaartide osa pakis, kus on kaks või enam kaitsemärgist. Järgmised testimised toimusid Laagri Roboringis esimese kuni kolmanda klassi noorte seas. Testimised toimusid kahel päeval (25. ja 26. märtsil), kui asendasin robootikahuviringi juhendajat tema huvitundides. Lapsevanemetele oli teada antud, et noored sel päeval robootika asemel tegelevad turvalise interneti teemade käsitlemisega. Mõlemal päeval osales testimises kaks rühma – esimeses rühmas osalevad esimeste klasside õpilased ning see huvitund kestab 60 minutit. Teises rühmas käivad teiste ja kolmandate klasside õpilased ning selle huvitunni kestvus on 90 minutit. Kõikidesse rühmadesse on registreerunud 16 õpilast, kuid Roboringi juhendaja sõnul käib tavapäraselt kohal 12-14 õpilast.

Valmistasin ette neli mängukomplekti – igas komplektis 12 tegelaskaarti, 36 pahavara žetooni ning täringud. Kaitsekaarte oli mul sellel testimisel kaks täiskomplekti – mõlemas komplektis olid kaitsekaardid kolmeks tasemeks jaotatud ning plaan oli alguses anda testimiseks esimese ja teise taseme kaitsekaardid.

Esimeses rühmas oli 13 õpilast. Jagasin nad kolmeks - kaks seltskonda mängisid 2+2 paaridena ning ühe laudkonna moodustasid 2+2+1. Kuna see oli esimene kord, kus pidin

nii suurele seltskonnale korraga mängu reegleid selgitama, oli algus veidi kaootiline. Suur viga oli see, et ma ei keelanud laual olevaid mängu elemente puutuda ja noorte tähelepanu hajus reeglite selgitamise ajal. Kui ütlesin, et nüüd võib mängima hakata, hakkasid kõik entusiastlikult tegutsema. Klassis ringi liikudes jäi küll silma, et iga rühm mängib eri reeglite järgi, kuid kuna kõik lapsed veerisid kõva häälega tekste ja püüdsid vastata küsimustele, siis tegelikult mängu reeglid ei olnudki olulised. Mäng on üksnes vahend, et noori motiveerida infot otsima ja omandama.

Umbes 10 minutit pärast mängimise algust tõstis üks poiss klassis käe ja uuris, et mis on mängu eesmärk ja kuidas mängu võita. Veidi oli piinlik, et unustasin sellise olulise info edastamata kohe alguses, kuid teiselt poolt on see väga hea näide, et mängu elemendid panevad lapsed aktiivselt tegutsema olukorras, kus reeglid on segased ning eesmärki pole öeldud. Üks seltskond lõpetas umbes 40 minutiga esimese mängu – neile andsin kolmanda taseme küsimused ning selline taseme tõus tekitas noortes nii palju elevust, et vaja oli kõva häälega sõpradele teise klassi otsa hüüda “Meil on kolmas tase!”, mis näitab, et kaitsekaartide jagamine tasemete järgi oli õigustatud ning see tekitab noortes saavutusrõõmu.

Aktiivne mäng kestis kuni 55 minutini – seejärel palusin mängu lõpetada ning mängu kokku panna. Noored küll palusid, et äkki saaks edasi mängida, kuid järgmine rühm oli ukse taga ning mul polnud võimalik mänguaega pikendada.

Järgmise grupiga oli mul tund veidi teistmoodi üles ehitatud, sest neil oli aega 90 minutit. Lasin neil esmalt valida ühe tegelase ning palusin tegelase ära värvida ning täita tegelaskaardi tagaküljel olev ankeet. Ülesanne meeldis kõigile lastele väga ning nad olid nõus jagama oma pilte värvitud tegelaskaartidest magistritöö lugejatega (vt *Joonis 25*).

Joonis 25 Laagri Roboringis toimunud testimisel värvisid lapsed tegelaskaarte

Teisel päeval kordasin sama süsteemi – esimene rühm mängis ning teine rühm värvis, täitis tegelaskaartide taga olevaid ankeete ning seejärel mängis. Kuigi muutusin reeglite seletamisega osavamaks iga korraga, siis ikkagi oli üsna palju vabas vormis tõlgendamist ning igal laudkonnal oli veidi erinev arusaam reeglitest, aga see asjaolu ei seganud mängimast.

Huvitav oli see, et teisipäeval teine rühm koosnes ainult Laagri kooli 2. klasside õpilastest, kes olid klassis *Powerpoint*'i põhist versiooni juba mänginud. Nad olid kõik väga entusiastlikud, et saavad jälle mängida ning kuna nende jaoks oli mängu loogika juba selge ning osad küsimused tuttavad, läks mäng tempokamalt kui teistel gruppidel ja üks laudkond jõudis kõigi kolme taseme pakkidega mängida.

Laste entusiasm mängu osas oli suur – vähemalt 2-3 last igast grupist uuris, et kust poest seda mängu ostma saaks minna ning nad isegi ei saanud aru, et tegu prototüübiga, kus kujundused küllaltki algelised. Järelikult oli sisu nende jaoks niivõrd köitev, et üldisele esteetikale ei pööratud eriti tähelepanu.

Joonis 26 Erinevad mänguga seotud tegevused

Sellelt testimiselt sain väga palju kasulikku tagasisidet noortelt. Tasemete kasutuselevõtt oli igati õigustatud – see motiveerib noori keerulisemate küsimustega tegelema. See testimine tõi ka välja selle, kui paljusid erinevaid oskusi mäng arendab - piltide värvimine aitab kaasa **peenmotoorika ning loovuse arendamisele**, tegelaskaartide tagakülgede ankeetide täitmine aitab **parandada kirjutamisoskust**, tekstide lugemine kõva häälega ning nende mõistmine on selgelt **funktsionaalse lugemisoskuse valdkond** ning eduka strateegia valik nõuab arusaama **tõenäosusteooriast ja matemaatilisest loogikast**. *Joonisel 26* on visuaalselt välja toodud mõned neist tegevustest.

3.6 Mängu testimine Tallinna 21. Koolis

29. märtsil 2019 viisin läbi testimise Tallinna 21. Kooli kahes kolmandas klassis. Tegu oli 45-minutiliste koolitundidega, mis tunniplaani järgi oleks pidanud noortel robootikatund olema, kuid õpetajal oli ülikooli õppenädal ning ta palus minul end asendada – leppisime kokku, et selles tunnis tegelen mängu testimisega.

Olen sügisel ühe asendustunni nendele klassidele teinud, kui tegin tollal neile oma tavapärase turvalise interneti külalistunni. Ehk noortel oli olemas teatud kogus infot mängus olevate teemade kohta. Väga huvitav oli minu jaoks erinevus noorte esialgse

entusiasmi osas (mida ma subjektiivselt tunnetasin). Laagri Roboringis asendan ma õpetajat sageli, korraldan piirkonnas erinevaid üritusi ja käin kaasas saatjana võistlustel ning tundub, et mul on kogunenenud noorte seas teatav usalduskrediit. Noored on alati väga entusiastlikud minu uute ideede osas. Tallinna 21. Koolis olen ma laste jaoks lihtsalt üks võõras inimene, kes vahel harva asendab nende õpetajat ning lapsed suhtuvad pigem ettevaatlikult minu tegemistesse ning tunni alguses olid osalejad pigem passiivsed ning ettevaatlikud kui aktiivsed ning entusiastlikud.

Passiivses klassis on reeglite seletamine märksa lihtsam - keegi ei avanud materjale enne kui ütlesin, et nüüd võib hakata tegelaskaarte valima. Klassis oli 4 laudkonda - esimeses tunnis oli 14 õpilast (laudades 4+4+4+2 õpilast) ja teises tunnis 13 õpilast (laudades 4+4+2+3 õpilast). Tegelaskaardid said kiiresti jaotatud - kõige rohkem elevust põhjustas taaskord VR prillidega vanaema ja *Fortnite*'i mängiv ema.

Kui esimesed viis minutit oli klassis üsna rahulik (võrreldes Laagris toimunud testimisega), siis umbes 20. minutiks oli mäng täies hoos ja kuulsin, kuidas tegelaskaartidele lugusid juurde mõeldi. See ajaraam kehtis mõlema testtunni kohta.

Esimeses tunnis jäi silma üks laudkond, kus üks osaleja ütles, et kogu see mäng täiesti mõttetu, sest ta teab internetist kõike. Jälgisin selles lauas toimuvat eriti tähelepanelikult. Dünaamika kujunes nii, et, et see n-ö kõiketeadja osaleja ei lasknud oma tiimikaaslasel vastata, vaid vastas alati ise ning umbes pooled küsimused neist valesti. Tiimikaaslane oli päris kuri, sest tema pakutud vastused oli päris sagedasti korrektsed. Peale esimest mängu rääkisin nendega, kuidas tiimitöös on oluline, et kõik tiimi liikmed saavad osaleda võrdselt ning teisel mängul vastati kordamööda ja tulemus oli märgatavalt parem. Kahjuks tund lõppes enne, kui teise mängu lõpp kätte jõudis, kuid see on hea näide, kuidas mängu abil saab noortele tiimitööd õpetada.

Teises tunnis tekkis probleem, kui ühte poissi keegi ei tahtnud oma tiimi võtta. See oli keeruline olukord, sest esialgu istuti nii, et igas lauas oli neli õpilast ja see üksik poiss jäi üle. Kuna ma noori ei tundnud ja ei teadnud enne tunni algust, et mitu õpilast kohale täpselt tuleb, ei osanud ma sellist olukorda ette näha. Õnneks tekkis olukord, kus üks laudkond noormehi hakkas toimetama ilma minu loata ning see andis mul võimaluse laudkonna kaheks jagada nii, et lauda jäid kaks poissi ja kaks poissi läksid sinna eraldi

istuva poisi lauda. Kui ma oleksin klassijuhataja rollis sellist olukorda kogenud, tekiks soov uurida olukorda põhjalikumalt – selline tõrjumine võib olla märk suuremast probleemist, kuid kuna asi lahenes ja tunni käigus kolm poissi sõbralikult mängisid, ei pidanud ma vajalikuks sel korral põhjalikumalt sekkuda.

Joonis 27 Mängu testimine Tallinna 21. Koolis

Joonisel 27 oleval pildil on laudkond Tallinna 21. Kooli testtunnist, kellel mängu käigus mingeid raskusi ei tekkinud ning kelle sõnul võiks seda mängu edaspidi mõnes tunnis mängida. Kõik pildid, mis siia testimistelt lisan, on tehtud laste nõusolekul ning täiendavalt on küsitud luba pildi avaldamiseks vanematelt. Paar laudkonda ei soovinud, et neid fotole jäädvustaksin ning nendest laudadest ma pilte ei teinud.

See katsetamine näitas taaskord, et tasemed on noorte jaoks olulised. Sain kinnituse oma kahtlusele, et päris originaalkujul siiski mängu tunnis läbi viia on keeruline. 45 minutit on veidi liiga lühike aeg, et mängulaud üles panna, mängida ja kõik ära koristada (viimase rühma puhul lasin neil mängida tunni lõpuni ja koristasin hiljem ise). Seega pean tegema õpetajate jaoks *Powerpoint*'i põhised küsimused ja lihtsustatud reeglid, mille abil läheks tund märgatavalt sujuvamalt.

3.7 Tagasiside ekspertidelt

Mäng valmib koostöös Telia Eesti AS-ga, mis toetab mängu välja andmist ning seetõttu kutsuti mind ka Telia lauamänguritele asja tutvustama. Kohal oli viis inimest, kellest enamik töötab IKT-ga seotud valdkonnas. Katsetasime seal mängu nelja erineva mängijaga - igal mängijal oli tegelaste komplekt ning enne paha häkkeri rünnaku veeretamist sai mängija valida, millisele teisele mängijale ta pahavara veeretab. See pani mängijaid ka aktiivsemalt jälgima teiste mängijate tegelaskaarte ja keerukam strateegia muutis mängu täiskasvanud lauamängurite jaoks põnevamaks.

Kaitsekaartide küsimused põhjustasid taaskord väga elavat (ja kohati ülimalt humoorikat) vestlust ning soovitati teha korporatiivne versioon, mida saaks äriklientidele kinkida. See idee tundus täitsa põnev, sest mängijate jutust sain aru, et nende klientidel on sarnased probleemid, mis korduvad sagedasti. Kuigi algselt vastati nii mõnelegi kaitsekaardil olevale küsimusele valesti, siis diskussiooni käigus jõuti kõigil juhtudel järeldusele, et vastusevariant kaitsekaardil on õige. Näiteks küsimusega „paned endale uue profiilipildi, mis sulle väga meeldib, aga keegi ei laigi seda tunni jooksul. Mida teed?“ tekkis arutelu, et miks ei võiks sõpradele kirja saata ja uurida, et mis pildil viga oli. Kuid peale lühikest arutelu olid kõik nõus, et see oleks veider, kui nad iga postituse kohta, mida nad meeldivaks ei märgi, hakkaksid tuttavatelt päringuid saama.

Lisaks mängu mehaanika testimisele püüdsin koguda võimalikult palju tagasisidet kaitsekaartide küsimustele. Kaitsekaartidel olevad küsimused on üle vaadatud mitmete ekspertide poolt, kes andsid väga sisulist ja väärtuslikku sisendit. Kaitsekaartidele on oma tagasiside andnud näiteks nutitunni projekti eestvedaja, Pelgulinna kooli IT-arendusjuht ning TTÜ küberkaitse lektor Birgy Lorenz, Telia Eesti turvaintsidentide valdkonnajuht Aare Kirna, veebikonstaabel Andero Sepp, haridustehnoloog Aet Mikli, Tartu Ülikooli Eetikakeskuse projektijuht Õnne Allaje ning Google’is töötanud arendusinsener Andres Soolo. Teoreetiliste allikate osas sain väga palju kasulikku sisendit oma juhendajalt Tartu Ülikooli sotsiaalmeedia lektorilt Maria Murumaa-Mengelilt ning oma retsensendilt Andra Siibakult.

Korduvamad teemad tagasisides on olnud järgmised:

- ***Häkkerite temaatika:*** hetkel on häkkeritel halb maine ühiskonnas – tihti pannakse võrdusmärk häkkeri ja kräkkeri vahele. Tekkis mitu diskussiooni, kas ei peaks kräkkeri mõiste täiendavalt mängijateni tooma. See läheks sihtrühma arvestades keeruliseks ja kõik olid peale diskussiooni nõus, et see oleks suur edasiminek, kui inimesed teaks, et häkker on neutraalne termin arvutist sügavamalt huvitatud inimese kohta ning häid ehk eetilisi häkkereid on väga vaja.
- ***Liiga konkreetsed juhtumid:*** algselt oli kaitsekaartidel näiteks Momo teema (Pau, 2018), mis oli aktuaalne eelmisel sügisel, kuid enne seda oli Sinivaala nimeline enesetapumäng ning kes teab, mis algaval sügisel tuleb. Muutsin päris palju kaitsekaardidel olevaid küsimusi soovituste põhjal abstraktsemaks, et mängu aktuaalsus säiliks kauem.
- ***Keerulised teemad*:** raske oli leida tasakaalu keeruliste teemade juures. Näiteks kas ja kuidas käsitleda küberkiusamiste teemasid ning kas peaks lastele suunatud mängus olema sõna "seksima" kasutusel. Nende teemade puhul püüdsin leida tasakaalupunkti - ühelt poolt kindlasti ei soovi suunata noori info poole, mis neile kahju võib teha ja avamata uksi nende jaoks avada, teiselt poolt ei näe mõtet teha n-ö steriilset mängu, kus kõik veidigi keerulisemad teemad on välja võetud ja räägitakse liialt üldist ja pinnapealset juttu.
- ***Tehnilised küsimused:*** ekspertidel puudub üksmeel selles osas, milline on parim parool, kui ohtlik on VPN jne. Lisaks kipub olema nii, et see, mis 99-l juhul toimib, sajandal korral ei tööta. Oli paras väljakutse teha sisulisi küsimusi valikvastustega, mille osas kõik kaasatud eksperdid ühel meelel oleks.
- ***Politsei ja täiskasvanute kaasamine:*** taaskord teema, mille osas puudub üksmeel. Millal peaks noor pöörduma täiskasvanu poole ja millal on juba politsei poole pöördumine õigustatud. Ühelt poolt pole mõtet koormata politseid probleemidega, mida vanemate või õpetajate kaasabil on lihtsam lahendada. Teiselt poolt kommenteeris veebikonstaabel Andero Sepp oma tagasisides kaitsekaardile küsimusega „42 Millal pöörduda veebikonstaabli poole?", et tihti ei ole algne lahendus lõplik ning probleem jõuab ikkagi politsei kätte - seega võibolla oleks eelinfo hea ka juhul, kui esialgu suudetakse probleem koolis või kodus ära lahendada.

Mängu arenduses oli oluline roll testimisel ja tagasisidel. Taaskord polnud tegemist lineaarse protsessiga, vaid tsükliga plaani-tegutse-testi-muuda. Olen tänulik kõigile, kes andsid tagasisidet. See etapp õpetas mulle uusi teadmisi võrguarhitektuurist, masinõppest, küpsiste failidest jpm ja kuulsin lugusid, mida saan kasutada koolitustel. Lisaks andsid kõik diskussioonid mulle uusi vaatenurki, mida kindlasti tulevikus jagan õpetajate ning lapsevanematega.

3.8 Mängu teema ja sisuga seonduvaid tähelepanekuid

Kokkuvõtvalt võib testimiste ja tagasiside tulemusena väita, et kaitsekaartidel olevad küsimused käsitlevad aktuaalseid teemasid nii laste kui täiskasvanute jaoks. Mõned teemad võivad tekitada teatud ebamugavust (näiteks küsimus "mida teed, kui keegi küsib, kas sa mängult seksida tahad?"), kuid kuna noored puutuvad väga varakult selliste teemadega kokku, siis on oluline, et teatakse, kuidas adekvaatselt käituda taolistes situatsioonides.

Testimiste jooksul selgus, et laste jaoks on terminid piksel ja manus võõrad, kuid peale selgitust suudeti mõiste konteksti asetada. Tänu tasemete loomisele on võimalik mängides alustada lihtsate küsimustega ning liikuda keerulisemate teadmiste omandamise juurde. Osad tekstid olid esimeste klassi lastele küllaltki keerulised lugemiseks, kuid alla ei antud ja veeriti nii kaua kuni küsimusest aru saadi. Arvestades, et kaitsekaartidel olevad küsimused ja vastused on kokku *ca* 37 lehekülge A4 teksti, on see suur tekstikogus algklassilaste jaoks. Segadust põhjustas täiskasvanutega, et küsimuste vastused on märgitud laste vaatenurka silmas pidades. Kahjuks pole sellist mängu võimalik luua nii, et samad kaitsekaardid sobiksid kõigile ning mängu "Häkkerite lahing" esmaseks sihtrühmaks on algklassides ja põhikoolis käivad lapsed koos peredega.

Tegelaskaartidel kujutatu on saanud kõigil testimistel väga positiivse tagasiside ning nende kasutuselevõtt on ennast õigustanud. Samuti on testimised näidanud, et paha häkkeri agentsust väljendavad artefaktid on mängija jaoks üheselt mõistetavad ning aitavad kaasa loo jutustamisele. Kuigi olen jõudnud järeldusele, et lauamäng on nagu Tallinna linn, mis kunagi lõplikult valmis ei saa, siis olen jõudnud punkti, kus hindan mängu funktsionaalsust piisavaks, et see suudab soovitud õpiväljundid täita ning selle saab edasi küljendamisse ja trükki suunata.

4 JÄRELDUSED JA DISKUSSIOON

Esmalt vastan selles peatükis lühidalt ja kompaktselt töö alguses esitatud uurimisküsimustele ning seejärel liigun edasi laiema diskussiooni juurde..

Millised teemad peavad olema internetiohte käsitlevas õpimängus kajastatud, et see aitaks kõige paremini ennetada erinevaid riske, millega noored digimaailmas kokku puutuvad?

Kuna noorte nutiseadmete kasutamine algab väga varakult (Vinter, 2013; OECD, 2015) ning tarbitakse ja jagatakse väga erinevat sisu (Macheroni ja Ólafsson, 2014; Sukk ja Soo, 2018), siis on oluline, et kaetud oleks võimalikult lai hulk teemasid. Ükskõik, kas jagame need teemad sisu, käitumise ja suhetega seotud riskideks (Livingstone jt, 2014), andmetega, reputatsiooniga, tervisega, vabadusega seotud riskideks ja pettusteks (Lorenz, 2017) või siis pigem kasutada DigComp digipädevuste liigitust (Kluzer ja Pujol Priego, 2018) peavad kõik kategooriad kaetud olema.

Paberkandjal õpimängu loomise puhul osutus oluliseks teemaks mängule sobiva abstraktsus-astme leidmine – liiga konkreetne teemade käsitlus võib kaasa tuua riski, et mängu sisu aegub liiga kiiresti, samas liiga abstraktsete küsimuste puhul ei suuda noored leida seost oma tegevusega ning muutub keeruliseks valikvastuste loomine.

Milliseid mängudisaini universaalseid elemente ja aspekte saab rakendada interneti-teemalise laumängu loomisel?

Mänguloome protsess on oma olemuselt sarnane teiste arendusprojektidega, kus esialgu on vajalik olukorra kaardistamine ning eesmärkide seadmine ning sealt edasi juba toote pidev täiendamine, mida võib teha näiteks Demingi tsükli (Moen ja Norman, 2006) plaani-tegutse-testi-muuda baasil. Selline protsess ei ole lineaarne, vaid tuleb

kombineerida empiirilisi tegevusi vaheldumisi uute andmete otsimise ning vajaliku teooria täiendamisega.

Käesoleva õpimängu loomisel kasutasin tavamängudes kasutusel olevaid artefakte - kaardid, žetoonid, täringud - sidudes need ära mängu temaatikaga. Mängu mehaanikas leidsin läbi testimiste tasakaalu juhuslikkuse, strateegia ja teadmiste vahel pidades silmas Kiili jt (2012) poolt antud soovitust, et tagasiside peab olema kohene, et tekiks soovitud voog mängija teadvuses, mis viib uute teadmiste omandamiseni.

Kuidas suhestuvad erinevad huvipooled mängus käsitletavate veebiriskidega?

Käesoleva magistritöö empiirilises osas viisin läbi erinevaid testimisi ning palusin mitmetelt ekspertidelt tagasisidet küsimustele kaitsekaartidel. Üldjoontes oldi nõus, et mängus tõstatuvad teemad on aktuaalsed ning arutelu nende üle on vajalik.

Algklassides käivate laste jaoks pakkusid küsimused ja vastused ilmselget huvi - mõned teemad osutusid küll veidi keerulisemateks ning puudus vajaminev sõnavara, kuid seegi on vajalik, et toimuks uute teadmiste omandamine.

Ekspertide sisend oli väga põhjalik ning paljud küsimused andsid alust pikemaks diskussiooniks. Tihti muutuvad internetiga seoses antud nõuanded ja uuringute tulemused võivad olla üksteisele vastu käivad ning seetõttu mõne vastuse puhul oli vajalik teatav kompromiss.

4.1 Enesereflеksioonil ja protsessi analüüsil põhinev diskussioon

Käesoleva töö tulemusena valminud mäng „Häkkerite lahing“ (vt *Joonis 28*) on digipädevusi ning küberhügieeni alaseid teadmisi arendav mäng, mille välja töötamisel kombineerisin oma praktilisi kogemusi turvalise interneti külalisõpetajana ning erinevaid akadeemilisi käsitlusi. Pidasin siin töös oluliseks tuua välja võimalikult palju erinevaid akadeemilisi vaatenurki, sest see peegeldab hästi ühiskonnas toimuvat – puudub ühene arusaam digivahendite rollist meie eludes ning meedia ning koolituste kaudu jõuab lapsevanemate ning õpetajateni väga palju infot, mis tekitab segadust. Seetõttu kasutasin küsimuste sisendina nii Livingstone, Kirwil, Ponte ja Staksrudi (2014), Lorenzi (2017) loodud riskide kategooriaid ja Kluzeri ja Pujol Priego (2018) välja pakutud DigComp raamistikku, sest selline erinevate riskide liigituste kasutamine mängukaartide loomisel

annab kindlustunde, et kõik olulised teemad on kaetud, kuna ekspertide nägemus sobivatest käitumispraktikatest on väga erinev.

Joonis 28 Mängu „Häkkerite lahing“ pakendi ideekavand

Üheks näiteks on eelpool kirjeldatud olukord, kus erinevatel ekspertidel oli erinev nägemus, milliste probleemide korral on asjakohane pöörduda politsei poole. Teine väga hea näide on laste ja seksiga seotud teemad – üks ekspert, kellega konsulteerisin kaitsekaartide küsimuste osas, arvas, et selliseid teemasid ei peaks lastega üldse käsitlema, sest tegu on väga tundliku teemaga ning on olemas oht, et see tekitab lapsevanemates või õpetajates ebamugavustunnet ning negatiivseid tundeid mängu osas. Teine ekspert jälle arvas, et antud teemat on mängus liiga vähe käsitletud ning pigem peaks olema selle teemalisi küsimusi rohkem. Tasakaalu leidmine taolistes olukordades oli väga keeruline ja mitmel korral pidin tegema otsused isikliku kogemuse ja tunnetuse baasil.

Selle mängu eripäraks on kindlasti suur avalik huvi. Hetkel on väga vähe õppematerjale, mille põhjal noortele turvalist internetikäitumist ja digipädevusi õpetada ning seetõttu oli väga lihtne kaasata valdkonna eksperte, sest kõigi sooviks on, et see mäng oleks võimalikult aktuaalne ning hariv. Teiselt poolt tõi selline suur huvi kaasa surve – sain väga palju ettepanekuid, mis minu ideega ei haakunud ning läks vaja küllaltki palju

diplomaatiat, et põhjendada otsuseid nii, et kaasatud eksperdid tunneks, et nende sisend on oluline, kuid samas püüdsin mitte teha liiga suuri kompromisse oma nägemusega.

Siinkohal võib esitada küsimuse, et kui on olemas avalik huvi, siis miks ma mängu välja andmist ei püüdnud rahastada läbi mõne riikliku toetusmeetme. See on teadlik otsus, sest olles ise väga aktiivselt olnud seotud kolmanda sektori tegevustega alates aastast 2002, tean väga hästi riske, mis kaasnevad selliste toetusmeetmetega tihti kaasneb suur aruandluskohustus ja kaasnevad piirangud toote hilisema müügiga seoses, seetõttu eelistan ma pigem ühisrahastust ja koostööd erasektoriga. Kui nendest kanalitest vajalikku finantseeringut ei õnnestu saada, võib see märk olla sellest, et sellisel kujul toodet/teenust turul vaja ei ole. Käesoleva projekti puhul on huvi täiesti olemas – 125 hooandjat toetasid projekti 4138 euroga ning leidsin Telia Eesti AS näol väga asjatundliku koostööpartneri erasektorist.

Hooandja projekt lõppes edukalt, kuid omamoodi tähendusrikas on see, et pidime projekti lõpu lükkama Hooandjas edasi kolme päeva võrra, kuna kaks päeva enne projekti esialgset plaanitud lõppu sattus veebikeskkond küberrünnaku ohvriks ning lehe töö oli mitu päeva häiritud. Lahing heade ja halbade häkkerite vahel käib ning seetõttu on head küberhügieeni alased teadmised vajalikud igale inimesele, kes internetti külastab.

Kui võrrelda mängu „Häkkerite lahing“ olemasolevate mängudega „Suurim julgus“ ning „Cybersec juhtumid“, siis minu loodud eripäraks on selle mängulisus. „Suurima julguse“ mängu puhul on vaja mängujuhti ning see sobib pigem vanemale kooliastmele. Selle mängu puhul on vaja ka suuremat hulka lapsi, sest üksi või kahekesi ei teki piisavalt diskussiooni. „Cybersec juhtumid“ on pigem sobiv mäng gümnaasiumiastmele või tudengitele ning see nõuab suuremat huvi küberteemade vastu. „Häkkerite lahing“ on sobiv just algklassilastele ning seda saab mängida nii üksi kui suurema seltskonnaga. Lisaks on mängul mitmeid artefakte (tegelaskaardid, häkkeri täringud, pahavara žetoonid, kaitsekaardid erinevate tasemetega), mis lisavad strateegiale sügavust ja loovad vajalikku põnevust, et õppimine ja lõbu oleksid tasakaalus (Arnab jt, 2015). Tasemed ja mängijate arv muudavad mängu keerukust, mis aitab kaasa sellele, et iga mängija saaks mängida vastavalt oma võimetele (Kiili, Lainema, de Freitas ja Arnab 2014).

Mängijate internetialaste teadmiste kohta mängu loomise protsessis mingeid suuri üllatusi ei tulnud, sest tegelen selle teemaga igapäevaselt ja mul on väga palju sisendit õpilastelt seoses nende murede ja rõõmudega digimaailmas. Suurem õppimiskurv avaldus mängu dünaamika ja artefaktide loomise protsessis. Väga huvitav oli jälgida, kuidas näiteks noorte eelistus oli küllaltki sarnane tegelaskaartide suhtes – eelistades alati pigem aktiivset ja omapärast tegelast passiivsele ja tavapärasele.

Tasemete teke mängus oli teema, mida ma alguses üldse ei osanud planeerida, kuigi selline tasemete kasutamine on mängudes üsna tavapärane. Kuna esimene ideekavand oli liiga keeruline, siis teise idee puhul püüdsin asju liiga lihtsustatud tasemel esialgu hoida. Hiljem võtsin kasutusele tasemed eelkõige seetõttu, et soovisin küsimusi jagada kategooriatesse. Mängijate motivatsiooni kasv ja suurem ind keerulistele küsimustele vastata, kui need kõrgemale tasemele kuulusid, oli ootamatuks lisaboonuseks.

Väljatoomist tasub ka seik, kuidas päevapoliitiline olukord tekitas dilemmasid mängu disainiprotsessis. Kasutan mängus n-ö hea häkkeri ja paha häkkeri vastandumist loona ning tundus väga loogiline visuaalis kasutada valget ja musta kübarat – terminid *white-hat hacker* ehk eetiline häkker ning *black-hat hacker* ehk kriminaalne häkker on kasutusel olnud IT ekspertide ja huviliste seas väga pikalt. Seoses 2019. aasta riigikogu valimistega ning ühiskonnas tekkinud diskussiooni üle Eesti Konservatiivse Rahvaerakonna (EKRE) parketikõlbulikkuse üle valitsuse moodustamise kontekstis omandas must kaabu, mida EKRE juhtkonna liikmed armastavad kanda, omaette looga sümboliks. Korraks tekkis mure, et kas selline võimalik seostamine päevapoliitikaga ei too kaasa mingeid riske mängu turule toomise osaks, kuid praeguseks hetkeks pole need riskid realiseerunud.

Mäng „Häkkerite lahing“ on väga mitmekülgne tööriist lastele digipädevuste õpetamiseks, kuid see ei lahenda ära kõiki noorte küberhügieeniga seotud kitsaskohti. Plaan on jätkata erinevate tööriistade loomist õpetajate ning lapsevanemate jaoks. Suvel valmivad mängu baasil tunnikavad ja õppematerjalid õpetajatele ning plaanis on käsile võtta nutiaabitsa loomine, mis aitaks lastel ette valmistuda kooliks, samal ajal õpetades algteadmisi nutiseadmete ja interneti kohta.

4.2 Soovitused õpimängu loomiseks

Lõpetuseks panen siia kirja mõned nõuanded neile, kellel on soov teha õpimängu, kuid päris täpselt ei tea, kuidas alustada.

Mängi erinevaid lauamänge

Enne kui alustad oma lauamängu loomist, mängi teiste loodud mänge. See annab tunnetuse ja ideid, et milliseid artefakte soovid kasutada ja millised reeglid võiksid olla. Minu enda jaoks olid inspiratsiooniks “Pandemic”, “Discworld”, “Meie Eesti”, “Riigimehed”, “Monopoly” ja “30 to Mars”. Iga mängu puhul mõtle, mis reeglid, strateegia ja artefaktid muudavad selle mängu sinu jaoks põnevaks.

Kaardista olemasolevad valdkonna õpimängud

Õpimänge on tegelikult palju, kuid väga paljud neist ei saa kunagi suuremat avalikkuse tähelepanu. Püüa leida võimalikult palju näiteid ja tööta need läbi. Õpimängude kohta saab kõige paremini infot eriala teemagruppidest sotsiaalmeedias või valdkonna ekspertidelt, et milliseid mängulised tööriistad on neil erakogudes olemas.

Ära jää teiste ideedesse kinni

Nüüd, kus oled mänginud toredaid lauamänge ning tutvunud suure hulga põnevate õpimängudega, on oluline mitte kinni jääda olemasoleva mängu strateegiasse või ülesehitusse. Mängu arendamine on loominguline protsess ning seda ei saa teha valemiga, et kui võtan 25% strateegiast siit ning 75% artefaktidest siit, siis kindlalt on tulemuseks üks eriti hea mäng.

Tee prototüüp kohe

Kui sul on esimene idee olemas, loo kohe prototüüp. Isegi kui saad väga hästi aru, et idee on toores ning sa täpselt ei tea, mis sellest välja tulema peaks. Prototüüp annab võimaluse katsetada asju koos sõpradega ning näha võimalusi, mida sa üksi ideed peas põrgatades kunagi ei näeks.

Leia endale tugigrupp

Sul on vaja enda ümber inimesi, kes kaasa mõtleks ja sulle jooksvalt tagasiside annaks. Tugigrupis peaks olema nelja eri tüüpi inimesi:

1. ***Lauamängudisainerid*** - minu isiklik kogemus on see, et Eesti lauamängudisainerid on väga lahked ja abivalmid ning alati nõus sinuga kohtuma ning su prototüübile pilgu peale viskama ja kaasa mõtlema. Jagatakse lahkesti koostööpartnerite kontakte ning antakse nõu ka müügikanalite ja tiraažide osas.
2. ***Valdkonna eksperdid*** - need inimesed, kes loovad õppematerjale, viivad läbi tunde või koolitavad koolitajaid. Nemad hoiavad valvsalt silma peal su mängu sisul ning vajadusel saad neilt head ja konstruktiivset kriitikat.
3. ***Tulevased mängijad*** - kes on need, kes sinu mängu abil uusi teadmisi hankima hakkavad? Algklassilapsed, gümnaasiuminoored või hoopis täiskasvanud? Igatahes on oluline leida endale paar sõpra sellest huvigrupist ning neilt vahepeal nõu ja sisendit küsida.
4. ***Mängu kliendid*** - eriti lastega seotud toodete puhul ei pruugi olla mängija koheselt klient. Kui su mäng on mõeldud eelkõige tundides kasutamiseks, on kliendiks õpetajad. Kui tegu on pigem koguperemänguga, on kliendiks lapsevanem.

Ideaalses maailmas võiks ju korra kuus kogu tugigrupi külla kutsuda ja vahepealseid arenguid tutvustada, kuid piisab sellest, kui nendega eraldi suhtled ja kursis hoiad mängu arenguga.

Alusta testimisi esimesel võimalusel

Mängu loomine on ajamahukas ettevõtmine ja seetõttu oleks äärmiselt rumal kõik valmis teha ning alles siis testida. Idufirmanduses on kasutusel termin minalaselt elujõuline toode (ingl *minimum viable product* – MVP) ning see tähistab toodet/teenust, millal on minimaalne vajalik funktsionaalsus, et seda saaks klientide peal testima hakata (Ries, 2011:104). Väga ahvatlev on ju mõte, et asi ei toimi selle pärast, et kujundus on kehv või reeglid pole veel kirjalikult, kuid suurem tõenäosus on selles, et mängu idee on liiga lihtne või keeruline ning mõlemal juhul kaob mängijate huvi kiiresti. Kui alustad testimisi varakult, on lihtsam vajalikke muudatusi teha.

Jaga oma ideid maailmaga

Väga palju inimesi kardab oma ideid jagada. Ühelt poolt kardetakse kriitikat ja teiselt poolt on hirm, et äkki idee on nii hea, et keegi varastab selle ära. Tegelikult on konstruktiivne kriitika edasiviiv jõud ning aktiivselt jagades võid leida kontakte ja võimalusi, mida sa isegi otsida ei oskaks.

Leia hea kujundaja

Kui prototüübi puhul ei ole oluline asja ilu, vaid mehaanika, siis valmis mängu puhul see reegel ei kehti. Eriti kui soovid teha mängu, mis on atraktiivne jaekaubanduses, on vaja, et mäng silma paistaks ning selles osas on sul vaja head kujundajat-kunstnikku. Arvesta, et headel tegijatel on tihti tööd ette planeeritud ning seega tuleb kokkulepped võimalikult varakult teha.

Leia koostööpartner mängu välja andmiseks

Kui soovid mängu ise välja anda, siis on variante palju. On erinevaid fonde ja rahastusmeetmeid, kuhu saad projekti kirjutada, võid leida mõne valdkonnas tegutseva firma sponsoriks või kasutada ühisrahastusplatvormi abi. Üheks võimaluseks on ühendust võtta mõne lauamänge tootva firmaga ja neile oma ideed pakkuda.

Tee oma idee teoks!

Kõige olulisem on see, et kui sul tekib mõni hea mõte, siis kindlasti vii see ellu. Jaga ideed julgelt ning küll leiad inimesed, kes aitavad asja valmis teha.

KOKKUVÕTE

Käesoleva magistritöö raames valmis hariv ja lõbus õpimäng „Häkkerite lahing“, mille eesmärgiks on õpetada vajalikke digipädevusi alg- ja põhikoolis käivatele noortele.

Mängu küsimuste koostamisel lähtuti eelkõige Livingstone jt (2014) ja Lorenzi (2017) töödes välja toodud ohtudest ning DigComp digipädevuste raamistuses (Kluzer ja Pujol Priego, 2018) välja toodud oskustest ja teadmistest. Tegu on õpimänguga, kus tavalise lauamängu elemente on rakendatud hariduslike eesmärkide saavutamiseks.

Mäng koosneb 12 tegelaskaardist (*Lisa 2*), mille on loonud tunnustatud Eest lasteraamatute illustraator Marja-Liisa Plats ning 150 kaitsekaardist (*Lisa 3*), mis on jaotatud viieks tasemeks. Lisaks on mängus kasutusel paha häkkeri tegevust kajastavad artefaktid: täringud ning pahavaražetoonid.

Mängu on testitud nii koolitunnis kui väljaspool seda ning selle tulemusena võib kindlalt väita, et mäng motiveerib lapsi uusi teadmisi õppima ning aitab kaasa diskussiooni tekkele erinevate olukordade üle internetis. Mäng antakse välja 2019. aasta sügiseks kasutades osaliselt ühisrahastust ning osaliselt koostööd Telia Eesti AS Suurima Julguse algatusega.

Ma väga loodan, et sellest magistritööst on tulevikus abi nendel, kes plaanivad mõnd õpimängu luua. Minu enda jaoks oli see protsess juba väga hariv ja lõbus väljakutse ning loodan, et mäng pakub uusi teadmisi ja mängurõõmu tuhandetele Eesti lastele.

SUMMARY

During this master's thesis, a fun educational game titled "Battle of Hackers" was created. The goal of the game is to teach elementary and primary school students how to safely use the internet.

The reason for creating the game originated primarily from the threats on the internet mentioned in the works of Livingstone et al. (2014) and Lorenz (2017) and suggested digital competencies by DigComp (Kluzer & Pujol Priego, 2018). It is an educational game where ordinary board game elements are implemented for achieving educational outcomes.

The game includes 12 character cards (appendix 2), which have been drawn by Estonian book illustrator Marja-Liisa Plats, and 150 question cards (appendix 3), which have been divided into five levels. The game also includes pieces reflecting the actions of criminal hackers: dice and malware-markers.

The game has been tested in school lessons, in youth work, at family gatherings, and in all of these settings has shown to motivate children to acquire new knowledge and to trigger discussions about different situations regarding the internet. The game will be published in the summer of 2019, funded by crowdfunding website Hooandja and co-financed by Telia Eesti Ltd.

I sincerely hope that this master thesis will be helpful to those who are interested in creating their own educational game. For me, this process was a highly educational and fun challenge, and I hope that the game offers new knowledge and joy of play to thousands of kids in Estonia.

KASUTATUD ALLIKAD

1. Age breakdown of video game players in the United States in 2018. (i.a). *The Statistics Portal.* Kasutatud 29.04.2019, https://www.statista.com/statistics/189582/age-of-us-video-game-players-since-2010/
2. Ait, J. (2017). Noored IT-seadmete ja interneti maailmas. *Statistikablogi*. Kasutatud 25.03.2019, https://blog.stat.ee/2017/10/26/noored-it-seadmete-ja-interneti-maailmas/
3. Akçayır, M., Dündar, H., & Akçayır, G. (2016). What makes you a digital native? Is it enough to be born after 1980?. *Computers in Human Behavior, 60*, 435-440.
4. Álvarez, M., Torres, A., Rodríguez, E., Padilla, S., & Rodrigo, M. J. (2013). Attitudes and parenting dimensions in parents' regulation of Internet use by primary and secondary school children. *Computers & Education, 67*, 69-78.
5. Arnab, S., Lim, T., Carvalho, M. B., Bellotti, F., De Freitas, S., Louchart, S., Suttie, N., Berta, R. & De Gloria, A. (2015). Mapping learning and game mechanics for serious games analysis. *British Journal of Educational Technology, 46(2),* 391-411.
6. Barker, L. J., & Aspray, W. (2006). The state of research on girls and IT. In J. M. Cohoon & W. Aspray (Eds.), *Women and information technology: Research on underrepresentation* (pp. 3–54). Cambridge: MIT Press.
7. Barlow, J., P. (1996). A declaration of the Independence of Cyberspace. *Electronic Frontier Foundation*, 8. veebruar. Kasutatud 19.04.2019, https://www.eff.org/cyberspace-independence
8. Bennett, S., Maton, K., & Kervin, L. (2008). The 'digital natives' debate: A critical review of the evidence. *British journal of educational technology, 39(5)*, 775-786.
9. Caillois, R. (2001). *Man, play, and games.* University of Illinois Press.
10. Clayton, K., von Hellens, L. & Nielsen, S. (2009) Gender Stereotypes Prevail in ICT; a *Research Review. Proceedings of the ACM SIGMIS Conference*, Limerick, Ireland, May 28–30, 2009.
11. Coil, D. A., Ettinger, C. L., & Eisen, J. A. (2017). Gut Check: The evolution of an educational board game. *PLoS biology, 15(4)*, e2001984.
12. Deci, E. L., & Ryan, R. M. (2008). Self-determination theory: A macrotheory of human motivation, development, and health. *Canadian psychology/Psychologie canadienne, 49(3)*, 182.
13. Digipööre (i.a). *Haridusministeerium*. Kasutatud 18.04.2019, https://www.hm.ee/et/tegevused/digipoore-0
14. Distribution of computer and video gamers in the United States from 2006 to 2018, by gender. (i.a). *The Statistics Portal.* Kasutatud 29.04.2019, https://www.statista.com/statistics/232383/gender-split-of-us-computer-and-video-gamers/

15. Domínguez, A., Saenz-De-Navarrete, J., De-Marcos, L., Fernández-Sanz, L., Pagés, C., & Martínez-HerráIz, J. J. (2013). Gamifying learning experiences: Practical implications and outcomes. *Computers & Education, 63,* 380-392.

16. Dorey, E., & McCool, J. (2009). The role of the media in influencing children's nutritional perceptions. *Qualitative Health Research, 19(5),* 645-654.

17. Furdu, I., Tomozei, C., & Köse, U. (2017). Pros and Cons Gamification and Gaming in Classroom. BRAIN: *Broad Research in Artificial Intelligence & Neuroscience, 8(2),* 56–62.

18. Gordon, G. (2008). What is play? In search of a universal definition. *Play and Culture Studies, 8,* 1-21. https://gwengordonplay.com/pdf/what_is_play.pdf

19. Gürer, D. and Camp, T. Investigating the Incredible Shrinking Pipeline for Women in Computer Science, *Final Report 9812016*, 2001. http://www.acm.org/women/

20. Hargittai, E. (2010). Digital Na(t)ives? Variation in Internet Skills and Uses among Members of the "Net Generation." *SOCIOLOGICAL INQUIRY, (1),* 92.

21. Helsper, E. (2008) *Digital natives and ostrich tactics?: the possible implications of labelling young people as digital experts*. Futurelab, Bristol, UK. Kasutatud 25. 03.2019, http://eprints.lse.ac.uk/26878/

22. Jenkinson, S. (2001). *The genius of play: Celebrating the spirit of childhood.* Hawthorn Press.

23. Kalmus, V., Blinka, L. & Ólafsson, K. (2015). Does it matter what Mama says: Evaluating the role of parental mediation in European adolescents' excessive internet use. *Children and Society*, 29(2), 122−133.

24. Kalmus, V., von Feilitzen, C., & Siibak, A. (2012). Effectiveness of teachers' and peers' mediation in supporting opportunities and reducing risks online. Children, risk and safety on the internet: *Research and policy challenges in comparative perspective,* 245-256.

25. Kiili, K., De Freitas, S., Arnab, S., & Lainema, T. (2012). The design principles for flow experience in educational games. *Procedia Computer Science, 15*, 78-91.

26. Kiili, K., Lainema, T., de Freitas, S., & Arnab, S. (2014). Flow framework for analyzing the quality of educational games. *Entertainment computing, 5(4),* 367-377.

27. Kindsiko, E., Türk, K. & Kantšukov, M. (2015*). Naiste roll ja selle suurendamise võimalused Eesti IKT sektoris: Müüdid ja tegelikkus.* Skype Microsoft Eesti - Tartu Ülikooli majandusteaduskond. Kasutatud 17.05.2019, https://www.mtk.ut.ee/sites/default/files/www_ut/naiste_roll_ikt._tu_mj-skype_uuring_2015.pdf

28. Kirschner, P. A., & De Bruyckere, P. (2017). The myths of the digital native and the multitasker. *Teaching and Teacher Education, 67*, 135-142.

29. Kluzer S., Pujol Priego L. (2018). *DigComp into Action - Get inspired, make it happen.* S. Carretero, Y. Punie, R. Vuorikari, M. Cabrera, and O'Keefe, W. (Eds.). JRC Science for Policy Report, EUR 29115 EN, Publications Office of the

European Union, Luxembourg, 2018. ISBN 978-92-79-79901-3, doi:10.2760/112945

30. Koolid ja lasteaiad saavad ligi 300 000 eurot õppetöö rikastamiseks (2019). *HITSA Uudised*, 27. märts 2019. Kasutatud 18.04.2019, https://www.hitsa.ee/uudised-1/koolid-ja-lasteaiad-saavad-ligi-300-000-eurot-tehnoloogia-ostmiseks
31. Koster, R. (2013). *Theory of fun for game design*.
32. Kõrvits, R. (2018). Roppustest kubisev Eesti laste lemmikmäng *Growtopia*. *Radar*, 25. september. Kasutatud 19.04.2019, https://tv.postimees.ee/6413055/roppustest-kubisev-eesti-laste-lemmikmang-growtopia
33. Leikop, M. (2018). *Miks.ee*, 26. aprill 2018. Kasutatud 18.04.2019, http://www.miks.ee/opetajale/uudised/hitsa-uus-strateegia-toetab-digipadevuste-arendamist
34. Leppik, Cenely, Haaristo, Hanna-Stella, Mägi, Eve (2017*). IKT haridus: digioskuste õpetamine, hoiakud ja võimalused üldhariduskoolis ja lasteaias*. Tallinn: Poliitikauuringute Keskus Praxis. Kasutatud 23.04.2019, http://www.praxis.ee/wp-content/uploads/2016/08/IKT-hariduse-uuring_aruanne_mai2017.pdf
35. Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2014). In their own words: What bothers children online?. *European Journal of Communication, 29(3)*, 271-288.
36. Lorenz, B. (2017). A Digital Safety Model for Understanding Teenage Internet User's Concerns (Digitaalse ohutuse mudel mõistmaks teismelise internetikasutaja vajadusi). *Doktoritöö.* Tallinna Ülikool: Informaatika Instituut.
37. Lorenz, B., Kikkas, K., & Laanpere, M. (2012). Comparing Children's E-safety Strategies with Guidelines Offered by Adults. *Electronic Journal of e-Learning, 10(3)*, 326-338.
38. Luik, P. (2018). Küberkiusamine: müüdid ja tegelikkus. *Õpetajate leht*, 15. juuni. Kasutatud 29.04.2019, http://opleht.ee/2018/06/kuberkiusamine-muudid-ja-tegelikkus/
39. Lõbus ja hariv lauamäng "Häkkerite lahing". (2019). *Hooandja*. Kasutatud 01.05.2019, https://www.hooandja.ee/projekt/lobus-ja-hariv-lauamang-hakkerite-lahing
40. Lõugas, H. (2019). Ekspert: Momo on sümptom, aga lapsevanemad peavad tegelema põhjusega. Talgukorras seda ei tee. *Geenius*, 5. veebruar. Kasutatud 28.04.2019, https://digi.geenius.ee/rubriik/uudis/ekspert-momo-on-sumptom-aga-lapsevanemad-peavad-tegelema-pohjusega-talgukorras-seda-ei-tee/
41. Mascheroni, G., & Ólafsson, K. (2014). *Net children go mobile: Risks and opportunities*. Kasutatud 14.04.2019, http://eprints.lse.ac.uk/56986/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_Net%20Children%20Go%20Mobile%20Project_Reports_Net%20children%20go%20mobile%20risks%20and%20opportunities%20(2nd%20ed.).pdf

42. Miller, L., & Budd, J. (1999). The Development of Occupational Sex-role Stereotypes, Occupational Preferences and Academic Subject Preferences in Children at Ages 8, 12 and 16. *Educational Psychology, 19(1),* 17–35.

43. Moen, R., & Norman, C. (2006). *Evolution of the PDCA cycle*. Kasutatud 20.04.2019, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.5465&rep=rep1&type=pdf

44. Murumaa-Mengel, M. (2017). Managing imagined audiences online: audience awareness as a part of social media literacies. *Doktoritöö.* Tartu: Tartu Ülikool.

45. Nicholson, S. (2015). A recipe for meaningful gamification. *Gamification in education and business (pp. 1-20).* Springer, Cham.

46. Niedenthal, S. (2009). What we talk about when we talk about game aesthetics. Chicago

47. OECD (2015), *Students, Computers and Learning: Making the Connection*, PISA. OECD Publishing: Paris. Loetud 15.04.2019, http://www.oecd.org/publications/students-computers-and-learning-9789264239555-en.htm

48. Orben, A., & Przybylski, A. K. (2019). Screens, Teens, and Psychological Well-Being: Evidence From Three Time-Use-Diary Studies. *Psychological Science.* https://doi.org/10.1177/0956797619830329

49. Pau, A. (2018). Palve vanematele; rääkige lastele, kes on Momo. *Postimees*, 10. detsember. Kasutatud 19.04.2019, https://tehnika.postimees.ee/6473921/palve-vanematele-raakige-lastele-kes-on-momo

50. Piotrowski, J. T., & Valkenburg, P. M. (2015). Finding orchids in a field of dandelions: Understanding children's differential susceptibility to media effects. *American Behavioral Scientist*, 59(14), 1776-1789.

51. Poudel, D. (2018a). *Turvaline internet. Digimaailma teejuht*. Tallinn: Digiabi

52. Poudel, D. (2018b). Diana Poudel: paljud vanemad ei tunne absoluutselt huvi lapse tegevuste vastu internetis. Mis on tagajärg? *Postimees*, 11. aprill. Kasutatud 28.04.2019, https://arvamus.postimees.ee/4467335/diana-poudel-paljud-vanemad-ei-tunne-absoluutselt-huvi-lapse-tegevuste-vastu-internetis-mis-on-tagajarg

53. Prensky, M. (2001a). Digital natives, digital immigrants part 1. *On the horizon, 9(5),* 1-6.

54. Prensky, M., & Berry, B. D. (2001b). Do they really think differently. *On the horizon, 9(6),* 6-9.

55. Raudla, H. (2018). Internet on nagu Šveitsi armeenuga. *Õpetajate leht,* 11. aprill. Kasutatud 28.04.2019, http://opleht.ee/2018/04/internet-on-nagu-sveitsi-armeenuga/

56. Raudla, H. (2019). Millest sõltub koolide digipädevus? *Õpetajate Leht*, 8. märts. Kasutatud 18.04.2019, http://opleht.ee/2019/03/millest-soltub-koolide-digipadevus/

57. Ries, E. (2011). *Nutikas idufirma*. Tallinn: Äripäev

58. Robootikaring Laagrisse. (2015). *Hooandja*. Kasutatud 01.05.2019, https://www.hooandja.ee/projekt/robootikaring-laagrisse

59. Rodríguez-de-Dios, I., van Oosten, J. M., & Igartua, J. J. (2018). A study of the relationship between parental mediation and adolescents' digital skills, online risks and online opportunities. *Computers in Human Behavior,* 82, 186-198.

60. Rohemäe, M.-A. (2015). Politsei kaardistab võimalikke MMS-i tarvitamise riskiperesid. *ERR.ee,* 11. oktoober. Kasutatud, 21.04.2019, https://www.err.ee/547039/politsei-kaardistab-voimalikke-mms-i-tarvitamise-riskiperesid

61. Romero, M., Usart, M., & Ott, M. (2015). Can serious games contribute to developing and sustaining 21st century skills?. *Games and Culture, 10(2),* 148-177.

62. Saar, A. (1997). *Laps ja mäng*. Riiklik Eksami- ja Kvalifikatsioonikeskus. Tallinn: EKK Trükikoda.

63. Salmela-Aro, K., Upadyaya, K., Hakkarainen, K., Lonka, K., & Alho, K. (2017). The dark side of internet use: two longitudinal studies of excessive internet use, depressive symptoms, school burnout and engagement among Finnish early and late adolescents. *Journal of youth and adolescence, 46(2),* 343-357.

64. Scutti, S. (2018). WHO classifies 'gaming disorder' as mental health condition. *CNN*, 18. juuni 2018. Kasutatud 21.04.2019, https://edition.cnn.com/2018/06/18/health/video-game-disorder-who/index.html

65. Seeman, P. (2007). Eesti *online*'i mängijad *World of Warcrafti* näitel. Tartu Ülikool: Sotsiaalteaduskond. *Bakalaureusetöö*.

66. Sheehan, R. 2003. Children's perception of computer programming as an aid to designing programming environments. In Interaction design and children: *Proceeding of the 2003 conference on interaction design and children.* New York: ACM Press

67. Siibak, A., & Tamme, V. (2013). 'Who introduced granny to Facebook?': An exploration of everyday family interactions in web-based communication environments. *Northern lights: Film & media studies yearbook*, 11(1), 71-89.

68. Sukk, M., Soo, K. (2018). *EU Kids Online'i Eesti 2018. aasta uuringu esialgsed tulemused.* Kalmus, V., Kurvits, R., Siibak, A. (toim). Tartu: Tartu Ülikool, ühiskonnateaduste instituut. Kasutatud 20.03.2019, https://sisu.ut.ee/sites/default/files/euko/files/eu_kids_online_eesti_2018_raport.pdf

69. Taipale, S. (2016). Synchronicity matters: defining the characteristics of digital generations. *Information, Communication & Society, 19(1),* 80–94. https://doi.org/10.1080/1369118X.2015.1093528

70. Turvaline internet – käsiraamat lapsevanematele & õpetajatele. (2018). *Hooandja*. Kasutatud 01.05.2019, https://www.hooandja.ee/projekt/turvaline-internet-kasiraamat-lapsevanematele

71. Valk, A. (2013). *Õpetajate oskused PIAAC andmete baasil*. Haridus- ja Teadusministeerium. Kasutatud 28.04.2019, https://www.hm.ee/sites/default/files/opetajate_oskused_piaac_andmete_baasil.pdf

72. Windle, G. (2011). What is resilience? A review and concept analysis. *Reviews in Clinical Gerontology*, 21(2), 152-169.

73. Vinter, K. (2013). Digitaalse ekraanimeedia tarbimine 5–7-aastaste laste seas ja selle sotsiaalne vahendamine Eestis. Pedagoogiline vaatekoht. *Doktoritöö*. Tallinna Ülikool.

74. Õppijate digipädevusmudel (2016). Kasutatud 18.04.2019, https://media.voog.com/0000/0034/3577/files/DigipadevusOppekavades2016.pdf

75. Yagoda, B. (2014). A Short History of "Hack". *The New Yorker*, 6. märts 2014. Kasutatud 20.04.2019, https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack

LISAD

Lisa 1. Mängude analüüs

Kaardimäng "Paaris või paaritu"
https://www.targaltinternetis.ee/wp-content/uploads/2015/12/paaris-voi-paaritu.pdf
2-6 mängijat; 70+4 kaarti (enda küsimused) + täring.
Loodud "Targalt internetis" projekti raames
Mängu autor: Birgy Lorenz
Mängu idee: mängijad peavad ära aimama teiste mängijate interneti ja arvuti alaseid eelistusi (näiteks Linux või Windows). Eesmärk tekitada diskussiooni mängijate vahel. Küsimuste põhjal tundub, et mängu sihtgrupp võiks olla põhikooli vanem aste.

Das rhetorische quartett (saksakeelne - tõlkes pealkiri „Retooriline nelik")
https://rhetorisches-quartett.de/
Päris täpselt mängust aru ei saa, kuid tundub, et eelkõige on eesmärgiks õpetada mängijaid ära tundma demagoogiat, libauudiseid ja muud sarnast, mis muudab internetis oleva info ebausaldusväärseks.

Cyber Poker Card Game
https://hciandcybersecurity.com/games-1/
Idee tore - kaartidel veebilehtede pildid ning vaja tuvastada, millised neist turvalised ja usaldusväärsed ning millised pigem mitte. Kahjuks teostuse osa kehvapoolne – väikesele mängukaardile mahutatud kaks kuvatõmmist ning vajalikke detaile ei ole näha. Samal tootjal veel paar mängu.

European Cyber Security Challange
Tundub start-up mäng olevat. Kahjuks reeglid üsna napid ja pole võimalik täpselt aru saada mängu taustaloos. Mängu eesmärgiks on suure tõenäosusega oskuste arendamine läbi missioonide täitmise.

Cards against humanity
https://cardsagainsthumanity.com/
Omamoodi mäng, mille loogika peale annaks kindlasti ka küberturvalisuse mängu luua. Kahjuks praeguse idee kontekstis ei ole kõige parem. Mäng internetis olemas ja litsentsi teksti osas saab mõningaid ideid.

Digital safety game
Tallinna Ülikool
http://www.dsg.onu.ee/
Küsimused-vastused tüüpi mäng. Küsimused jagatud järgmistesse kategooriatesse: võrk, häkkimine, manipuleerimisründed, pahavara, privaatsus, internet.

Lisa 2. Mängus olevad tegelaskaardid

Tegekaskaardid on loonud Marja-Liisa Plats ning näidiskaardid pildil on värvinud lapsed, kes mängu on testinud.

Lisa 3. Kaitsekaartide küsimused

Tase 1

1 Kellele tohib oma parooli öelda?
A Parimale sõbrale
B Kellelegi ei tohi parooli öelda peale ema isa
C Õpetajale
Parool on sama isiklik asi kui hambahari ja sa ei laena ju oma hambaharja parimale sõbrale või õele/vennale kasutamiseks.
Vanematele võid muidugi parooli öelda – siis on hea küsida, kui endal meelest läheb.
Ole ettevaatlik ka siis, kui parooli või koodi sisestad. Tihti lähevad paroolid uitama, kui nähakse, millist parooli inimene kasutab.

2 Mängid koos sõpradega arvutis ja avaneb aken: "Kliki siia ja võida miljon eurot!". Mida teed?
A Sulgen akna ja mängin sõpradega edasi
B Klikin lingil, et täpsemalt uurida
C Küsin sõpradelt, mida teha
Sellised reklaamid on petuskeemid ja neid tuleb ignoreerida. Ära kliki lingil ega jaga seda linki edasi sõpradele.
Kui su arvuti liiga tihti selliseid reklaame näitab, siis tee arvutile viirusetõrje ja puhasta oma veebilehe küpsised, sest võimalik, et su arvuti on pahavaraga juba nakatunud. Püüa vältida tundmatuid veebilehti ning ära tõmba programme ja faile ebaseaduslikest kanalitest, sest tihti satub pahavara just sellisel moel sinu arvutisse.

3 Kellega võib jagada oma telefoninumbrit?
A Kõigiga, sest see pole salajane info
B Pereliikmetega
C Sõpradega, keda tunnen ka päriselus
Kuigi telefoninumber pole ülisalajane info, ei tasu seda ikkagi liiga kergekäeliselt jagada. Ka telefoninumbrid on andmed, mida müüakse tumeveebis ning on mitmeid pettusi, mis on seotud just telefoninumbri teadmisega. Seega jaga oma telefoninumbrit ainult inimestega, keda sa ka päriselus tead ja usaldad. Kui sulle helistab võõras number, siis kindlasti kontrolli suunakoodi +372 – välismaalt tulevatele kõnedele ei tasu vastata.

4 Mis programm peab igas nutiseadmes olema?
A Viirusetõrje
B Sinu lemmikmäng
C Youtube
Igas nutiseadmes peab olema viirusetõrje. Muidugi tuleb arvestada sellega, et viiruseid on väga palju ning ka kõige parem viirusetõrje ei pruugi kõiki viiruseid ja pahavara ära tunda. Seetõttu tuleb väga ettevaatlik olla linkide klikkimise, manuste avamise ja rakenduste allatõmbamisega ka siis, kui viirusetõrje on nutiseadmes olemas.

5 Miks pahad häkkerid jagavad tasulisi mänge tasuta?
A Neil on kahju lastest, kes vähe taskuraha saavad
B Nad ise ostsid selle mängu ja tahavad seda teistega jagada
C Nad tahavad kasutajate arvutisse sokutada pahavara ja viirusi
Pakkudes tasulisi mänge ja programme tasuta, sokutavad kurjategijad arvutitesse nuhkvara, viiruseid ja muud pahavara.
Kui sa mängu ostad, siis ei ole lubatud seda edasi jagada. Internetis on ka

palju vabavaralisi programme ja mänge, mille eest sa ei pea maksma. Internetipiraatlus on ebaseaduslik ning selle eest võid karistada saada nii sina kui ka sinu vanemad.

6 Mida ei tohi mängudes teha?
A Lisada võõraid oma sõbralisti
B Saada sõpradest rohkem punkte
C Jagada isiklikku informatsiooni
Kui lisad mängudes oma sõbralisti võõraid, saavad nad sind palju lihtsamini mängus üles leida ning vaikselt sinu tegevust jälgida. Igasuguse isikliku info jagamine mängus on samuti ebaturvaline, sest sa ei saa kunagi täiesti kindel olla, kelleni see info jõuab. Ausas mängus sõpradest rohkem punkte saada on täiesti lubatud.

7 Sõbrad kutsuvad sind liituma uue ja põneva rakendusega. Pead seal looma konto. Mis infot võib sisestada ilma vanematega läbi arutamata?
A Pangakaardi konto
B Telefoninumber
C Hüüdnimi
Uut kontot luues peaksid alati rakendust enne vanematele näitama.
Kui konto loomiseks pole vaja muud kui ainult hüüdnime, siis sellise hüüdnime sisestamine, mida sinu pärisnimega seostada ei saa, on küllaltki ohutu. Juhul kui lisaks hüüdnimele pead ka meilikonto sisestama, pead kindlasti vanematega asjad läbi arutama.

8 Kui sul on koer nimega Pitsu, siis mis on kõige parem parool?
A Pitsu123
B R0tve1ler
C MinuKoeraN!miE1OleMuri
Ära pane parooliks oma lemmiklooma nime, sest seda teevad paljud inimesed ja nii on kurjategijal lihtne parooli välja nuputada, kui ta sinu lemmiklooma nime teab.
Samuti ei ole turvaline kasutada ainult ühte sõna sisaldavat parooli, sest ka seda on lihtne ära aimata.
Hea parool on piisavalt pikk ja võiks sisaldada mitut sõna, mis ei moodusta väga loogilist ja tavapärast lauset.

9 Parool on sinu internetikonto jaoks nagu ...
A …kulp poti jaoks
B ...võti ukse jaoks
C ...korsten maja jaoks
Parool on võti, mis hoiab sinu virtuaalse kodu turvalisena. Sa ei anna ju võtit suvalisele inimesele, samamoodi pead valvama ka oma parooli. Muidugi oleks mugav, kui üks võti kõik lahti teeb, kuid see poleks eriti turvaline. Nii on ka parooliga – on parem, kui kasutad erinevatel lehtedel erinevaid paroole.

10 Mis võib viidata sellele, et su on nutisõltuvus?
A Unustan rulapargist õigel ajal koju tulla, kui sõpradega trikivõistlusi filmime
B Mu uue telefoni aku on alati õhtuks tühi
C Kooliasjad jäävad tegemata, sest veedan liiga palju aega internetis
Sulle tundub, et sa pole eriti üldse telefoni kasutanud, aga selle aku on pidevalt tühi? See võib olla märk sellest, et sa ei saa ise aru, kui palju aega sa tegelikult nutiseadmes veedad. Nutisõltuvus on ohtlik haigus, mis võib kaasa tuua depressiooni ja ärevushäired.
Lisaks sellele kipub liigne nutiseadmes viibimine mõjuma õppimisvõimele ning hinded muutuvad halvemaks. Vahepeal tuleks teha mõni tehnikavaba päev, et nutisõltuvust ennetada.

11 Kas häkkimine on halb?
A Jah
B Ei
C Sõltub eesmärgist
Häkkimine on oma tehniliste teadmise

kasutamine veebilehe või programmi turvaaukude leidmiseks. Oluline on see, mida turvaaugu leidmise korral tehakse. Head häkkerid annavad kohe leitud turvaaugust teada ja aitavad seda parandada.
Pahad häkkerid hoiavad infot salajas ja püüavad välja nuputada, kuidas seda nõrkust enda eesmärkide jaoks ära kasutada.

12 Mida teha, kui satud küberkiusamise ohvriks?
A Anna sellest teada usaldusväärsele täiskasvanule
B Blokeeri kiusaja ja raporteeri lehe haldajale
C Helista kohe politseisse
Kui satud küberkiusamise ohvriks, siis räägi sellest kohe mõnele usaldusväärsele täiskasvanule, et nad saaksid aidata sul olukorda lahendada. Kui kiusamine toimub sotsiaalmeedia kanalis, siis blokeeri kiusaja ja raporteeri lehe haldajale. Kui õpetajate ja vanemate abiga ikka olukord ei lahene, siis võta ühendust lasteabiga (www.lasteabi.ee, tel 116 111), kust vajadusel suunatakse sind juba edasi veebikonstaabli juurde.

13 Mida tähendab ütlemine „internetis on asjad pilves“?
A Kui päike paistab, siis asju pole
B Sinu failid (fotod, dokumendid jm) on kellegi teise arvutis
C Vihmase ilmaga on internet aeglasem
Me kasutame tihti oma nutiseadet nagu väravavõtit mõnes võluri raamatus. See viib meid hetkega kuhugi kaugele – kellegi teise serverisse. Näiteks kui mängida mõnd mängu koos sõpradega internetis, siis see mäng ei toimu sinu enda nutiseadmes, vaid kellegi teise serveris. Sama kehtib ka Youtube´i videote ja Facebooki piltide kohta. Kuna tegevus toimub väljaspool sinu enda seadmeid, siis on väga oluline, et kaitseksid oma asju korralikult turvalise parooliga.

14 Mis asi on piksel?
A Arvutimäng, kus saab erinevaid maailmu ehitada
B Punkt, mis koos teiste punktidega moodustab arvutis pildi
C Välgulöök, mis on arvuti jaoks ohtlik

Piksel on kõige väiksem pildi osa arvutis. Piksel saab olla ainult ühte värvi ning pikslite arv määrab selle, kui suurena saab pilti vaadata ja välja printida.
„Pixel“ on mäng internetis, ja nagu näha, on väga oluline õiget kirjapilti tähele panna.
Pikslite abil kirjeldatakse ka ekraanide kvaliteeti. Mida rohkem piksleid, seda parem ekraan on. Näiteks 4K kuvar tähendab seda, et horisontaalselt suudab see ekraan näidata umbes 4000 pikslit.

15 Mis võib juhtuda nutisõltuvuse tagajärjel?
A Ülekaalulisus
B Kehvad hinded koolis
C Unehäired
Nutisõltuvus tähendab seda, et inimene püüab järjest rohkem aega veeta internetis ja jätab selle soovi täitmiseks oma ülejäänud kohustused tegemata.
Nutisõltuvuse tulemusena võib tõusta kehakaal (väheneb liikumine) ja halveneda hinded, sest kodus ei õpita, samuti tekivad raskused uinumise ja hommikuse ärkamisega. Kui kardad, et sul hakkab tekkima nutisõltuvus, siis tee nädalas endale paar tehnikavaba päeva.

16 Mis neist on internetis kõige ohtlikum?
A Kõikvõimas häkker, kes näeb internetis kõike
B Viirused, mis su arvuti aeglaseks muudavad
C Rumalad ja ohtlikud mängud, mille eesmärgiks on lapsi hirmutada ja panna tegema rumalaid asju.
Vahetevahel levivad internetis mängud, mille eesmärgiks on panna lapsi rumalalt käituma või endale haiget tegema. Tavaliselt ähvardatakse sellises mängus, et kui laps ei tee seda, mida kästakse, siis juhtub midagi halba tema pere või sõpradega. Kui sind kutsutakse mõnd kahtlast mängu mängima, siis lõpeta kohe kutsujaga suhtlemine ning näita vestlust usaldusväärsele täiskasvanule.

17 Mis on GIF?
A Posteri jaoks tehtud pilt
B 30-sekundiline video
C Liikuv pilt

GIF on liikuv pilt, millel võib olla ka mingi tekst. See võib olla animeeritud tegelane või mingi lühike filmilõik. GIF-e kasutatakse väga palju kommentaarides ja vestlusrakendustes. See on üks võimalustest, kuidas oma emotsiooni virtuaalses keskkonnas edasi anda.

18 Millised numbrid peaksid sul kindlasti telefonis salvestatud olema?
A Lasteabi 116 111
B Vanemate numbrid
C Naabripoisi telefoninumber
Lisaks vanemate numbrile võiks sul telefonis olla ka Lasteabi number ja pähe õpitud number 112. Kui sul on mingi mure, siis Lasteabis on spetsialistid, kes oskavad väga erinevatel teemadel nõu anda. Samuti võivad sinna helistada lapsevanemad või õpetajad. Vanemate numbrid võiksid ka peas olla juhuks, kui telefon maha jääb, aga nendega on vaja ühendust võtta.

19 Teed suhtlusrakendusse kontot ja pead endale nime valima. Milline valik on kõige turvalisem?
A Kasutan oma pärisnime
B Kasutan varjunime, et keegi ei teaks, kes ma olen
C Kasutan nime, mis annab teistele vihje, kes ma olen
Alati on kõige turvalisem kasutada nime, mida pole kuidagi võimalik sinuga seostada.
Kindlasti ära kasuta kasutajanimes oma sugu, riiki, vanust, sünniaastat või mingit muud sinu kohta käivat infot. Kui mängid mõnd mängu, kus saad oma maailma ehitada ja siis sellele nime panna, siis mõtle ka see nimi põhjalikult läbi. Kindlasti ära kasuta kooli või kodutänava nime.

20 Kes neist ei ole usaldusväärne täiskasvanu?
A Täiskasvanud inimene, kellega internetis tutvusin
B Vanaema, kes ei oska internetti kasutada
C Paralleelklassi õpetaja
Usaldusväärne täiskasvanu on inimene, keda sa tunned päriselust ning keda tunnevad või teavad ka sinu vanemad. Usaldusväärsed täiskasvanud on kindlasti pereliikmed ja õpetajad. Kahjuks on nii, et pahad inimesed oskavad jätta endast väga head muljet, kuid nende eesmärk võib olla sinult saladuste väljameelitamine, et hiljem saaks sinult välja pressida, ähvardades neid saladusi internetti postitada.

21 Miks on Snapchat ohtlikum kui Facebook Messenger?
A Sõnumid kustuvad ise ära
B Selle logol on kummitus
C Seal on palju rohkem kasutajaid

Igasugused sõnumirakendused on ohtlikud, sest nende kaudu saavad sinuga ühendust võtta inimesed, keda sa ei tunne, ning saab saata halbu sõnumeid. Snapchat on aga ohtlik seetõttu, et sõnumid kustuvad ära ning kui sa kiiresti ei reageeri ja häirivat sõnumit ei salvesta, on hiljem probleemi tekkides väga raske olukorda lahendada.

22 Kas ema ja isa võivad sinust üles panna fotosid, mis sulle piinlikkust valmistavad?
A Ei tohi, sest sul on õigus otsustada, mis info sinust internetis üleval on
B Tohivad küll, sest nad on sinu eestkostjad
C Sõltub sellest, miks see foto sinu jaoks piinlik on
Igal inimesel on õigus otsustada, milline info tema kohta internetti postitatakse ning see kehtib ka laste puhul. Lapsevanem peab küsima lapselt nõusolekut tema foto lisamiseks internetti ning laps ei pea oma keeldumist põhjendama.
Parim variant on see, kui kõik pereliikmed otsustavad ühiselt, mis infot nad internetti panna soovivad ning kindlasti tasub ka üksteise kontodel silm peal hoida.

23 Miks ei tohi võõrastele öelda oma kooli nime?
A Nad tahavad ka minu kooli õppima tulla, aga klassides pole ruumi
B Direktor saab riielda, kui õpilased kooli nime internetti postitavad
C Kui keegi teab kooli nime, siis saab ta mind lihtsasti üles leida
Kooli nime järgi on võimalik sind üles leida ning kui sa peaksid sattuma väljapressimise või küberkiusamise ohvriks, võib kiusaja ka kooli gruppidesse või meililistidesse sinu kohta soovimatut infot saata. Kellegi kooli nime teades on kergem luua ka libakontot, millega selle inimese identiteeti varastada.

24 Saad kettkirja, kus on kirjas, et pead selle saatma 10 sõbrale või muidu juhtub sinu elus suur õnnetus. Mida teed?
A Saadan kirja edasi 10 sõbrale
B Kirja edasi ei saada, kuid olen mitu päeva ettevaatlik – ehk juhtub miskit halba
C Kustutan kirja ja ignoreerin selle sisu, sest tegu on lihtsalt rumala pettusega
Sellised kettkirjad on parimal juhul infomüra, halvimal juhul püütakse nende abil välja kaardistada naiivseid inimesi, kellele edaspidi juba mingeid ohtlikumaid petukirju saatma hakata. Kettkirju ei tohi edasi jagada ning ei tasu muretseda, et see kuidagi sinu elu mõjutab.
Kui mõni sõber sulle sellise kirja saadab, siis selgita ka talle, et selline käitumine on rumal ning võib teda muuta pahade häkkerite sihtmärgiks.

25 Näed internetis kuulutust, et uut iPhone´i müüakse 25 euroga. Mida teed?
A Ignoreerin seda pakkumist
B Lähen ja ostan telefoni ära, enne kui otsa saab
C Jagan linki ka sõpradele
Kui internetis on mõni tavapäraselt kallis asi üliodav, siis tuleb eriti ettevaatlik olla. Tihti on selliste pakkumiste eesmärk kätte saada kergeuskliku ostja pangakaardi number, mida seejärel kasutatakse kiiresti mõnes teises kohas kaupade ja teenuste eest maksmiseks. Kui tingimata soovid siiski riskida, siis kasuta ajutist virtuaalkaarti, kus ongi limiidiks summa, mida vajad selleks ostuks. Tundmatutel lehtedel ei tohi sisestada pangakaardi numbrit!

26 Miks peab õppimise ajal nutiseadmed kinni ja vaikseks panema?
A Paljud rakendused teevad hääli ja see segab keskendumist
B Aku saab muidu liiga kiiresti tühjaks
C Ei pea kinni panema, sest ma oskan mitut asja korraga teha
Inimese aju on selline, et kõige parema tulemuse saab siis, kui teha ühte asja korraga. Paljud nutirakendused on tehtud nii, et need püüavad pidevalt meie tähelepanu ja see häirib teisi tegevusi.
Kui õpid, pane parem telefon hääletu peale, nii saad kodutööd palju kiiremini tehtud. Miskit hullu ei juhtu, kui sa kohe oma sõnumitele ei vasta.

27 Teete perega toreda pannkoogihommiku. Mis ei peaks laual olema?
A Moos
B Telefon
C Nuga
Hea komme on ühise söögikorra ajal mitte nutiseadmeid vaadata, vaid omavahel vestelda. Kui kõigil on suur kiusatus telefoniekraani vaadata, siis võite teha ühe mängu – pange kõik telefonid keset lauda, ekraan allapoole. See, kes esimesena oma telefoni kätte võtab, peab nõud pesema ja köögi korda tegema.

28 Mis vanusest alates on lubatud Facebooki kontot teha?
A 10
B 13
C 16
Facebooki lubatud vanusepiir on 13 aastat. Kui keegi valetab oma vanuse kohta, siis on võimalik teada anda, et kasutaja on tegelikult noorem, ning konto kustutatakse. Vanusepiiri eesmärk on lapsi kaitsta, sest Facebookis liigub ka väga palju pahatahtlikke inimesi. Samuti jagatakse seal sisu, mis ei ole algklassilastele sobiv.

29 Mis raamatust saad infot interneti ja arvutite kohta?
A „Turvaline internet. Digimaailma teejuht“
B „Tere, Ruby! Programmeerimisseiklused“
C „Harry Potter ja tarkade kivi“
Arvuti- ja internetiteemalisi raamatuid ei ole palju ja seega tasub olemasolevatega tutvuda. Algklassides tasub kindlasti lugeda Ruby seiklustest. Kui hakkad aktiivsemalt internetis ringi liikuma, siis raamatust „Turvaline internet. Digimaailma teejuht“ leiad nii lugusid elus enesest kui ka häid soovitusi, kuidas internetis turvaliselt liikuda.

30 Mitme minuti järel tuleks nutiseadmes või arvutis tegutsedes paus teha?
A 45 minuti
B kahe tunni
C 10 minuti
Igas tunnis peaksid vähemalt 5–10 minutit liikuma. Kuna arvutis tegutsedes või nutiseadmes mängides võib ajataju kaduda, siis on hea mõte panna taimeri tööle. Kui taimer 45 minuti pärast heliseb, tee paus ja liiguta ennast veidi. Enne uuesti tegutsema hakkamist pane taimer taas tööle.

Tase 2

31 Kas telefonil peab ekraanilukk peal olema?
A Jah, igal juhul
B Ei, sest muidu ei saa minuga ühendust võtta, kui telefon ära kaob ja keegi selle leiab
C Ainult siis, kui mul on telefonis väga olulisi asju
Lukustamata telefon on nagu lukustamata koduuks. Pahatahtlik

võõras võib sinna sattudes palju pahandust teha. Näiteks postitada sinu kontodele, sinu sõpradelt infot välja meelitada, e-posti abil saab ka kontode paroole ümber muuta, kasutades linki "Unustasin parooli". Samuti võib telefoni leidja teha kõnesid tasulistele numbritele või välismaale ja sa saad suure arve. Pane kindlasti oma telefon lukku, et võõras sinu andmetele ligi ei pääseks.

32 Milline neist on kõige turvalisem kood?
A 9758
B 1234
C Minu sünnikuupäev
Kindlasti ei ole hea kood sinu sünnipäev ega lähedaste sünnipäev. Numbrikombinatsioone 1234 või 0000 kasutatakse samuti väga palju ja neid proovitakse ka kõige rohkem.
Kõige parem kood on suvaline number või huvitav arvude jada, mida sul oleks lihtne meeles pidada.

33 Mida pahavara teha võib?
A Saata sinu paroolid ja failid pätile
B Teha sinu arvuti kiiremaks ja paremaks
C Kustutada kogu arvutis oleva sisu ja nõuda taastamise eest raha
Pahavara võib teha väga palju erinevaid asju. Näiteks klahvinuhk (keylogger) salvestab sinu klaviatuuri löögid ja nii saab pätt kätte su logimisinfo ja pangakaardi numbri. Ka viirused on pahavara, näiteks krüptoviirus paneb kasutaja failid lukku ja nõuab raha, et nendele uuesti ligi pääseks. Osa pahavarasid muudab andmeid arvutis või veebilehtedel.

34 Sõber annab sulle oma mängukonto parooli, et aitaksid teda. Mida teed?
A Selgitan sõbrale, miks ei tohi paroole jagada, ja kutsun ta külla, et koos mängida
B Mul endal pole aega, aga annan info edasi ühele teisele sõbrale, kes lubab aidata
C Login sisse ja aitan. Sõpru tuleb ju aidata!
Mitte kunagi ei tohi oma parooli kellegagi jagada! Ka mitte mängukontode oma. Kui keegi sulle parooli jagab, siis ka sellest võib tulla palju pahandust, kui ta konto näiteks skämmitakse ja ta sind selles süüdistama hakkab.
Kui tahad sõpra aidata, siis kutsu ta külla ja õpeta talle, kuidas keerulistest kohtadest edasi saada ja kiiremini kõrgemale tasemele jõuda.

35 Mis neist on skämm?
A Sulle saadetakse e-kiri, kus pakutakse vitamiine müügiks
B Saad kirja, et oled võitnud loteriis, kuigi sa pole lotopiletit ostnud
C Keegi logib sinu mängukontole sinu kasutajaga
Skämm on petuskeem, kus püütakse sind meelitada oma andmeid avaldama või raha üle kandma. Spämm on rämpspost reklaamiga, mida sa ei soovi (nt see vitamiinide kiri). Kui keegi logib su kontole sisse sinu kasutajaga ilma sinu teadmata, siis see on identiteedivargus, kuigi on täiesti võimalik, et info sinu parooli kohta saadi sinult endalt kätte mõnd petuskeemi kasutades. Ära kunagi kliki linkidele, mis on võõra inimese saadetud kirjas, ning ära kunagi vasta sellisele kirjale.

36 Milline seadistus peaks olema alaealise Instagrami kontol?
A Avalik
B Privaatne
C Sõltub sellest, mida postitan
Instagrami konto lubatud vanusepiir on 13 aastat ning alguses on turvalisem teha privaatne konto – nii saad kontrollida, kes su pilte näevad. Kui ikkagi soovid teha avalikku kontot, siis palu kindlasti usaldusväärsel täiskasvanul jälgida sinu kontot ja hoida silm peal su uutel postitustel.

37 Pead kooli arvutisse sisse logima, aga arvuti teatab, et kasutajanimi või parool on valed. Mida teed?
A Ütlen sõbrale oma kasutajanime ja parooli ning palun tal proovida
B Küsin sõbralt tema kasutajanime ja parooli, et saaksin lehele sisse logida
C Vajutan lingile, et unustasin parooli, või kui sellist linki ei näe, siis palun õpetaja abi
Oma parooli ei tohi mingil juhul jagada, samuti ei ole lubatud teise kasutaja paroolidega sisse logida. Kui parooli ära unustad, siis tavaliselt on veebilehel link „Unustasin parooli“. Seda vajutades saadetakse e-postile link, mille abil saad uue parooli panna. Kui sellist linki ei leia, siis palu abi õpetajalt.

38 Kas oma mängukonto müümine on hea mõte?
A Ei ole, sest see võib kaasa tuua palju probleeme
B On küll, kuid ainult siis, kui makstakse sularahas
C Jah, sest nii saab raha teenida
Enamik mänge on mängureeglitesse kirja pannud, et konto müümine ei ole lubatud. Juhul kui selline tehing tuvastatakse, kustutatakse kõik nii ostja kui ka müüjaga seotud kontod. Ja isegi kui konto müümine on lubatud, võib sellise tehingu käigus võõra kätte minna ka su parool, isiklikud sõnumid või mingi muu info, mida saab pahatahtlike eesmärkide saavutamiseks ära kasutada.

39 Miks on avalik WiFi ohtlik?
A Teised võivad ligi pääseda sinu failidele
B Ebaturvalisel veebilehel on võimalik konto kaaperdada
C Häkkeritel on lihtsam sinu andmesidet pealt kuulata
Avalik WiFi on turvarisk, sest samas võrgus viibijad saavad sinu andmetele lihtsamini juurdepääsu. On ka veebilehti, mis ei kasuta turvalist ühendust ning selliste lehtede puhul on häkkeril võimalik sinu sessioon kaaperdada ja sinu nimel sõnumeid saata või su kontol olevate materjalidega tutvuda. Pealegi ei saa sa kunagi kindel olla, kes tegelikult seda avalikku WiFit jagab.

40 Mida tähendab häkkimine?
A Arvutisüsteemide nõrkade kohtade leidmine
B Arvutiprogrammide kirjutamine
C Microsoft Office programmi kasutamine

Häkkimine tähendab arvutisüsteemide turvalisuse testimist ning vigade leidmist, mis võimaldavad arvutis või veebilehel teha asju, mis võivad rikkuda lehe tööd või kätte saada andmeid, mis ei ole mõeldud avalikuks kasutamiseks. Häkkerite üheks oluliseks oskuseks on programmeerimine. Osavad häkkerid teavad palju ka inimeste psühholoogiast, sest tänapäeval on lihtsam inimesi ära petta kui masinaid.

41 Mis on pahade häkkerite eesmärk?
A Kätte maksta
B Ebaausal teel raha või võimu saada
C Luua kaost
Pahade häkkerite (ingl black-hat

hackers või crackers) eesmärk on suurendada oma vara ebaseaduslikul teel või lõhkuda teiste asju ja teistele halba teha.
Kättemaks, pettused ja kaos on mõned eesmärgid, mille nimel halvad häkkerid tegutsevad. Eesmärgiks võib olla ka pahatahtlik luuretegevus ning vaenuliku võõrriigi jaoks andmete kogumine või väljapressimise teel raha saamine.

42 Millal pöörduda veebikonstaabli poole?
A Kui näen internetis videot alasti lapsest või loomapiinamisest
B Kui minust tehakse trenni riietusruumis poolalasti pilt
C Kui klassikaaslane minu kohta midagi rumalat FBs postitab
Veebikonstaabli poole tasub pöörduda siis, kui pere ja õpetajad sind aidata ei saa. Kui sinust tehakse trenni riietumisruumis pilt, siis räägi sellest kohe treenerile ja vanematele ning klassivenna rumalast postitusest anna teada õpetajale. Veebikonstaablid on väga head ja abivalmid, aga neil on palju tööd ja seetõttu peab kõigepealt proovima probleemi lahendada usaldusväärsete täiskasvanute abil.

43 Mida saab programmeerimise abil teha?
A Luua toredaid mänge
B Leida võrgust ebaturvalisi veebilehti
C Lahti muukida paroole
Hea programmeerimisoskusega saab teha väga palju asju, nii häid kui halbu. Mida paremini saad aru, kuidas programmid töötavad, seda paremini oskad ennast internetis kaitsta. Programmeerimist võib õppida juba algklassides, selleks on olemas palju toredaid rakendusi ning kindlasti vaata ka lehele https://scratch.mit.edu/, kus saab ise mänge ja animatsioone teha.

44 Milline neist ei ole operatsioonisüsteem?
A Windows
B Android
C Safari
Levinumad operatsioonisüsteemid on Windows, iOS, Android, Linux, Mac OS. Operatsioonisüsteem on programmide kogum, mis juhib arvutisüsteemi tööd. Safari on veebilehitseja ehk brauser nagu näiteks ka Chrome, Opera, Edge ja Internet Explorer.

45 Viirus ja pahavara on nagu...
A Koer ja kass
B Kana ja lind
C Lill ja kapsas
Iga viirus on pahavara, aga pahavara võib olla ka muu pahatahtlik tarkvara nagu näiteks nuhkvara, reklaamvara või trooja hobune. Arvutiviiruse unikaalseks omaduseks on tema isepaljunemisvõime. Kui viirus arvutisse satub, kopeerib ta ennast ja püüab nakatada teisi võrgus olevaid arvuteid või siis saata ennast edasi näiteks e-posti kaudu. Sama loogika, et iga kana on lind, aga lind võib olla kana, jaanalind või kotkas.

46 Kuidas tasuta mängud võivad kalliks maksma minna?
A Et hästi mängida, peab mängus asju ostma
B Tasuta mänge mängides võib tekkida nutisõltuvus
C Tasuta ei saa olla kallis
Sageli on mängudes selline ärimudel, et saad mängu alla laadida küll tasuta, kuid hiljem pead ostma lisateenuseid, et saaksid kõrgemal tasemel mängida või rohkem punkte koguda. Samuti on kõigi mängude puhul oht, et kui mängid neid üleliia palju, võib tekkida nutisõltuvus ning selle tulemusena vajad aina rohkem mänge ja isegi kui see rahaliselt kalliks ei lähe, toob see ikkagi kaasa probleeme.

47 Mis on manus?
A Veebilehel olev PDF-fail
B E-kirjaga kaasas olev fail
C Mängu pandud summa õnnemängus
Manus (attachment) on fail, mis on e-kirjaga kaasas. See võib olla tekst, pilt, esitlus või mis iganes. Suurte failide saatmisel ei pruugi vastuvõtja postkastis olla su kirjale piisavalt ruumi ning teinekord ei lähe need ka läbi spämmifiltritest. Gmail näiteks laseb saata maksimaalselt 25 MB suurust faili. Kui soovid suuremat saata, siis kasuta näiteks Google Drive'i või failijagamisteenust WeTransfer.

48 Mis on kuvatõmmis?
A Pilt, mis ilmub ekraanile, kui sa arvutit ei kasuta
B Ekraanikaitse, mis kaitseb ekraani päikesevalguse eest
C Ekraanipilt hetkel ekraanil toimuvast
Kuvatõmmis (screenshot) on ekraani salvestamine. Arvutis saab seda teha PrintScreen (PrtScr) nupuga, nutitelefonis peab vastavalt telefoni margile vaatama, milliseid klahve on kuvatõmmise tegemiseks vaja. Kuvatõmmise tegemine on vajalik oskus, sest see võimaldab kiirelt salvestada ebameeldivaid tekste ja sõnumeid ning neid vajadusel taasesitada (näiteks politseile).

49 Sa mängid *online*-mängu ja tundmatu kasutaja tahab sind sõbraks lisada. Mida teed?
A Lisan ta sõbraks, sest rohkem sõpru on lahedam
B Ignoreerin seda kutset
C Küsin tundmatult enne mõne küsimuse, et teda paremini tundma õppida
Kui lisad kellegi mängus sõbraks, leiab ta sind lihtsamini mängus üles, saab sind jälgida, mida sõpradega räägid jne. Seega ära mitte kunagi lisa mängudes sõpradeks tundmatuid kasutajaid. Kui mõni tundmatu väga lahke on ning oma asju jagab, siis ära võta neid vastu. Internetis tundmatult mängunänni vastuvõtmine on sama kui tänaval võõralt inimeselt kommi vastuvõtmine – ja seda sa ju ei teeks.

50 Mida peab tegema, enne kui postitad foto internetti?
A Mõtlema postituse juurde kolm teemaviidet (*hashtag*'i)
B Küsima luba foto postitamiseks inimestelt, kes on fotol äratuntavad
C Kontrollima tausta, et seal poleks kalleid asju ega isiklikku infot
Kindlasti peab sul enne postitamist olema kõigi inimeste nõusolek, kes on pildil.
Samuti kontrolli tausta – selleks pane ekraan hästi heledaks ja tee pilti suuremaks. Tihti on nii, et mobiili väikesel aknal ei ole veidrad asjad taustal hästi näha, kuid kui keegi vaatab pilti suurelt ekraanilt, võib näha taustal asju, mis võivad sulle piinlikkust valmistada või pättidele liiga palju infot anda.

51 Kas internetist leitud materjale võib edasi jagada?
A Jah
B Ei
C Sõltub pildi autoriõigustest
Kui jagad algset allikat – veebilehte või pildilinki –, siis võid leitud infot jagada. Kui soovid pildi salvestada ja oma konto kaudu edasi jagada, siis pead kindel olema, et selle pildi või teksti autoriõigused lubavad sellist jagamist. Kui sa selles päris kindel pole, jaga pigem algset allikat.

52 Millist infot võib internetis jagada?
A Kooli nime, kus õpin
B Järgmise reisi kuupäevi
C Oma lemmik-GIF-i
Iga kord, kui internetti infot postitad,

mõtle selle peale, kas mõni pahatahtlik inimene saab neid andmeid kurjasti ära kasutada. Näiteks järgmise reisi kuupäevi postitades või välisriigis check-in´i tehes annad sa teada, et sind pole sel ajal kodus. Samuti võib kooli nimi olla pahatahtliku inimese jaoks oluline infokild.

53 Tundmatu laigib igat su postitust ja saadab sõnumeid. Sina temaga suhelda ei taha. Mida teed?
A Saadan talle kirja, kus selgitan, miks ma ei taha temaga suhelda
B Olen viisakas ja suhtlen veidi
C Blokeerin selle kasutaja
Kui võõras kasutaja suhtleb aktiivselt ja sina teda ei tunne, siis pole vaja viisakas olla, vaid bloki ta kohe. Internet on täis libakontosid, mis on loodud selleks, et valeuudiseid levitada, reklaami spämmata või isegi mingeid petuskeeme läbi viia. Sageli ei olegi selliste kontode taga pärisinimesed, vaid arvutiprogrammid, mis postitavad kommentaare ja laigivad postitusi täiesti suvaliselt. Ära lase ennast ära kasutada!

54 Kes neist on usaldusväärne täiskasvanu?
A Koolipsühholoog
B Minuga samal tänaval elav täiskasvanu
C Täiskasvanu, kellega olen pikalt internetis suhelnud
Iga täiskasvanu ei ole usaldusväärne ning ka kurjategijad elavad kellegi tänaval. Seetõttu ole ettevaatlik, kellega suhtled päriselus ja internetis ning kui sul on mingi mure, siis pöördu vanemate, sugulaste või koolipersonali poole. Vajadusel võid helistada lasteabi telefonil.

55 Keegi postitab sinust internetti pildi, mida sa avalikult jagada ei soovi. Mida teed?
A Palun pildi ära kustutada. Kui ta seda ei tee, siis teavitan lehe haldajat, õpetajat või lapsevanemat
B Mitte midagi ei saa teha
C Postitan temast veel nõmedama pildi internetti
Enne kui postitad video või foto internetti, pead küsima luba kõigilt inimestelt, keda on pildil või videos näha. Kui mõni inimene ei soovi, et tema info internetti läheb, peab seda soovi austama. Kui keegi oma kontole sinust pildi postitab, siis saad paluda lehe omanikul selle eemaldada. Kui ükski eelnimetatud abinõu ei aita, võid pöörduda ka veebikonstaabli poole.

56 Näed internetis reklaami, mis kutsub sind osalema mängus, kus võid võita kalli nutitelefoni. Mida teed?
A Täidan ankeedi ja osalen loosimises
B Jagan lehte ka sõpradega, et nemadki saaksid osaleda
C Ei tee reklaamist välja ehk ignoreerin reklaami
Selliste mängude eesmärgiks võib olla inimesi meelitada liituma täiesti mõttetute sisuteenustega, saada nende isikuandmed või hullemal juhul meelitada välja pangakaardiandmeid. Näiteks suure tekstiga on kirjas, et võida telefon, kuid väikeses kirjas on info, et kui paned oma telefoninumbri ja sellele saadud koodi lehele, siis hakkad iga nädal saama ühe mõttetu SMS-i ning pead selle eest maksma paar eurot või rohkemgi.
Ole väga ettevaatlik, kuhu sa oma telefoninumbri internetis sisestad!

57 Mis ei ole küberkiusamine?
A Kellegi video alla halvustava kommentaari kirjutamine
B Sõbrast naljaka pildi postitamine ilma tema nõusolekuta
C Sõbrakutsest keeldumine

Sõbrakutsest keeldumine ei ole kiusamine ega kellegi solvamine. Võta vastu ainult need sõbrakutsed, mille puhul tunned inimest hästi ja ta meeldib sulle. Kui sõbrakutse saadab inimene, kes sulle päriselus ei meeldi, pole kindlasti vaja seda vastu võtta.

58 Saad sõbrakutse inimeselt, keda sa ei tunne, kuid teil on mitu ühist sõpra. Mida teed?
A Lisan ta sõbraks, sest küllap oleme mõne ühise sõbra juures kohtunud
B Keeldun sõbrakutsest
C Kirjutan talle sõnumi ja küsin, kas oleme kohtunud
Pole mõtet võtta vastu sõbrakutset inimeselt, keda sa ei tunne. Kahjuks lisavad paljud inimesed sõpru oma sõbralisti ilma pikemalt mõtlemata ning seetõttu ei tähenda paar ühist tuttavat sugugi seda, et tegu ei võiks olla libakonto või mõne pahatahtliku inimesega. Kui tingimata soovid teada, kes see inimene on, siis küsi ühiselt sõbralt, kas ta päriselt tunneb seda inimest.

59 Mida peab tegema, kui veebileht tundub veider?
A Näitama seda veebilehte vanematele
B Klikkima erinevatel linkidel, et paremini aru saada, mis leht see on
C Lahkuma sellelt lehelt
Internet on täis veebilehti, mis sisaldavad valeuudiseid, petuskeeme ja lastele sobimatut sisu. Seetõttu ei tohi imelikul või kahtlasel veebilehel pikemalt klikkima hakata, vaid näita seda esimesel võimalusel usaldusväärsele täiskasvanule. Kui sa seda kohe kellelegi näidata ei saa, tee kuvatõmmis ning lahku veebilehelt. Näita kuvatõmmist usaldusväärsele täiskasvanule esimesel võimalusel.

60 Kas lapsed on internetis targemad kui täiskasvanud?
A Üldiselt küll, mõne erandiga
B Kõik on internetis targad
C Mängudes tihti on, kuid muudes asjades pigem mitte
Mõnikord arvavad täiskasvanud, et lapsed on internetis targemad, kuid uuringud näitavad, et see ei ole nii. Ükski inimene ei tea internetist kõike ning lastel ja täiskasvanutel on erinevad kogemused ja oskused. Seega kõige parem on omavahel suhelda ning koos asju läbi arutades on kõigil internetis turvalisem.

Tase 3

61 Mis asi on kaheastmeline autentimine?
A Võltsitud isikutunnistus
B Turvameede, mis nõuab võõrast arvutist sisenemisel ka mobiilile saadetud koodi sisestamist
C Üks programm, millega saab teiste paroole välja nuhkida
Kaheastmeline autentimine (KA) on väga hea võimalus oma oluliste kontode turvalisemaks lukustamiseks. Kui KA on sisse lülitatud, siis isegi kui mõni pätt saab sinu konto parooli kätte, peab ta võõrast arvutist sisenedes sisestama ka koodi, mida näed mobiiltelefonist. KA sisselülitamine muudab sinu konto palju turvalisemaks ning kindlasti tasuks seda võimalust rakendada Google'i ja Facebooki kontodel.

62 Saad tundmatult numbrilt sõnumi, et sinust on lisatud foto internetti. Mida teed?
A Ignoreerin sõnumit
B Vastan viisakalt ja uurin, mis pildist käib jutt
C Vajutan lingile, et pilti vaadata. Kui mulle pilt ei meeldi, siis palun kustutada
Kui sa taolist sõnumit ei oota ja sa ei tea, kes selle sõnumi saatis, siis kustuta see sõnum. Lingile klikkides võib su nutiseade nakatuda pahavaraga.
Kui sulle helistab või saadab sõnumeid tundmatu number, võib tegu olla automaatprogrammiga, mille eesmärk on võimalikult palju nutiseadmeid pahavaraga nakatada.

63 Milliselt lehelt saab kontrollida, kas su andmed on sattunud kurjategijate kätte?
A https://www.internet.ee/
B haveibeenpwned.com
C www.google.com
Liigagi tihti saab uudistest lugeda, kuidas üks või teine andmebaas on ära häkitud ja kasutajate andmed on kurjategijate kätte sattunud. Kui sul on kahtlus, et sinu konto andmed on lekkinud, tasub kindlasti vahetada parool nii sellel saidil, kust see lekkis, kui ka teistes kohtades, kus sama parooli kasutad.

64 Milline neist on hea parool?
A Parool123
B J22t!sekokte!l
C q1w2e3r4t5y6
Hea parool on selline, mida keegi teine ei kasuta. Parool123 ja q1w2e3r4t5y6 on mõlemad väga populaarsed paroolid ja seega on neid väga lihtne häkkeril ära aimata.
Eestis on väga populaarsed ka sellised paroolid nagu lammas, minaise, maasikas, kallis, killer, armastus, lollakas, samsung, teretere jne.
Aga ära nüüd ka J22t!sekokte!li kasuta, vaid mõtle enda jaoks unikaalne parool.

65 Mis või kes teevad interneti ohtlikuks?
A Viirused
B Programmid
C Inimesed
Interneti teevad ohtlikuks kõik kolm. Viirused on ju ise ka programmid. Kasutatakse ka võltsprogramme, et meelitada sind viiruseid alla laadima. Olemas on näiteks võlts-antiviirus, mängud, mille sisse on peidetud pahavara jms. Ja kõik need asjad on valmis teinud kurjade kavatsustega inimesed.
Sul võib olla väga hea nutiseade, aga kui sa ise ettevaatlikult ja mõistlikult ei käitu, on sul ikkagi internetis ohtlik olla.

66 Mis on veebilehe küpsised (*cookies*)?
A Väike andmefail, mis võimaldab kasutaja tegevust internetis jälgida
B Auhinnad veebilehel, mida külastajatele jagatakse
C Küpsised, mis on programmeerija laua peal
Veebilehe küpsised on väikesed andmefailid, mis salvestatakse sinu arvutisse ning nende eesmärk on salvestada kasutaja kohta mingeid andmeid. Just nende küpsiste tõttu on nii, et kui mõnel veebilehel käid, siis hakkad igal pool internetis nende kohta rohkem reklaami nägema. Nende abil on võimalik saada täpset infot, kus sa internetis liigud ja mida teed. Küpsised ei loe su arvuti kõvaketast, kuid kindlasti vähendavad need privaatsust. Vahetevahel võiks küpsised ära kustutada.

67 Mida kindlasti ei tohiks oma telefoni turvamustriks panna?
A Oma eesnime esitähte
B Liiga keerulist sümbolit
C Sama kujundit, mida ka ema oma telefonis kasutab
Väga palju inimesi kipub oma telefoni turvamustriks panema enda eesnime esimest tähte – seda on väga lihtne ära aimata. Samuti ei tasu PIN-koodiks panna oma sünnikuupäeva, sest see on esimene asi, mida proovitakse, kui keegi püüab seadet lahti murda.

68 Mida võivad pahatahtlikud inimesed teha sinu piltidega?
A Loovad võltskonto sinu nimel
B Leiavad sealt infot sinu elukoha kohta
C Kasutavad neid pilte piinlikes reklaamides
Enamik inimesi saab aru, et internetis ei tohi avaldada elukohta, kooli nime ja muud taolist, kuid tegelikult on andmeteks ka pildid, mida sa jagad internetis või privaatse sõnumiga. Pilte saab kasutada võltskontode loomiseks või siis tehakse neist meem või reklaam, mille sõnum on mõnitav või veider. Lisaks võib pildifailis olla asukohamärgis, mis annab võimaluse tuvastada täpne pildi tegemise asukoht.

69 Miks ei tohi konto andmetes valet vanust panna?
A Mulle hakatakse ebakohaseid reklaame näitama
B Vanus ei ole oluline info, see ei mõjuta midagi
C Leht võib muuta mu andmed lihtsamini internetis leitavaks
Alaealiste kontosid kaitstakse rohkem – neile näidatakse vähem reklaame, samuti ei jagata nende kontode andmeid nii lihtsalt otsingumootoritega. Aga kui märgid ennast tunduvalt vanemaks, siis ei oska leht sind kaitsta ning pahadel häkkeritel on palju lihtsam sinu andmeid leida. Samuti näed rohkem tüütuid reklaame.

70 Kui leiad telefoni, millel on ekraanilukk peal, siis mida teed?
A Annan kohalikku infopunkti
B Panen pildi Facebooki ja palun sõpradel jagada
C Vaatan SIM-kaardilt, millise operaatori juures on leping ja viin telefoni nende esindusse
Kui leiad telefoni, siis vaata SIM-kaardi pealt, millise firmaga on omanikul leping ja vii telefon selle firma esindusse. Anna kindlasti ka politseile teada, kust ja millise telefoni leidsid ja kuhu selle viisid. Telefonifirma saab kontrollida, kellele SIM-kaart kuulub. Kui leiad telefoni koolis, vii see kooli infolauda, bussis leitud telefon jäta bussijuhi kätte jne. Facebookis jagamine pole mõistlik, sest infomüra on suur ja info ei pruugi jõuda omanikuni.

71 Mida teevad head häkkerid?
A Aitavad testida programmide turvalisust
B Panevad uued filmid torrentisse
C Aitavad kurjade riikide serveritesse sisse murda
Head häkkerid (ingl white-hat hackers või ethical hackers) aitavad muuta internetti turvalisemaks.
Nad testivad erinevate veebilehtede ja programmide turvalisust ning kui leiavad vea, siis annavad sellest kohe veebilehe või programmi omanikule teada. Kindlasti ei lisa head häkkerid filme torrentitesse, sest see ei ole seadusega lubatud, ega murra sisse teiste riikide serveritesse, sest selline tegevus võib kaasa tuua palju probleeme.

72 Veebileht internetis on nagu ...
A suvaline ruum suvalises riigis
B naabri maja minu kodutänaval
C pood kaubanduskeskuses

Veebileht internetis on nagu suvaline ruum suvalises riigis. Isegi kui veebilehel on tekst eesti keeles, ei tähenda see seda, et ka leht ise asuks Eestis ja omanik oleks siitkandist. Samuti ei garanteeri .ee lõpp lehe usaldusväärsust. Seega kui lähed uuele ja tundmatule veebilehele, siis käitu seal sama ettevaatlikult, nagu teeksid seda näiteks Lõuna-Aafrika tundmatus laohoones ringi liikudes.

73 Mida vanad arvutid teha ei osanud?
A Mõelda
B Arvutada
C Käsku täita
Vanemad arvutid oskasid väga hästi arvutada ja kasutajate käske täita, kuid nad ei osanud mõelda.
Arvutiprogrammid muutuvad aga järjest keerulisemaks ning tänapäeval õpivad arvutid ise uusi asju ja võib juba isegi öelda, et arvutid mingil määral mõtlevad ise.
Tehisintellekt on teadusharu, mille eesmärgiks on luua arvuti, mis suudab täiesti iseseisvalt mõelda ja tegutseda.

74 Mis on netikett?
A Viisakusreeglid internetis
B Kettkiri sotsiaalmeedias
C E-kirjaga kaasas olev info
Netikett ehk interneti etikett on reeglite kogumik, mida on viisakas võrgus suheldes järgida.
Suurte tähtedega kirjutamine tähendab karjumist.
Kui satud arvuti taha, kust inimene on unustanud välja logida, siis ära loe tema isiklikke sõnumeid, vaid logi välja.
Ole ettevaatlik sõnumite ja e-kirjade edasi saatmisel – pead kindel olema, et sul on algse kirja kirjutaja luba jagamiseks.

75 Tegid koolis MS Wordi abil tekstifaili, aga kodus seda programmi ei ole. Millise programmiga saad faili muuta?
A Google Docs
B Google Sheets
C OpenOffice
Sageli võib juhtuda nii, et koolis kasutatakse programme, mida koduses arvutis ei ole. Seetõttu tasub õpetajalt uurida, kas on vabavaralisi programme, millega sama tööd saab teha. Näiteks MS Wordi faile saad avada ja muuta Google Docsi ja Openoffice'i abil; vabavaralisi programme on teisigi.

76 Milline neist rakendustest aitab sul võõras kohas teed leida ja sobivaid bussiaegu teada saada?
A Dropbox
B Google Maps
C Evernote
Kõik need on väga toredad ja head rakendused, millega võiksid tutvuda, kuid Google Maps on see, mis aitab sul ka võõras linnas teed ning sobiva bussi või rongi leida.
Kaardi lugemine on oskus omaette ja seetõttu harjuta alguses kodu lähedal selle rakenduse kasutamist.
Arvutis on Google Mapsil veel üks väga vahva võimalus – lohista ekraaninurgas olev kollane mehike kaardile ja vaata, mis juhtub.

77 Mis on *vlog*?
A Youtube'i kanal
B Videoblogi
C TikTok konto
Vlog on videoblogi. Nagu blogisid võib ka vlogisid olla erinevaid – mõni räägib videotes enda tegemistest, mõni tutvustab uusi mänge, mõni õpetab süüa tegema... Ühisosa on see, et vlogi autor loob ise sisu ning see on video vormis. Youtube on lihtsalt üks tööriist, mille abil vloge teha.

78 Kas Google'i otsingu tulemusi saab alati usaldada?
A Jah, sest Google'i algoritm on maailma parim
B Ainult siis, kui olen väga õiged otsisõnad sisestanud
C Ei, sest kuvatakse ka makstud reklaami ja algoritme saab petta
Google'i otsingualgoritm on hea, kuid see ei ole kindlasti eksimatu. Paljud kelmid püüavad oma kodulehte võimalikult kõrgele kohale saada ning see võib neil ka õnnestuda. Pealegi, kui su arvutis ei ole reklaamiblokeerijat, võivad esimesed kolm otsingutulemust olla hoopis reklaamid.

79 Kui saad e-kirja, et oled võitnud miljon eurot, siis mida teed?
A Klikin kirjas olevale lingile
B Vastan kirjale ja küsin, kuidas raha kätte saan
C Märgin kirja pettuseks ja kustutan ära
Väga levinud petuskeemiks on ülihea palga või ärivõimaluse pakkumine. Nende pettuste eesmärgiks on saada kätte isikuandmeid või meelitada raha välja ning mitte mingil juhul ei tohiks sellistele kirjadele vastata, ühelegi kirjas olevale lingile klikkida või kirjaga kaasas olevat manust avada. Lastele suunatud levinud petuskeem on näiteks see, et lubatakse mänguraha juurde anda, aga tegelikult varastatakse logimisandmed.

80 Pead täitma ühe ankeedi. Kuidas käitud?
A Täidan kõik lüngad tõese infoga
B Enne kui hakkan ankeeti täitma, näitan seda vanematele
C Panen kõikidesse kastidesse suvalised vastused
Kui hakkad mõnda ankeeti täitma, siis näita seda enne oma vanematele. Tihti on ankeetides teksti, mis paneb sulle kohustusi.
Seetõttu peab täiskasvanu asjad üle vaatama, et koos otsustada, kuidas seda asja kõige paremini täita ja kas üldse peab täitma.
Ka e-post ja telefoninumber on info, mille jagamisel võõrastele võib probleeme tekkida.

81 Miks võib telefoni asukoha määrang vajalik olla?
A Fotodele saab lisada asukohamärgiseid
B Vanemad saavad vajadusel lapse asukoha kohta jooksvalt infot
C Kui telefon ära kaob, saab vaadata, kus see on
Kui sul on seadetes asukohamäärang sisse lülitatud, siis saab vaadata nutiseadme asukohta reaalajas. See võib väga kasulik olla olukorras, kui telefon ära kaob või kui kuskil ära eksid ja vanemad peavad su üles leidma. Arvesta aga sellega, et seda infot kasutavad paljud rakendused ning kui su paroolid ja privaatsusseaded pole korralikult paigas, võib info sinu täpse asukoha kohta jõuda võõraste inimesteni.

82 Sõber soovitab programmi, millega saad oma lemmikmängus raha juurde tekitada. Mida teed?
A Kontrollin, kas viirusetõrje on uuendatud, enne kui alla laen
B Lähen ja tõmban kohe programmi alla
C Ei hakka riskima, sest sellised programmid on tihti pettused ja sisaldavad viiruseid
Igasugused mänguhäkid ja mänguraha generaatorid on suuremas osas petuskeemid, mille eesmärk on saada kätte kasutajanimi ja parool. Samuti on sellised rakendused hea viis nutiseadmesse viirus või pahavara sokutada. Isegi kui tegemist ei ole pahavaraga, on selliste rakenduste kasutamine enamikus mängudes keelatud ja su konto võidakse bännida.

83 Kas kõike, mis internetis kirja pandud, peaks uskuma?
A Jah, sest internetti postitavad ainult targad inimesed
B Jah, sest kõike, mida internetti postitatakse, kontrollivad õpetajad üle
C Ei
Internetti saab infot postitada igaüks ja keegi ei kontrolli, et see info ka tõele vastaks. Mõnikord postitavad inimesed teadmatusest valesid fakte, kuid mõnikord tehakse seda ka teadlikult. Eesmärgiks võib olla inimeste hirmutamine või paanika külvamine. Seega ole info osas alati väga ettevaatlik ja ära jaga asju edasi, kui sa pole täiesti kindel, et tegu on tõese infoga.

84 Millistelt lehtedelt saab infot, kuidas küberkiusamist vältida?
A noor.targaltinternetis.ee
B https://suurimjulgus.ee/
C kiusamisvaba.ee
Küberkiusamine on väga nõme asi ning on kurb, et leidub inimesi, kes tahavad teistele liiga teha. Kui keegi sind kiusab (kas internetis või päriselus), siis kindlasti ei tohi vaikides kannatada, vaid räägi sellest nii sõpradele kui ka täiskasvanutele. Ka internetis on mitu asjalikku lehte, kust saab häid nõuandeid, kuidas käituda, kui koged või näed pealt küberkiusamist.

85 Miks ei tohi võõrastele öelda oma pangakaardi numbrit?
A Nad saavad internetist oste teha minu raha eest
B Nad võivad mu kaardinumbri ära häkkida
C Nad võivad selle abil mu kaardi pangas lukku panna
Pangakaardi numbrit teades saab internetis sellega oste teha ja pole ju üldse tore, kui keegi teine kõik su kogutud raha ära kulutab.
Isegi kui postitad kaardinumbri osaliselt, on võimalik, et proovitakse seda ikkagi kasutada. Ning kui pank sellist kahtlast tegevust näeb, siis üldjuhul su pangakaart suletakse. Ära mitte mingil juhul jaga kaardil olevat infot teksti ega pildina.

86 Kas kõik juutuuberid on eksperdid?
A Ainult need, kellel on palju fänne
B Mõned võivad olla, kuid mitte kõik
C Ei ole, sest eksperdid ei tee endale Youtube'i kanalit
Youtube'i kanali võib selle lehe reeglite järgi teha iga üle 13-aastane kasutaja ning videote üleslaadimiseks ei ole vaja ette näidata mingeid tunnistusi ega oskusi. Seega võib juutuuber olla igaüks. Kindlasti ei tähenda kanali populaarsus info usaldusväärsust, pigem on jälgijate hulk seotud kanali meelelahutusliku väärtusega. See muidugi ei tähenda, et Youtube'is ei ole ka ekspertidel oma kanaleid.

87 Kes on süüdi, kui üks õpilane logib teise õpilase kontoga sisse ja kustutab mõned failid?
A See, kes andis oma paroolid teisele õpilasele
B See, kes paroole kasutas ja faile kustutas
C Õpetaja
Isegi kui üks õpilane oli nii rumal ja andis oma parooli teisele (mida ei tohiks kunagi teha), siis süüdi on ikkagi see, kes seda infot kasutas ning failid kustutas. See, kui keegi käitub internetis rumalasti, ei ole vabandus, et ka ise võiks rumalalt käituda.

88 Mida kõik häkkerid usuvad?
A Turvalisi süsteeme pole võimalik häkkida
B Igal süsteemil on mõni nõrkus
C Võidab see, kellel on kõige vingem arvuti
Häkkerid usuvad, et igal süsteemil on

mõni nõrkus ja seda on võimalik leida. Head häkkerid tahavad aidata selle nõrkuse ära parandada. Pahad häkkerid tahavad seda nõrkust ise ära kasutada, et lehelt andmeid kätte saada või midagi muud valgustkartvat korraldada.
Kusjuures süsteemi nõrkus ei tähenda alati tehnikat, vaid eelkõige kasutatakse ära kasutajate naiivsust, et sokutada nutiseadmesse mõni pahavara.

89 Mida head häkkerid kunagi ei tee?
A Püüavad kasutajate paroole lahti murda
B Otsivad süsteemides nõrkusi
C Kasutavad kasutajate kontosid ilma nende teadmata
Head häkkerid (ingl white-hat hackers) küsivad eelnevalt luba, kui hakkavad veebilehe või programmi turvalisust testima. Nad annavad turvaaukude kohta leitud info lehe või programmi omanikule edasi.
Kindlasti ei kasuta hea häkker mitte kunagi kellegi kontot ilma selle inimese teadmata ning ei hoia leitud turvaauke saladuses lehe omaniku või haldaja eest.
Heade häkkerite eesmärk on see, et kõigil oleks internetis turvalisem ja julgem olla.

90 Kui kaugel peaks ekraan silmadest olema?
A vähemalt 1 meeter
B vähemalt 20 cm
C vähemalt 40 cm
Silmade tervise jaoks on hea, kui ekraan on silmadest 40 cm kaugusel või kaugemal. See kehtib ka nutitelefoni ekraani kohta. Samuti soovitatakse ekraani eredust madalamaks keerata, et see silmi vähem ärritaks. Kui silmad on kuivad või hakkavad punetama, võib see olla märk sellest, et hoiad telefoni liiga silmade lähedal. Ekraanidest eralduv sinine valgus takistab melatoniini ehk unehormooni tootmist ning ei lase sul magama jääda.

Tase 4

91 Miks kasutatakse veebilehtedel CAPTCHA kontrolli?
A Kontrollitakse, kas oled piisavalt vana, et kontot teha
B Kontrollitakse, ega sa robot ei ole
C Kontrollitakse, kas sa said lehe reeglitest aru
CAPTCHA kontroll on veebilehtedel seetõttu, et internetis on väga palju bot-programme. Bot-programmid on automaatsed programmid, mis käivad mööda veebilehti ringi, loovad kontosid ja postitavad igasugust spämmi. Selle vältimiseks palutakse ankeetide täitmisel või kommentaaride kirjutamisel lahendada inimesele lihtne ülesanne, mille täitmisega bot-programmid hakkama ei saa, näiteks pildil oleva arvutustehte lahendamine.

92 Mis asi on NFC?
A Mittefunktsioneeriv kood
B Numbritest koosnev parool
C Kontaktivaba side
NFC on kontaktivaba side ja see võimaldab vahetada andmeid läbi õhu, kui kaks NFC seadet lähestikku satuvad. Näiteks on kasutusel pangakaardid, mida nimetatakse viipekaartideks, seda kasutatakse ühistranspordis ning samuti on paljudel telefonidel NFC tugi. Selle tehnoloogia muudab ohtlikuks asjaolu, et näiteks saab pangakaardilt raha maha võtta ka nii, et inimene ise ei märka.

93 Kas torrenti programmi installimine on seaduslik?
A Jah
B Ei
C Sõltub asjaoludest
Torrenti kliendiprogramm ei ole ebaseaduslik ning on palju vabavaralisi

programme, mida võib täiesti ametlikult torrentist tõmmata. Ebaseaduslik on tõmmata torrenti kaudu materjale, mille omanikud pole andnud õigust neid levitada üle torrenti või mis tavapäraselt pole tasuta. Lisaks autoriõiguste rikkumisele võivad torrenti kaudu jagatavad materjalid olla viirustega nakatunud.

94 Mis asi on zombi-arvuti?
A Arvuti, mille omanik on Zombi
B Arvuti, mis on surnud
C Arvuti, mis on nakatunud viirusega ja mida saab kasutada ka võõras inimene
Zombi-arvuti on arvuti, mis on nakatunud pahavaraga ning kuuletub ka kellegi teise käskudele. Pätid kasutavad zombi-arvuteid selleks, et peita internetis oma jälgi, saada tasuta arvutivõimsust või kasutada sinu arvuti kõvaketta ruumi. Zombi-arvutid võivad saata rämpsposti, korraldada rünnakuid teistele arvutitele või hoida ebaseaduslikke faile sinu arvuti kõvakettal.

95 Millal peab paroole vahetama?
A Vahetan siis, kui süsteem seda nõuab
B Vähemalt korra kvartalis
C Ei peagi, kui on hea parool ja lehte pole häkitud
Kui sul on piisavalt pikk ja keeruline parool (20+ tähemärki, sisaldab numbreid ja sümboleid ning kasutad eri lehtedel erinevaid paroole), siis tegelikult ei pea parooli muutma, kui just leht ise seda ei nõua.
Paroolid muudab ohtlikuks see, kui kasutatakse lühikesi ja tavapäraseid paroole või erinevatel lehtedel alati sama parooli. Et sinu parooli teada saada, piisab, kui vaid üks leht on pahade kavatsustega häkkerite poolt loodud.

96 Milliseid õigusi vajab üks taskulambi rakendus?
A Ligipääsu kontaktidele
B Ligipääsu kaamerale
C Ligipääsu asukohale
Mobiili kasutamiseks taskulambina piisab täiesti ligipääsust kaamerale, et rakendus tööle hakkaks. Tihti küsivad rakendused aga nutiseadmes õigusi, mida neil tegelikult vaja ei lähe. Ole ettevaatlik rakendustele õiguste andmisel ning kui tundub, et mõni rakendus tahab ligipääsu kõigile su andmetele, siis püüa leida alternatiivne rakendus, mis on usaldusväärsem.

97 Kuidas on võimalik, et sinu arvuti osaleb pangaröövis?
A See pole võimalik
B Pätt varastas selle ära ja müüs juppidena maha
C Mu arvutis on viirus, mis muudab ta zombi-arvutiks ning seda kasutas keegi teine pangaröövi läbiviimisel
Väga sageli kasutavad küberkurjategijad jälgede peitmiseks teisi arvuteid.
Luuakse pahavara, millega nakatumisel saab pätt kontrolli kasutaja arvuti üle. Selliseid arvuteid kasutatakse erinevate kuritegude sooritamiseks: serveritesse häkkimiseks, reklaami levitamiseks, pornograafilise materjali salvestamiseks. Kasutaja ise tavaliselt ei tea, et tema arvutit kasutab ka keegi teine.

98 Kas mobiiltelefoni saab kasutada maksevahendina?
A Ei saa
B Ainult siis, kui sinna krediitkaardi number panna
C Saab küll
Enamik mobiilioperaatoreid laseb vaikimisi kasutada mobiiltelefoni ka maksevahendina. Näiteks saad sellega maksta tasulistele numbritele helistades, sõnumeid saates või internetis mingeid

teenuseid tellides. Kui sa ei soovi üllatust liiga suure telefoniarve näol, siis on mõistlik paluda mobiilioperaatoril selline maksmise lisateenus sulgeda.

99 Millest koosneb sinu digitaalne jalajälg?
A Sotsiaalmeedia kontodest
B Kommentaaridest
C Laikidest
Digitaalse jalajälje moodustavad kõik meie tegevused internetis. Kuigi võib tunduda, et üks laik või kommentaar ei ole oluline, siis tegelikult võivad need olla abiks, kui keegi püüab su identiteeti varastada või sinu kohta midagi uurida. Samuti kasutavad veebilehed igat su liigutust, et sind paremini reklaamijate jaoks kirjeldada.

100 Mis või kes on *bitcoin*?
A „Growtopias" kasutatavad mündid
B Käsk, mille abil saab teada arvuti ostuhinna
C Virtuaalne raha
Bitcoin on krüptoraha, millega saab internetis osta ja müüa ning mille omanikku on raske tuvastada. Selle raha anonüümsust kasutavad palju ära kurjategijad. Näiteks on loodud krüptoviirused, kus kasutajalt nõutakse makset bitcoin'ides, et ta saaks tagasi oma arvutis olevad failid. Bitcoin'e tekitatakse spetsiaalse tarkvaraga, mis peab lahendama matemaatilisi probleeme ja selle töö tulemusena tekivadki bitcoin'id.

101 Programmeerimine on ...
A ... protsessori ühendamine emaplaadiga
B ... arvutile täpsete käskude andmine
C ... kellegi teise loodud häki kasutamine
Programmeerimine on see, kui programmeerija annab arvutile käske. Selleks peab õppima selgeks mõne programmeerimiskeele, mida arvuti tunneb.
Programmeerimiskeeled on näiteks Python, Java, JavaScript, PHP, Ruby, C++ jms.
Algklassides ja põhikoolis saad õppida programmeerimist näiteks Scratchi abil. Seal saad teha vahvaid animatsioone ja luua ise mänge.
https://scratch.mit.edu/

102 Mis on vabavaraline programm piltide töötluseks?
A Adobe Photoshop CC
B Gimp
C Windows Movie Maker
Gimp on vabavaraline ja väga hea programm, millega saab teha pilte nii raster- kui ka vektorgraafikas. Rastergraafika tähendab seda, et pilt koosneb pikslitest; sellise pildi puhul on pildi algne suurus oluline, et seda suurelt ja kvaliteetselt välja printida. Näiteks digifotod on rastergraafikas. Vektorgraafikas kirjeldatakse pilti matemaatiliste kujundite (näiteks joonte ja ringide) abil ja tänu sellele saab suurt pilti sama kvaliteediga välja printida.

103 Mis on server?
A Toidupood
B Arvuti või programm, mis pakub teenuseid teistele arvutitele või kasutajatele
C Võti, millega saab avada SIM-kaardi pesa
Server on arvuti või tarkvara, mis pakub kasutajatele internetis teenust. Näiteks Gmail jookseb meiliserveris, Fortnite mäng mänguserveris ja Facebook on veebiserver.
Dropbox ja Google Drive on failiserverid, mis annavad sulle võimaluse oma failidele ligi pääseda erinevatest kohtadest ja neid ka vajadusel teistega jagada.

104 Milline on korrektne domeen?
A facebook.com/turvalineinternet
B https://ee.postimees/
C ekool.e-u
Domeen ehk veebilehekülje aadress võib koosneda paljudest osadest, kuid kaks asja on igal domeenil – nimi ja laiend. Domeeninimi on näiteks facebook ja laiend .com. Eesti veebisaitidel on laienditeks tavaliselt .ee, aga võib ka olla .eu. Oluline on jälgida, et enne laiendit oleks õige domeeninimi, sest internetis on ka õngitsuslehti, kus püütakse kasutajat segadusse ajada, kasutades meile tuttava veebilehe nime.

105 Mida tähendab BTW?
A Muuseas
B Kõvasti naerma
C Tuntud ka kui
Internetis kasutatakse vestluses erinevaid lühendeid. Näiteks:
LOL – laughing out loud (kõvasti naerma)
SRY – sorry (vabandust)
IM(H)O – in my (honest) opinion (minu arvamuse kohaselt)
TNX – thank you (aitäh)
YOLO – you only live once (sa elad ainult ühe korra)
BTW – by the way (muuseas)
XOXO – musid ja kallid
PLZ – please (palun)
AKA – as known as (tuntud ka kui)

106 Mida tähendab rööprähklemine (*multitasking*)?
A Mitme asja korraga tegemine
B Kahe või enama protsessoriga arvuti
C Matemaatiline võrrand
Rööprähklemine on see, kui teeme mitut asja korraga. See hajutab tähelepanu ning me teeme kõiki asju, mida me korraga püüame teha, kehvemini kui neid ükshaaval tehes. Näiteks kui püüad samal ajal mängida ja õppida, kulub sul rohkem aega ja tulemused tulevad kehvemad, kui mõlemat tegevust eri aegadel teha.
Püüa teha ühte asja korraga ning eriti hea oleks see, kui sa õppimise ajal nutiseadmeid ei vaata.

107 Milline neist on arvuti riistvara?
A Acrobat Reader
B Protsessor
C Google Drive
Arvuti riistvaraks nimetatakse neid osasid, millest arvuti füüsiliselt koosneb.
Arvuti riistvara on emaplaat, protsessor, kõvaketas, videokaart, helikaart jmt.
Arvuti lisaseadmed on hiir, klaviatuur, kõrvaklapid jne.
Programme, andmefaile ja operatsioonisüsteemi kutsutakse arvuti tarkvaraks, need juhivad riistvara ja lisaseadmete tegevust.

108 Millised neist on usaldusväärsed allikad?
A wikipedia.ee
B www.eki.ee
C www.stat.ee
Usaldusväärsed allikad on teadusartiklid, ametlikud andmebaasid ja hea mainega ajakirjandusväljaanded. Tihti otsitakse infot ka Vikipeediast, kuid seda ei loeta usaldusväärseks allikaks, sest seda saab igaüks muuta. Kui leiad Vikipeediast põneva fakti, mida soovid koolitöös kasutada, kontrolli seda alati esmasest allikast – viited algallikatele on iga artikli all.

109 Saatsid võõrale endast pildi. Nüüd tahab ta videokõne teha, et rääkida su vanematele ära, et saadad võõrastele pilte. Mida teed?
A Teen temaga videokõne
B Räägin ise vanematele ära
C Valetan, et kaamera ei tööta
Sageli on halvad inimesed internetis väga osavad manipulaatorid ning

suudavad esialgu jätta endast eriti sõbraliku ja toreda mulje. Ent niipea, kui oled saatnud mingit isiklikku või salajast infot, see tore inimene kaob ja sult võidakse hakata täiendavat infot välja pressima. Mitte kunagi ei tohi väljapressimisega kaasa minna, vaid kohe tuleb suhtlus lõpetada ja ise vanematele lugu ära rääkida.

110 Paned endale uue profiilipildi, mis sulle väga meeldib, aga keegi ei laigi seda tunni jooksul. Mida teed?
A Panen uue profiilipildi
B Saadan sõpradele sõnumi ja uurin, miks nad minu pilti ei laigi
C Jätan ikkagi selle pildi, sest mulle endale see väga meeldib
See ei ole oluline, kas sinu pilti laigitakse või mitte. Internetis on palju infot ja seetõttu ei pruugi sinu kõik postitused jõuda su sõpradeni. Laikide arv ei näita sõprade tegelikku arvamust ning sina ära muuda oma käitumist laikide saamise nimel. Aga kindlasti tuleb jääda alati viisakaks ka teiste suhtes!

111 Postitasid sõbra postituse alla inetu kommentaari, mida nüüd kahetsed. Mida teed?
A Midagi pole teha, püüan järgmine kord targem olla
B Kustutan kommentaari ära lootes, et sõber seda ei näinud
C Kustutan kommentaari ära ja vabandan sõbra ees
Kui mingi asi sind internetis kurjaks või pahaseks muudab, siis kõigepealt kirjuta oma mõtted kuhugi privaatsesse faili ja oota pool tundi, enne kui postitad. Tihti ei tahagi me halba postitust teha, kui esimene emotsioon möödas on. Kui siiski postitad solvava kommentaari, mida hiljem kahetsed, kustuta see ära ja saada kindlasti ka vabandav sõnum.

112 Sõbraga koos tehtud video sai väga populaarseks, kuid sõbrale see enam ei meeldi ja ta palub video kustutada. Mitu meeldimist (*like*) peab videol olema, et sa võiksid seda internetis alles hoida?
A 100
B 1 000 000
C Laikide arv pole oluline
Laikide arv ei muuda infot tõesemaks või seaduslikumaks.
Seega, kui keegi palub maha võtta pildi või video endast, siis peab seda tegema sõltumata sellest, kui populaarne foto või video on.
Üks võimalus on ka see, et vaatad koos sõbraga video üle ja lõikate maha need osad, mis teda häirivad.

113 Ema paneb FB kontole pildi sinust, mis sulle üldse ei meeldi. Mida teed?
A Kurdan sõpradele, kui nõmedad vanemad mul on
B Panen enda kontole emast veel nõmedama pildi
C Räägin emaga ja palun pildi maha võtta, sest mul on õigus otsustada info üle, mis minu kohta käib
Igal inimesel on õigus otsustada, millist infot tema kohta internetti postitatakse ning see kehtib ka laste puhul.
Lapsevanem peab küsima lapselt nõusolekut tema foto lisamiseks internetti ning laps ei pea oma keeldumist põhjendama.
Kindlasti ei tohi ka emast, isast või sõbrast postitada pilte ilma nende loata.

114 Mida teed, kui näed, et sinu sõbra postituse alla kirjutatakse mõnitavaid kommentaare?
A Raporteerin ebasobivast sisust
B Räägin sellest usaldusväärsele täiskasvanule
C Ei tee midagi, sest sõber peab ise selle teemaga tegelema
Kui näed internetis, et keegi käitub

ebasobivalt, siis kindlasti anna sellest teada lehe omanikule või usaldusväärsele täiskasvanule.
Väga vale teguviis on see, et kui näed, et kellelegi tehakse liiga, ja sa laigid seda halba kommentaari või postitust.

115 Kas Facebooki kinnise grupi sõnumeid võivad näha inimesed, kes pole grupi liikmed?
A Jah
B Mõni eriti tark häkker võib näha
C Ei
Internetis ei saa kunagi kindel olla, et sinna ükskõik kui privaatselt postitatud sõnumid siiski edasi ei levi. Näiteks FB-grupi puhul piisab, kui üks inimene kopeerib teksti ja postitab selle kuhugi avalikult.
Või häkitakse grupiliikme konto ja mõni võõras pääseb andmetele ligi.
Või unustab inimene end avalikus arvutis enne lahkumist kontolt välja logida ja järgmine inimene, kes arvuti taha satub, saab tema kontol rahulikult ringi vaadata.

116 Saad SMS-i tundmatult numbrilt, kuid aimad, kes see võiks olla. Kuidas käitud?
A Näitan sõnumit vanematele või õpetajale
B Vastan sõnumile ja uurin, kas saatja on see, keda arvan
C Ignoreerin sõnumit
Isegi kui oled peaaegu kindel, et see sõnum on tuttavalt, kes on numbrit vahetanud, näita ikkagi sõnumit mõnele usaldusväärsele täiskasvanule, enne kui sellele vastad. Kui otsustad siiski tagasi helistada, peida oma number juhuks, kui tegu on paha kavatsusega inimesega. Siis ta ei tea, kes helistab.
Kui saadad ise võõralt numbrilt sõnumi, pane oma nimi alla, et sellist segadust ei tekiks.

117 Millist meemi ei tohi internetti postitada?
A Teise inimese pildiga ilma tema loata
B Oma koera või kassi pildiga
C Solvava tekstiga
Meem on mingi idee, näiteks pilt, tekst või video, mida kasutatakse mingi sõnumi edastamiseks. Meemid võivad olla väga naljakad, kuid siin on oht, et need teevad mõnele inimesele haiget. Kui hakkad kellestki meemi postitama, küsi kindlasti tema nõusolekut ning solvava tekstiga meemi parem ära üldse tee. Internet on negatiivseid asju täis ja pole vaja neid sinna juurde panna.

118 Kuidas internetis vähem reklaame näha?
A Paigaldan endale reklaamiblokeerija
B Teen reklaamidest kuvatõmmised ja kirjutan tarbijakaitsele avalduse
C Näitan neid reklaame usaldusväärsele täiskasvanule
Reklaamid on tüütud, kuid enamiku ajast ei ole need otseselt ohtlikud. Seega on kõige mõistlikum installida oma veebilehitsejale reklaamide blokeerija, nii saadki ebavajalikest reklaamidest lahti. Ole laienduse paigaldamisega ettevaatlik, sest mõnikord püütakse laienduse või programmi sisse peita ka pahavara. Eelista programme ja laiendusi, millel on palju kasutajaid ja mis on pikalt kasutusel olnud.

119 Mida soovitad sõbrale, kellelt on konto kaaperdatud?
A Midagi pole teha, järgmine kord tuleb targem olla
B Võtku ühendust lehe omanikuga ja andku juhtunust teada
C Hoiatagu sõpru ja tuttavaid, sest kurjategija võib kontot kasutada nende petmiseks
Kui konto on kaaperdatud, tuleb sellest kohe teavitada lehe omanikku. Samuti peaks sellest tuttavatele teada andma, sest pätid võivad püüda tuttavatele

viirusega linke või faile saata. Kindlasti tuleb kõik paroolid ümber vahetada ka teistel kontodel, sest arvutis võib olla pahavara, mis paroolid pättidele saatis.

120 Milliselt lehelt saab infot mängude soovituslike vanusepiiride kohta?
A neti.ee
B pegi.info
C stuudium.com
PEGI (Pan European Game Information) on leht, kus on kõigi mängude kohta soovituslikud vanusepiirid ja ka see, mis põhjustel mingi vanusepiir pandud on.

Tase 5

121 Mida teeb krüptoviirus?
A Lukustab su arvuti ja nõuab raha
B Salvestab su arvuti töölauale palja naise pildi
C Saadab kõigile su sõpradele rumala kirja
Krüpto- ehk lunarahaviirus lukustab kasutaja failid ning nõuab raha, et kasutaja saaks võtme, mis aitab neid faile avada. Parim kaitse krüptoviiruse vastu on see, kui sul on värske tagavarakoopia olulistest failidest ja andmetest välisel kõvakettal või mälupulgal. On ka selliseid viiruseid, mis hakkavad su arvutis täiskasvanutele mõeldud piinlikke lehti avama ja neid su sõpradele edasi saatma.

122 Millise olukorra puhul võib olla tegu identiteedivargusega?
A Keegi varastab sinu õpilaspileti või ID-kaardi
B Keegi teeb sinu nime ja fotoga konto sotsiaalmeediasse
C Keegi ütleb vale telefoninumbri
Identiteedivargus on see, kui keegi kehastab sind, näiteks loob sinu nimega konto, kuhu paneb ka sinu pildi ja sinu kohta käiva info. Sellisel juhul tuleks salvestada võimalikult palju ja teha avaldus politseile. Dokumendi vargus võib olla esimene samm identiteedivarguse suunas, kuid kuni keegi pole neid dokumente sinu kehastamiseks kasutanud, on tegu lihtsalt dokumentide vargusega. Identiteedivargus on ka see, kui kaaperdatakse su konto ja seal sinu nimel sõnumeid saadetakse.

123 Mis või kes on *keylogger*?
A Programm, mis salvestab su tegevust ja mille abil saab kasutaja paroolid teada
B Lahe võtmehoidja, mida saab mobiiliga häält tegema panna
C Üks hästi kuulus USA juutuuber
Keylogger ehk klahvinuhk on programm, mis salvestab klaviatuuri klahvide vajutusi ja saadab selle info edasi. Niimoodi saab teada kasutaja paroolid, kontoandmed, krediitkaardinumbrid ja palju muud infot, mida on võimalik pahatahtlikult ära kasutada. Klahvinuhk on pahavara ja see võib sattuda arvutisse samal viisil nagu viirused.

124 Miks on tundmatu VPN-i (*Virtual Private Network*) kasutamine ohtlik?
A Arvuti võib plahvatada
B Võõrad inimesed võivad näha sinu paroole ja vestlusi
C VPN ei ole kunagi ohtlik
VPN ehk virtuaalne privaatvõrk on väga hea võimalus selleks, kui sul on vaja turvaliselt ligi pääseda kooli või töökoha internetivõrku.
Kui sa aga täpselt ei tea, kelle teenust kasutad, siis on risk, et sinu andmeid saab salvestada või pealt kuulata. Eriti ettevaatlik peaks olema nendega, kes pakuvad tasuta VPN-teenust. Internetis kipub kehtima reegel, et kui miski on täiesti tasuta, siis kaubaks oled järelikult sina ise.

125 Kuidas turvalised veebilehed

paroole salvestavad?
A Räsitult ehk ühesuunaliselt krüpteeritult
B Nii nagu kasutaja neid sisestab ehk algsel kujul
C Võimalikult paljudes erinevates andmebaasides
Turvalised veebilehed salvestavad paroole krüpteeritult. Krüpteerimine on nagu salakoodiga kirjutamine ja niimoodi ei saa võõras kellegi parooli teada isegi siis, kui ta andmebaasi sisse häkib.
Kahjuks on arvutid järjest võimsamad ning lühikesi ja tavalisi paroole annab ära aimata isegi krüpteeritult. Seetõttu on oluline, et kasutaksid pikki paroole, mis sisaldavad ka numbreid ja erinevaid märke.

126 Milline veebileht neist võib olla õngitsemiseks tehtud?
A facepook.com
B elu24.postimees.ee
C seb.ee.bankaccount.com
Õngitsemine (ingl phishing) on selline petuskeem, kus tehakse veebileht, mis näeb välja nagu mõni usaldusväärne leht (nt pank, e-kool, sotsiaalmeediasait või e-post), ning siis püütakse inimesi meelitada sinna lehele sisse logima, et saada kätte nende kasutajaandmeid. Õngitsuslehtede puhul on oluline osata kontrollida domeeni õigsust. Tihti suunatakse inimesi võltslehtedele e-kirja teel.

127 Milliste klahvidega saab Windowsi arvuti kiiresti lukku panna, kui arvuti juurest ära lähed?
A WIN+L
B CTRL+C
C CTRL+ALT+DEL
Kui lähed arvuti juurest eemale, siis kindlasti pane arvuti lukku. Tee seda ka kodus, sest siis ei unusta sa seda kooliarvutit või avaliku internetipunkti arvutit kasutades. Arvuti lukku panekuks võid menüü kaudu välja logida või siis kasutada klahvikombinatsiooni WIN+L
Veel mõni otsetee:
Alt + Tab – saad akende vahel liikuda
Alt + F4 – sule aktiivne rakendus
WIN+ D – peida või näita töölauda

128 Kuidas kaitsta kontaktivaba pangakaarti?
A Hoian seda rahakoti keskmises vahes
B Panen kaardi fooliumi sisse, kui ma seda ei kasuta
C Kaitsen spetsiaalse kaitsekaanega
NFC (ingl Near Field Communication) ehk lähiväljaside on uudne tehnoloogia, mida kasutatakse näiteks pangakaartides või mobiilmaksetel. NFC-kaardi kaitsmiseks on vaja takistada selle signaali, kui sa seda kaarti või seadet ei kasuta. Telefonis saab NFC-funktsiooni välja lülitada, kuid pangakaardile tasuks ümber panna foolium või osta spetsiaalne kaarditasku, mis aitab signaali peita. Rahakoti keskmises vahes hoidmine teeb signaali kättesaamise keerulisemaks, kuid lugemisseadmed muutuvad järjest võimsamaks ning tavaline rahakott pole piisav kaitse.

129 Mida saab teha veebilehel virustotal.com?
A Luua ise viiruseid
B Kontrollida kahtlaseid faile
C Kontrollida kahtlaseid veebilinke
Kui saad kahtlase manuse või saadetakse sulle link, mis tundub väga võõras, siis saad need failid ja lingid sellel lehel ära testida. Alati on parem olla veidi rohkem paranoiline, sest piisab ühest ettevaatamatust klikist valele lingile või viirusega nakatunud faili avamisest, et hakkaks juhtuma palju jama

130 Kes või mis on Anonymous?
A Rahvusvaheline häktivistide grupp
B Inimene, kes kasutab varjunime
C Üks Youtube´i kanal
Anonymous on lihtsalt üks kaubamärk, mida internetis kasutatakse päris palju. Alguses oli inimeste grupp, kes aitab avaldada salastatud infot, mida nende meelest ei tohiks salastada. Praegu on ka sellenimeline Youtube'i kanal, kuid tegelikkuses võib igaüks selle maski pähe panna ja internetti mõne üleskutse postitada. Kuna esmapilgul on väga keeruline aru saada, mis sellise üleskutse eesmärk on, siis ole hästi ettevaatlik infoga, mis sinuni sellenimelistest allikatest tuleb.

131 Milline aine ajus tekitab nutisõltuvust?
A Dopamiin
B D-vitamiin
C Doping
Dopamiin on virgatsaine, mis vabastatakse meie ajus siis, kui juhtub midagi meeldivat ja meil tekib rahuldustunne. Kui meil teatud aja jooksul on dopamiini tase kehas kõrgem, harjume sellega ära ning kui tase langeb, siis on meil paha olla. Paljud rakendused on disainitud nii, et nende kasutamine vabastab dopamiini ja seetõttu soovime järjest rohkem neid kasutada ning nii võibki tekkida sõltuvus.

132 Millal loodi Google'i otsing?
A 1991
B 1996
C 2001
Google'i otsingu lõid 1996. aastal kaks Stanfordi ülikooli tudengit – Larry Page ja Sergey Brin.
Veel aastaarve:
2003 – Skype (asutajad Priit Kasesalu ja Jaan Tallinn)
2004 – Gmail
2005 – Youtube
2006 – Facebook
2010 – Instagram

133 Mida tähendab viraalne?
A Haigena arvutimängude mängimine
B Kui arvutis on palju viiruseid
C Kui meemid levivad väga kiiresti
Viraalne tähendab seda, et pilt, tekst, või mingi muu meem levib väga kiiresti, sest kõik tahavad seda jagada.
Häda on selles, et niimoodi võib levida ka valeinfo või mõni pilt, mis on pandud üles ilma pildil oleva inimese loata. Ja kui postitus viraalseks muutub, on seda väga keeruline kustutada.
Seetõttu ole eriti ettevaatlik sellega, mida edasi jagada otsustad.

134 Kes või mis on Amanda Todd?
A Tuntud häkker
B Kanada tüdruk, kes tegi küberkiusamise tõttu enesetapu
C Viirus, mis kustutab kõik dokumendid sinu arvutist
Kanada koolitüdruk Amanda Todd hakkas internetis suhtlema võõra inimesega, kes alguses tundus väga tore ja sõbralik. Mingi hetk saatis ta sellele inimesele väga isikliku pildi endast, kus tal pluusi seljas polnud. Seejärel hakkas see inimene temalt täiendavat infot välja pressima, lubades muidu selle pildi avalikult internetti panna. Asi läks aina hullemaks ning lõpuks tegi tüdruk enesetapu. Kui keegi hakkab sinult internetis välja pressima või sind ähvardama, lõpeta kohe selle inimesega suhtlemine ja räägi juhtunust usaldusväärsele täiskasvanule.

135 Kui ma teen Google'is otsingu 'eesti and kass -must', siis milliseid tulemusi kuvatakse?
A Eesti mustad kassid
B Eesti kassid
C Eesti kassid, kes ei ole mustad
Google'i otsingus tähendab sõna and seda, et soovid näha tulemusi, kus on

mõlemad sõnad sees. Miinusmärk otsingusõna ees tähendab, et seda sõna ei tohi otsitavas tekstis olla. Lisaks saab Google'is otsida ka näiteks failitüübi järgi. Filetype:pdf kuvab ainult tulemusi, kus otsitav tekst on PDF-failina. Pannes teksti jutumärkidesse, saad tulemusena konkreetse fraasi.

136 Mis asi on protsessor?
A Õpetaja, kes töötab ülikoolis
B Arvuti „aju", ilma milleta nutiseade ei töötaks
C Äpp, millega saab Instagrami jaoks põnevaid videoid teha
Protsessor on nagu nutiseadme aju, mis määrab ära, kui kiire või aeglane su seade on.
Selle ülesandeks on programmide käivitamine, andmete töötlemine ning sisend- ja väljundseadmete töö koordineerimine.
Mõnikord võib arvutis olla ka mitu protsessorit.

137 Mida saab teha energiaga, mis kulub ühe suure manusega e-kirja saatmiseks?
A Panna taskulambi 2 sekundiks tööle
B Sõita autoga kümme kilomeetrit
C Keeta tassitäis teevett
Meile võib tunduda, et internetis juhtuvad asjad maagiliselt, väga vähe mõeldakse selle peale, kui palju energiat interneti jaoks kulub. Enne kui meie kiri jõuab õige saajani, läbib see kümneid kui mitte sadu arvuteid ja kulutab energiat. Samamoodi kulutab energiat igasugune otsing. Kuigi Google püüab oma otsingumootoreid optimeerida ja meile tundub, et selle sekundiga ei kulu ju miskit, siis tegelikult on ka see tegevus energiamahukas.

138 Mis on plagiaat?
A Valeinfo levitamine
B Loomevargus
C Suur bänner
Plagiaat on loomevargus ehk kellegi teise tehtud töö esitamine enda nimel. Kõige sagedamini on plagiaati koolitöödes, kus kopeeritakse veebis või kellegi teise koolitöös olevat teksti ja ei viidata allikale. Plagiaat on koolis ja ülikoolis väga suur rikkumine ning selle tulemusena võidakse õpilane kooli nimekirjast ka välja arvata. Ole väga ettevaatlik tekstiga, mille sa kuskilt enda töösse lõikad ja kleebid – seda tuleb alati viidata.

139 Kui mõni sõber, kellega tutvusid internetis, tahab kohtuda, siis mida teed?
A Lepin kokku aja ja koha – kodus kuulen kogu aeg, et sõpradega peab ka päriselt kokku saama
B Räägin oma vanematele ja küsin, kuidas käituda
C Ma ei kohtu inimesega, kellega tutvusin internetis. See pole turvaline.
Kohtumine inimesega, keda tead ainult interneti kaudu, võib olla väga ebaturvaline ja ohtlik.
Kui siiski on vaja mingil põhjusel kohtuda, siis räägi sellest kõigepealt vanematele ja küsi neilt nõu. Juhul kui vanemad on kohtumisega nõus, vali kohtumispaigaks koht, kus on palju inimesi ja turvakaamerad. Kõige parem on minna koos usaldusväärse täiskasvanuga, kes vajadusel sekkuda saab.

140 Saad sõbralt kirja, kus on manus, mida sa ei oodanud. Mida teed?
A Avan manuse ja saan teada, miks sõber selle saatis
B Küsin sõbralt, kas tema saatis selle manuse ja mis seal on
C Küsin oma vanematelt, kas on OK seda manust avada
Ainult sõber oskab öelda, kas ta saatis sulle kirjaga manuse või mitte. Kui sõbra arvuti on nakatunud pahavaraga, võib see kiri olla hoopis pahavara katse nakatada ka sinu arvuti. Helista sõbrale ja uuri, kas ta tahtis sulle seda faili saata ja kas ta on kindel, et selles ei ole pahavara või viirust. Kui ta ei tea kirjast midagi, kustuta see kiirelt.

141 Näed internetis videot, kus ühte teie kooli õpilast pekstakse. Mida teed?
A Saadan lingi klassi vestlusgruppi, et uurida välja, kes on ohver
B Leian kohe usaldusväärse täiskasvanu ja näitan talle seda videot
C Saadan video lingi õpetajale või kooli direktorile
Võimalusel näita seda videot kohe õpetajale või direktorile. Kui näed seda videot väljaspool kooli, saada õpetajale e-kiri või näita usaldusväärsele täiskasvanule, kes sellest politseid teavitaks. Kindlasti ära jaga videot edasi, isegi mitte klassikaaslaste gruppi.

142 Mida teha, kui mängus keegi uurib sinult, kas sa mängult seksida tahad?
A Login välja ja kustutan konto
B Teen kuvatõmmise ja lähen otsin kiirelt usaldusväärse täiskasvanu
C Ignoreerin teda ja mängin edasi
Mitte üheski lastemängus ei tohi keegi alaealise kasutajaga seksist rääkida. Kui keegi seda teeb, siis see on kuritegu ja sellest tuleb politseid teavitada. Tee vestlusest kuvatõmmis (screenshot) ja näita seda esimesel võimalusel usaldusväärsele täiskasvanule, kes saab info politseile edasi saata. See, kui keegi sinuga ebasobivatel teemadel suhelda tahab, ei tähenda, et sina oleks midagi valesti teinud!

143 Näed internetis videot, mis on väga vägivaldne ja hirmutab sind. Mida teed?
A Sulgen video ja püüan selle ära unustada
B Panen video pausile ja lähen otsin usaldusväärse täiskasvanu, kellele räägin, mida ma nägin
C Saadan lingi sõpradele ja küsin, mis nemad arvavad
Kui näed internetis videot, mille sisu sind häirib (vägivald, paljad inimesed vms), siis pane video kohe pausile ja kutsu mõni usaldusväärne täiskasvanu, kes oskab seletada, miks selline video on internetis ja kas peaks ehk politseid teavitama. Kindlasti ära jaga selliseid videoid oma sõpradega.

144 Sulle saadab sõnumi võõras, kes väidab, et teab, kus sa elad. Mida teed?
A Näitan sõnumit kohe usaldusväärsele täiskasvanule
B Teen sõnumist kuvatõmmise (*screenshoti*) ja blokeerin sõnumi saatja
C Ignoreerin sõnumit ja toimetan edasi
Kui keegi võõras väidab, et ta teab, kus sa elad, siis tuleb see sõnum kindlasti salvestada ja sellest ka usaldusväärset täiskasvanut teavitada. Väga võimalik, et tegu on rumala naljaga, kuid alati on parem sellistest vahejuhtumitest rääkida. Kindlasti ei tohi ise selle võõraga pikemalt suhtlema hakata teemal, et kust ja kuidas ta teab, sest mõnikord püütakse sellise alguslausega hoopis sind ennast oma aadressi avaldama panna.

145 Mida teha, kui näed täiesti võõrast inimest kooli ees pildistamas?
A Teen temast foto ja postitan Facebooki
B Lähen ja küsin, miks ta pildistab
C Lähen otsin usaldusväärse täiskasvanu, kes uuriks, miks ta pildistab
Võib palju erinevaid põhjuseid olla, miks keegi kooli ees pilte teeb, ta võib olla ajakirjanik, ehitaja, kohalik ametnik jne. Kindlasti ei tohi üle reageerida, näiteks teha FB-postitus „kahtlane inimene" vms. Kui olukord tundub kahtlane, siis leia mõni täiskasvanu, kes läheb ja uurib, mis toimub. Viisakas pöördumine head inimest ei häiri, aga pahade kavatsustega inimene läheb minema, kui teda märgatakse.

146 Tahan õpetajale e-kirja saates koopia kirjast ka emale saata. Mis väljale on viisakas ema e-post sisestada?
A To:
B Cc:
C Bcc:
E-kirjal on kolm erinevat välja, kuhu saab aadressi kirjutada. To: (Kellele:) väljale kirjutatakse need aadressid, kellele kiri on mõeldud ja kellelt soovid ka vastust. Cc: (Koopia:) väljale pane need inimesed, kellele on kiri infoks mõeldud ja kellelt aktiivset vastust sa ei oota. Kolmas väli on Bcc: (Pimekoopia:) ning sinna pannakse need kirja saajad, keda soovid nii informeerituna hoida, et teised kirja saajad sellest ei teaks. Koopia saajad on viisakas panna Cc: väljale, et kõik seda infot näeks.

147 Käid oma lemmikartisti kontserdil ja salvestad selle videole. Kas tohid videot sõpradega jagada?
A Ikka tohin
B Ainult siis, kui mul on sõbralistis vähem kui 300 sõpra
C Ei tohi ilma artisti loata
Kui sa salvestad kellegi esinemist, siis ei kuulu selle video autoriõigused sulle, vaid artistile, keda salvestad. Kui soovid seda videot sõpradega jagada, siis peaksid ka artistilt endalt luba küsima. Soovitus: kui lähed kontserdile, naudi emotsioone ja ära näe vaeva salvestamisega – internet on kehva kvaliteediga videoid täis ning ega muusikutele ka ei meeldi, kui enamik inimesi kontserdi nautimise asemel seda nutiseadmetega filmivad.

148 Mis asi on asukohamärgis (*geotag*)?
A Kood, mis näitab pildi tegemise täpset asukohta
B Üks lahe rakendus, mis aitab geograafiat õppida
C Viirus, mis nakatab ainult ühes riigis olevad arvutid
Asukohamärgis on kood, mis pannakse pildifaili sisse. Seal on kirjas täpne pikkus- ja laiuskraad, kus pilt tehtud on. Telefoni seadetest saab muuta seda, kas kaameral on ligipääs asukohale või mitte.
Kui asukohamärgise info on faili lisatud, saab iga huviline kiirelt teada foto tegemise täpse asukoha.

149 Miks tehakse manipuleerimisründeid (*social engineering*)?
A Inimesi petta on lihtsam kui masinaid
B Tehakse siis, kui pätid ei oska programmeerida
C Nii saab rohkem nalja
Manipuleerimisrünnete (ingl social engineering) käigus kasutatakse ära inimeste psühholoogiat, meelitades või ähvardades neid kurjategijale soovitul viisil. Näiteks e-kirjades lubatakse lotovõitu või suurt palka, teeseldakse kedagi teist (nt kõne pangast) või kasutatakse libakontosid, et inimest endaga suhtlema meelitada. Selliste

rünnakute eesmärgiks võib olla pahavara sokutamine arvutisse või andmete väljameelitamine.

150 Millise laiendiga faili avamisel peab ettevaatlik olema?
A .exe
B .gif
C .doc
Kõik failid võivad teatud olukordades ohtlikud olla ning avada ei tohi ühtegi faili, mille usaldusväärsuses sa kindel ei ole. Kui sõber saadab sulle faili või lingi ilma täpsustamata, mis selles on, siis uuri enne faili avamist see järele. On olemas viirused, mis häkivad e-posti või sotsiaalmeediakontod ära ning hakkavad siis nakatunud faile saatma kontol olevatele kontaktidele.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Diana Poudel,

1. Annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose

Digipädevusi arendava õpimängu "Häkkerite lahing" loomine,

mille juhendaja on Maria-Murumaa Mengel (Phd),

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Diana Poudel

29.05.2019