L2D

MEDIA LITERACY COMPETENCES FOR YOUTH WORKERS

JUHISED INTERNETI OHUTUKS KASUTAMISEKS

ONLINE TURVAMOODUL

`

Pealkiri:	JUHISED INTERNETI OHUTUKS KASUTAMISEKS
Märksõnad:	Veebiohutus, Interneti-ohutus, digitaalne privaatsus, küberturvalisus, turvalised võrgutavad, privaatsus, andmeturve, paroolihaldus, võrguohud, väärkasutusest teatamine, privaatsusseaded
Valmistas:	
Keel:	Eesti
Eesmärgid:	● Veebiohutuse määratlemine: selgitage võrguohutuse mõistet ja selle tähtsust tänapäeva digimaailmas. ● Võrguohtude tuvastamine: aidake õppijatel ära tunda erinevaid võrguohtusid, nagu andmepüük, pahavara, identiteedivargus, küberkiusamine ja pettused. ● Privaatsusprobleemide mõistmine: suurendage osalejate teadlikkust isikliku teabe võrgus kaitsmise tähtsusest ja privaatsusrikkumiste võimalikest tagajärgedest. ● Tugevate paroolide väljatöötamine: õpetage konto turvalisuse suurendamiseks tugevate unikaalsete paroolide loomise tehnikaid. ● Andmepüügikatsete eest kaitsmine: pakkuge strateegiaid andmepüügimeilide, sõnumite ja veebisaitide tuvastamiseks ja nende ohvriks langemise vältimiseks. ● Turvalised sotsiaalmeedia profiilid: pakkuge juhiseid privaatsusseadete kohandamiseks, isikliku teabe jagamise kontrollimiseks ja sõbrakutsete haldamiseks. ● Turvalise võrgusuhtluse edendamine: õpetage tõhusaid meetodeid turvaliseks suhtluseks sotsiaalmeedias, foorumites ja sõnumiplatvormidel, rõhutades tundlike andmete jagamise vältimist. ● Kriitilise mõtlemise arendamine: edendage teabe ja allikate kriitilise hindamise oskust, eriti "võltsuudiste" ja veebipõhise desinformatsiooni kontekstis. ● Võrguahistamise ja jälitamisega tegelemine: andke nõu, kuidas reageerida võrgus ahistamise või jälitamise juhtumitele ja sellest teavitada.
Õpitulemused:	
Sisuindeks:	

Co-funded by the European Union

	2.2. TUNNISTA HOIATUSMÄRGID 2.3. ONLINE OHUTUSTE IGORRAMISE TAGAJÄRGED 3. ISIKUANDMETE KAITSE 3.1. PRIVAATSUSKAITSE TÄHTSUS 3.2. TURVALINE ONLINE KONTO HALDUS 3.3. VASTUTUSTULINE SOTSIAALMEEDIA JAGAMINE 4. SIRVI OHUTU SOTSIAALMEEDIAS 4.1. PRIVAATSUSSÄTETE KOHANDAMINE 4.2. HALDAGE SÕBRA TAOTLUSID JA SÕNUMID 4.3. TEATA JA BLOKERI KURITAV KONTOD 5. KÜBERTURVASED JA MOBIILSEADMED 5.1. TURVALINE NUTITELEFONID JA TABLETTID 5.2. RAKENDUSE KASUTUSLOAD JA JUURDEPÄÄS ANDMETELE KAITSKE MOBIILSEADMEID VARGUSE JA KAOTUSE EEST
Sisu arendus:	1. INTERNETI TURVALISUS 1.1. INTERNETI TURVALISUSE MÄÄRATLUS Interneti-turvalisus, tuntud ka kui võrguturvalisus, on tava järgida kehtivaid juhiseid, omandada igakülgne arusaam kaasaegsest tehnoloogiast ja kaitsta ennetavalt oma digitaalseid seadmeid, et kaitsta end võrgumaailma erinevate pahatahtlike aspektide eest. Kuna Interneti-kasutajate arv kogu maailmas kasvab, tunnevad mitmed sidusrühmad, sealhulgas valitsused, organisatsioonid ja Interneti-teenuse pakkujad, üha enam muret haavatavate elanikkonnarühmade, nagu lapsed, noorukid ja vanurid, turvalisuse pärast, kui nad sisenevad tohutusse virtuaalsesse keskkonda. valdkond. Murettekitav statistika näitab, et enam kui 45% Interneti-kasutajatest on teatanud, et on langenud mingisuguse küberkiusamise vormi ohvriks, mis rõhutab tungivat vajadust edendada turvalisemaid võrgutavasid ja kasvatada digitaalse vastutuse kultuuri. Nende pakiliste probleemide lahendamiseks ja turvalisema digimaastiku propageerimiseks tähistatakse igal veebruaril ülemaailmselt turvalise Interneti päeva. See iga-aastane üritus toimib spetsiaalse platvormina Interneti-ohutuse teadlikkuse tõstmiseks, julgustades üksikisikuid ja

	kogukondi olema oma võrgusuhtluses valvsad, informeeritud ja ennetavad. Valitsused, mittetulundusühingud ja tehnoloogiaettevõtted üle maailma osalevad aktiivselt turvalise Interneti päeva algatustes, korraldades teadlikkuse tõstmise kampaaniaid, harivaid töötubasid ja interaktiivseid üritusi, et anda internetikasutajatele teadmisi ja oskusi, mis on vajalikud veebimaailmas turvaliseks navigeerimiseks. Ühendkuningriigis on kampaania Get Safe Online end tõestanud juhtiva jõuna Interneti-ohutuse edendamisel. Valitsuse tõsiste organiseeritud kuritegude agentuuri (SOCA) olulise sponsorluse ja suuremate Interneti-ettevõtete, nagu Microsoft ja eBay, kampaania eesmärk on anda Interneti-kasutajatele praktilisi nõuandeid ja ressursse, et end küberohtude eest kaitsta. Tänu hõlpsasti juurdepääsetavale teabele, nõuannetele ja tööriistadele aitab Get Safe Online parandada üksikisikute digitaalset vastupanuvõimet, muutes Ühendkuningriigi Interneti-kogukonna tugevamaks ja vähem haavatavaks võrguohtude suhtes. Kuna internet areneb edasi ja mängib meie igapäevaelus üha olulisemat rolli, muutub turvalisuse tagamine Internetis oluliseks. Julgustades vastutustundliku käitumise kultuuri veebis, tõstes teadlikkust selliste algatuste kaudu nagu turvalisema Interneti päev ja pakkudes juurdepääsetavaid ressursse, nagu kampaania Get Safe Online, saame ühiselt töötada selle nimel, et luua turvalisem ja turvalisem digitaalne keskkond kõigile. Meie alati ühendatud maailmas ei saa Interneti-turvalisuse tähtsust üle tähtsustada. Internet pakub võrratuid võimalusi õppimiseks, suhtlemiseks ja meelelahutuseks, kuid seab kasutajad ka potentsiaalsetele riskidele ja ohtudele. Kuna tehnoloogia areneb ja võrguohud muutuvad keerukamaks, on igas vanuses inimeste jaoks oluline olla Interneti-ohutusega kursis ja ennetav. Laste ja teismeliste jaoks, kes on sageli digitaalsed põliselanikud, on Interneti-ohutuse mõistmine vastutustundliku ja turvalise võrgusuhtluse jaoks hädavajalik. Vanematel, kasvatajatel ja eestkostjatel on oluline roll noorte Interneti-kasutajate juhendamisel, õpetades neile isikuandmete jagamise, võõrastega suhtlemise ja ohtlikes veebitegevustes osalemise võimalikke riske. Interneti-turvalisuse parandamiseks on oluline olla kursis küberturvalisuse viimaste suundumuste ja parimate tavadega. Tarkvara ja rakenduste regulaarne värskendamine,

	maineka viirusetõrjetarkvara kasutamine ja automaatsete värskenduste lubamine võivad tugevdada digitaalseadmete kaitset tekkivate ohtude eest. Lisaks lisab võimaluse korral mitmefaktorilise autentimise integreerimine veebikontodele täiendava kaitsekihi. Positiivse ja turvalise veebikogukonna edendamine hõlmab ka digitaalse empaatia ja austuse edendamist. Lahkuse ja empaatia julgustamine võrgusuhtluses aitab võidelda küberkiusamise ja mürgise käitumisega ning muudab Interneti kõigile meeldivamaks ruumiks. 1.2. Saage aru KOHALDAMISEST JA TÄHTSUSEST 1.2.1. Interneti-turvalisuse ulatus ● Kaitse küberohtude eest, nagu viirused, pahavara, andmepüügi, lunavara ja identiteedivargused. ● Kaitske isiklikku teavet ja digitaalset identiteeti volitamata juurdepääsu ja väärkasutuse eest. ● Liikuge sotsiaalmeedias vastutustundlikult ja tegelege küberkiusamise või veebiahistamisega. ● Tagada veebitehingute turvalisus ja kaitsta finantsteavet veebis ostes või pangas ostes. ● Kasutage ja hallake mobiilseadmeid turvaliselt, et vältida andmete ja privaatsuse rikkumisi. ● Tuvastage ja vältige võrgupettusi, petturlikke veebisaite ja andmepüügikatseid. ● Õpetage lastele ja noorukitele veebiturvalisust ning aidake neil kujundada vastutustundlikke digiharjumusi. 1.2.2. Interneti-turvalisuse tähtsus ● Isiku- ja finantsteabe kaitse: Interneti-turvameetmed kaitsevad tundlikke andmeid, vältides identiteedivargust ja finantspettusi. ● Säilitage privaatsus ja digitaalne maine: võrgutegevuste tähelepanelikkus aitab inimestel säilitada oma privaatsust ja kaitsta oma digitaalset mainet. Kaitse küberohtude eest: võrguriskidest teadlik olemine ja turvatavade järgimine aitab kaitsta küberohtude eest, mis võivad elu häirida ● igapäevane äritegevus või tundliku teabe kahjustamine. ● Positiivsete digitaalsete kogemuste reklaamimine: Interneti-turvalisus võimaldab inimestel saada veebis positiivseid ja rikastavaid kogemusi, kartmata ahistamist või ohvriks langemist.

	● Julgustada digitaalset kodakondsust. Interneti-turvalisusega aitavad inimesed kaasa vastutustundliku ja lugupidava digitaalse kogukonna loomisele. Majanduslik mõju: küberjulgeolekuintsidentidel võivad olla üksikisikutele, ettevõtetele ja valitsustele tõsised majanduslikud tagajärjed, muutes Interneti-turvalisuse üldise turvalisuse oluliseks aspektiks. ● Kaitske haavatavaid inimesi: Interneti-ohutus on eriti oluline lastele, noorukitele ja haavatavatele elanikkonnarühmadele, kes võivad olla võrguohtudele vastuvõtlikumad. 1.3. TURBEKONTSEPTSIOONIDE EVOLUTSIOON INTERNETIS Interneti-turvalisuse kontseptsioonide areng viitab sellele, kuidas arusaam Interneti-turvalisusest ja kasutajate võrguohtude eest kaitsmiseks võetud meetmed on aja jooksul arenenud. Kuna Internet on kasvanud ja muutunud, on küberohtudest tulenevad väljakutsed suurenenud, mis on viinud uute kontseptsioonide ja strateegiate väljatöötamiseni veebiturvalisuse tagamiseks. Selles jaotises vaadeldakse ajaloolist konteksti ja peamisi verstaposte, mis on kujundanud Interneti-turvalisuse tavasid. ● Varajane Internet: Interneti algusaegadel oli võrguturbe kontseptsioon suhteliselt lihtsustatud. Enamik kasutajaid olid tehnoloogiliselt teadlikud isikud või spetsialistid, kes mõistsid isikuandmete veebis jagamisega seotud riske. Siiski oli avalikkuse teadlikkus võimalikest küberohtudest vähe. Veebisuhtluse tõus: Interneti-suhtlusplatvormide ja sotsiaalmeedia esilekerkimisega on Interneti-turvalisus võtnud uued mõõtmed. Kasutajad hakkasid rohkem isiklikku teavet jagama, mis tõi kaasa kasvavad privaatsusprobleemid. ● privaatsuse kaitse ja identiteedivargus. Sellised mõisted nagu andmepüük ja rämpspostid on hakanud esile kerkima, kuna küberkurjategijad püüavad kasutajate usaldust ära kasutada. ● Küberturvalisuse teedrajavad meetmed: ohtude paljunemisega silmitsi seistes on küberturvalisuse meetmed hakanud arenema. Viirusetõrjetarkvarast, tulemüüridest ja krüpteerimistehnoloogiatest on saanud olulised vahendid pahavara ja volitamata juurdepääsu eest kaitsmisel. Need varajased küberturvalisuse lahendused panid aluse arenenumatele kaitsemehhanismidele tulevikus.

	● Teadlikkuse tõstmise kampaaniad ja algatused. Küberohtude leviku tõttu on mitmed organisatsioonid, valitsused ja tehnoloogiaettevõtted alustanud teadlikkuse tõstmise kampaaniate ja algatustega, et harida avalikkust Interneti-ohutuse teemal. Nende jõupingutuste eesmärk oli tõsta teadlikkust levinud võrguriskidest ja julgustada kasutajaid kasutama turvalisemaid võrgutavasid. ● Kasvav mure küberkiusamise pärast: sotsiaalmeedia ja võrgusuhtluse tõus on toonud tähelepanu ka küberkiusamise probleemile. Kuna veebiahistamise ja küberkiusamise juhtumid sagenevad, on Interneti-turvalisusega seotud jõupingutused suurenenud, et võidelda selle digitaalse agressiooni vormiga ja toetada neid. ● Mobiilne internet ja uued väljakutsed: nutitelefonide ja mobiilse Interneti-juurdepääsu tulek on toonud kaasa uued väljakutsed Interneti-turvalisusele. Mobiilseadmetega seotud ainulaadsed riskid, nagu rakenduste load ja mobiili pahavara, nõudsid kohandatud turvameetmeid. ● Autentimise edusammud: kuna paroolid on osutunud veebikontode kaitsmiseks ebapiisavaks, on populaarsust kogunud kahefaktoriline autentimine (2FA) ja mitmefaktoriline autentimine (MFA). Need meetodid pakuvad täiendavat turvalisust, vähendades volitamata juurdepääsu ohtu. ● Rõhk digitaalsele kirjaoskusele: Interneti-turvalisuse kontseptsioonid on hakanud hõlmama mitte ainult tehnilisi turvameetmeid, vaid ka digitaalset kirjaoskust ja kriitilise mõtlemise oskusi. Kasutajate koolitamine valeinformatsiooni, võltsuudiste ja veebipettuste tuvastamiseks on muutunud võrguohtude vastu võitlemisel üliolulisek s. Küberjulgeolekutööstuse tõus: küberohtude arenemine on loonud tugeva küberjulgeolekutööstuse. Küberturbeteenustele, ohuanalüüsile ja intsidentidele reageerimisele spetsialiseerunud ettevõtted ja spetsialistid on mänginud üliolulist rolli pidevalt arenevate võrguriskide eest kaitsmisel. Interneti-turvalisuse integreerimine haridusse: tunnistades Interneti-ohutusalase hariduse tähtsust, on koolid ja haridusasutused hakanud seda oma õppekavadesse integreerima. Lastele ja noortele täiskasvanutele vastutustundliku veebikäitumise ja digitaalse kodakondsuse õpetamisest on saanud tänapäevase hariduse oluline aspekt.

	Meediaõpetus on õppeaine, mis tekkis eesmärgiga anda inimestele kõik vajalikud vahendid, et paremini mõista meedia pakutavat dünaamikat ja sõnumeid ning neid iseseisvalt ja kriitiliselt ümber töötada. ● Tänapäeval on vaja õpetada inimesi paremini juhtima oma suhet sotsiaalmeediaga, harida ja koolitada neid teemal "mida ja kuidas postitada" või kuidas "võltsuudiseid" ära tunda. Interneti kasutamine tänu nutitelefonidele pakub lõputut õppimispotentsiaali, aga ka riske, mis on seotud "nende tööriistade pealiskaudse kasutamisega". Kõige rohkem puutuvad kokku „digitaalsed immigrandid“, kuna nad pole harjunud hallama virtuaalmaailma kirjutamata reegleid, kuhu nad ei kuulu. Sageli ei tunne nad peamisi sidesüsteeme ja neil puudub suutlikkus uusi sõnumeid töödelda, et anda kogukonnale oma panus, jäädes seega passiivseteks elementideks. 1.4. Turvalise võrgukogemuse põhielemendid "Turvalise võrgukogemuse põhielemendid" on olulised elemendid, mis aitavad Interneti kasutamisel luua turvalise ja kaitstud keskkonna. Need elemendid hõlmavad erinevaid tavasid, käitumisviise ja tööriistu, mida üksikisikud saavad kasutada oma ohutuse ja privaatsuse tagamiseks võrgus. Nende põhielementide mõistmine ja rakendamine on positiivse ja turvalise Interneti-kogemuse jaoks hädavajalik. Küberturvalisuse teadlikkus: hea küberturvalisuse teadlikkus on turvalise veebikogemuse jaoks hädavajalik. See seisneb viimaste küberohtudega kursis olemises, levinud ründe meetodite (nt andmepüügi ja pahavara) mõistmises ning kahtlase tegevuse hoiatusmärkide äratundmises. Teadlikkus annab inimestele võimaluse teha teadlikke otsuseid ja võtta vajalikke ettevaatusabinõusid digimaailmas navigeerimisel. ● Privaatsus: privaatsus on Interneti-turvalisuse oluline aspekt. Selle eesmärk on olla ettevaatlik võrgus jagatava teabe suhtes ja vältida liiga paljude isiklike andmete avaldamist. Tundlike andmete, nagu finantsteave ja isikut tõendavad dokumendid, kaitsmine on identiteedivarguste ja pettuste ärahoidmiseks hädavajalik. ● Tugev autentimine: veebikontode puhul on oluline kasutada tugevaid autentimismeetodeid. Nende hulka kuuluvad tugevate unikaalsete paroolide kasutamine iga konto jaoks ja täiendavate turvakihtide, näiteks kahefaktoriline autentimine (2FA) või biomeetriline

	autentimine, kui see on saadaval. Tugevad autentimismeetmed aitavad vältida volitamata juurdepääsu kontodele ja kaitsta tundlikku teavet. ● Ohutu sirvimise tavad: pahatahtlike veebisaitide ja võimalike ohtude vältimiseks on vaja omaks võtta turvalise sirvimise harjumused. Nende hulka kuuluvad veebisaitide URL-ide kontrollimine enne tundliku teabe sisestamist, kahtlastel linkidel või hüpikakendel klõpsamise vältimine ja sisseehitatud kaitsetega turvaliste brauserite kasutamine. ● Regulaarsed tarkvaravärskendused: tarkvara, operatsioonisüsteemide ja rakenduste ajakohasena hoidmine on turvalise võrgukogemuse tagamiseks hädavajalik. Regulaarsed värskendused sisaldavad sageli turvapaiku, mis parandavad teadaolevaid haavatavusi, muutes küberkurjategijatel nende ärakasutamise raskemaks. ● Turvalised võrgud: turvaliste ja usaldusväärsete võrkudega ühenduse loomine on edastatavate andmete kaitsmiseks hädavajalik. Oluline on vältida avalikke WiFi-võrke ilma piisavate turvameetmeteta, et vältida võimalikku andmete pealtkuulamist ja volitamata juurdepääsu. ● Ohutu sotsiaalmeedia tavad. Isikliku teabe kaitsmiseks ja sotsiaalse manipuleerimise rünnakute ohvriks langemise vältimiseks on oluline olla sotsiaalmeediaplatvormide kasutamisel ettevaatlik. Privaatsusseadete kohandamine, sõbrakutsete valimine ja delikaatsete andmete avalikust jagamisest hoidumine on olulised sotsiaalmeedia ohutuse tavad. ● Valvsus andmepüügi vastu: oluline on olla andmepüügikatsete suhtes valvs. See hõlmab meili saatjate identiteedi kontrollimist, kahtlastel linkidel mitte klõpsamist või tundmatutest allikatest manuste allalaadimist ning andmepüügikatsetest teatamist. ● Vanemlik kontroll ja järelevalve: vanemate ja eestkostjate jaoks on vanemliku kontrolli rakendamine ja laste võrgutegevuste jälgimine noorte kasutajate turvalise Interneti-kogemuse olulised osad. See aitab tagada eakohase juurdepääsu sisule ja kaitseb lapsi potentsiaalselt kahjuliku veebisisu eest. ● Digitaalne kirjaoskus ja kriitiline mõtlemine: digitaalse kirjaoskuse ja kriitilise mõtlemise arendamine on väärinformatsiooni, võltsuudiste ja veebipettuste tuvastamiseks hädavajalik. Teabeallikate hindamise ja sisu

	usaldusväärsuse kontrollimise mõistmine aitab kaasa turvalisemale veebikogemusele. 2. ONLINE OHUD 2.1. ONLINE OHUTUSTE LIIGID Interneti-ohtude tüübid viitavad mitmesugustele pahatahtlikele tegevustele ja rünnetele, mis võivad ohustada Interneti-kasutajate ja nende andmete turvalisust, privaatsust ja terviklikkust. Nende ohtude mõistmine on vajalik asjakohaste ettevaatusabinõude võtmiseks ja enda kaitsmiseks digitaalsel maastikul navigeerimisel. Siin on mõned levinumad võrguohtude tüübid. Andmepüük: andmepüük on petlik tehnika, mida küberkurjategijad kasutavad, et meelitada kasutajaid avaldama tundlikku teavet, nagu sisselogimisandmed, finantsandmed või isikuandmed. Andmepüügikatsed hõlmavad sageli võltsitud e-kirju, veebisaite või sõnumeid, mis esinevad seaduslike üksustena, et meelitada ohvreid oma teavet esitama. Pahavara: pahavara on pahatahtlik tarkvara, mis on loodud seadmete või võrkude nakatamiseks ja kahjustamiseks. Nende hulka kuuluvad viirused, ussid, troojalased, lunavara ja nuhkvara. Pahavara võib kahjustada andmeid, varastada teavet, häirida toiminguid või isegi muuta seadmed kasutuskõlbmatuks. Lunavara: lunavara on spetsiifiline pahavara, mis krüpteerib kasutaja andmed, takistades neil juurdepääsu oma failidele või süsteemidele. Küberkurjategijad nõuavad dekrüpteerimisvõtme andmiseks lunaraha, kuid pole mingit garantiid, et lunaraha maksmine toob kaasa andmete tagastamise. Sotsiaalne manipuleerimine: sotsiaalne manipuleerimine hõlmab inimestega manipuleerimist, et saada volitamata juurdepääs tundlikule teabele või süsteemidele. Seda saab teha identiteedivarguse, manipuleerimise või inimpsühholoogia ärakasutamise teel, et meelitada kasutajaid avaldama konfidentsiaalset teavet. Andmerikkumine: andmetega seotud rikkumine toimub siis, kui küberründajad saavad volitamata juurdepääsu organisatsiooni või üksikisiku andmetele. See võib hõlmata isikuandmeid, finantsdokumente või intellektuaalomandit.

	Andmerikkumistel võivad olla tõsised tagajärjed üksikisikute privaatsusele ja põhjustada identiteedivargust või rahalist kahju. Identiteedivargus: identiteedivargus hõlmab isikuandmete (nt sotsiaalkindlustuse numbrite, krediitkaardiandmete või sisselogimisandmete) varastamist, et teeselda, et olete keegi, kes te ei ole. muul viisil pettuse eesmärgil. Küberkurjategijad saavad seda varastatud teavet kasutada kasumi teenimiseks või muude kuritegude toimepanemiseks. Küberkiusamine: küberkiusamine on võrgus ahistamise või hirmutamise vorm, mis tavaliselt toimub sotsiaalmeedia platvormidel või sõnumirakenduste kaudu. See hõlmab haavavate sõnumite saatmist, kuulujuttude levitamist või piinliku sisu jagamist eesmärgiga ohvrit kahjustada, hirmutada või alandada. Teenuse keelamise (DoS) ja hajutatud teenuse keelamise (DDoS) rünnakud: DoS-i ja DDoS-i rünnakute eesmärk on ületada veebisait või võrguteenus liikluse tulvaga, muutes selle seaduslikele kasutajatele kättesaamatuks. Need rünnakud võivad häirida võrguteenuseid ja põhjustada ettevõtetele rahalist kahju. Man-in-the-Middle (MitM) rünnakud: MitM-i rünnakud hõlmavad kahe osapoole, näiteks kasutaja ja veebisaidi vahelise suhtluse pealtkuulamist ja pealtkuulamist. Seejärel saab ründaja vahetatud andmeid vaadata või nendega manipuleerida ilma suhtlevate osapoolte teadmata. Nullpäevased ärakasutused: Nullpäeva ekspluatatsioonid sihivad tarkvara turvaauke, mis pole müüjale ega arendajatele veel teada. Küberkurjategijad kasutavad neid turvaauke rünnakute käivitamiseks enne, kui plaaster või parandus on saadaval, muutes nende kaitsmise raskeks. Asjade Interneti (IoT) haavatavused: kuna üha rohkem seadmeid on Internetiga ühendatud, on asjade Interneti haavatavused muutunud probleemiks. IoT-seadmete nõrku turvameetmeid saab ära kasutada koduvõrkudele juurdepääsu saamiseks või privaatsuse ohustamiseks. 2.2. TUNNISTA HOIATUSMÄRGID Hoiatusmärkide äratundmine on oluline Interneti-ohutuse oskus. See tähendab, et Interneti kasutamisel tuleb olla tähelepanelik indikaatorite suhtes, mis näitavad, et midagi on

	valesti või potentsiaalselt ohtlik. Hoiatusmärke ära tundes saavad inimesed kiiresti tegutseda, et kaitsta end võrguohtude eest ja vältida pettuste, küberrünnakute või muu pahatahtliku tegevuse ohvriks langemist. Siin on mõned olulised hoiatusmärgid, millele tähelepanu pöörata: Soovimatu suhtlus: olge ettevaatlik tundmatutest või kahtlastest allikatest pärit soovimatute meilide, sõnumite või sõbrakutsete suhtes. Küberkurjategijad kasutavad neid vahendeid sageli andmepüügikatsete käivitamiseks või pahavara levitamiseks. Halb grammatika ja õigekiri: paljud andmepüügimeilid ja petukirjad sisaldavad grammatilisi vigu, õigekirjavigu või ebamugavat keelekasutust. Need vead võivad olla märk sellest, et side ei pärine seaduslikust allikast. Isikuandmete päringud: olge ettevaatlik tundliku teabe (nt sisselogimismandaadid, finantsandmed või sotsiaalkindlustusnumbrid) taotluste suhtes, eriti kui päring on ootamatu või tundub ebavajalik. Kiireloomuline või ähvardav keel: sõnumid, mis kasutavad kiireloomulist või ähvardavat keelt, et sundida teid kohe tegutsema, võivad viidata kelmuse või andmepüügi katsele. Ebatavalised lingid või URL-id: hõljutage kursorit meilides või sõnumites olevate linkide kohal, et näha, kuhu URL tegelikult läheb. Olge ettevaatlik lühendatud URL-ide või linkidega, mis suunavad ümber kahtlastele veebisaitidele. Sobimatud või võlts-URL-id: jälgige URL-e, mis näivad olevat õigustatud, kuid millel on kirjavigu või peeneid variatsioone. Petturid võivad kasutajate petmiseks kasutada domeeninimesid, mis sarnanevad väga tuntud veebisaitidega. Tundmatud meilisaatjad: kontrollige meili saatjate identiteeti, eriti kui kiri sisaldab ootamatuid manuseid või tundliku teabe taotlusi. Ootamatud allalaadimised: olge ettevaatlik allalaadimiste või manuste suhtes, mida te ei algatanud ega oodanud, kuna need võivad sisaldada pahavara. Ebatavaline kontotegevus: vaadake regulaarselt üle oma online-konto tegevus ja olge valvsa volitamata sisselogimiste või tehingute suhtes.

	Seletamatu süsteemi käitumine: kui teie arvuti või seade käitub ebatavaliselt (nt sagedased kokkujooksmised, aeglustused või ootamatud hüpikaknad), võib see viidata pahavara olemasolule või muudele turvaprobleemidele. Turvatarkvara hoiatused: pöörake tähelepanu oma viirusetõrje- või turvatarkvara hoiatustele, kuna need võivad viidata võimalikele ohtudele või kahtlasele tegevusele. Soovimatud pakkumised ja reklaamid: olge ettevaatlik soovimatute pakkumiste või reklaamide suhtes, mis tunduvad liiga head, et tõsi olla, kuna need võivad olla pettused, mille eesmärk on petta teid isikuandmeid esitama. 2.3. ONLINE OHUTUSTE IGORRAMISE TAGAJÄRGED Internetiohtude eiramisel võivad olla tõsised ja kaugeleulatuvad tagajärjed, mis võivad negatiivselt mõjutada üksikisikuid, ettevõtteid ja isegi ühiskonda tervikuna. Kui võrguohtudega tegeleda või nende vastu asjakohaseid meetmeid ei võeta, võib inimene muutuda haavatavaks erinevate küberriskide ees, mis võib kaasa tuua rahalisi kaotusi, privaatsusrikkumisi, mainet ja isegi õiguslikke tagajärgi. Siin on mõned võrguohtude ignoreerimise peamised tagajärjed. Rahaline kahju: pettuste, andmepüügirünnakute või võrgupettusskeemide ohvriks langemine võib kaasa tuua märkimisväärse rahalise kahju. Küberkurjategijad võivad varastada pangamandaate, krediitkaarditeavet või teha volitamata tehinguid, põhjustades pangakonto kaotust ja finantsraskusi. Identiteedivargus: identiteedivarguse hoiatusmärkide eiramine võib lubada küberkurjategijatel varastada isiklikku teavet, nagu sotsiaalkindlustuse numbrid, sünnikuupäevad ja aadressid. Nad võivad kasutada seda varastatud teavet finantspettuste toimepanemiseks, ohvri nimel kontode avamiseks või muus kuritegelikus tegevuses, millel võivad olla ohvrile tõsised pikaajalised tagajärjed. Andmerikkumised: tugevate turvameetmete rakendamata jätmine või haavatavuste kõrvaldamine võib põhjustada üksikisikute ja organisatsioonide andmetega seotud rikkumisi. Andmerikkumine võib paljastada tundlikku teavet, sealhulgas kliendiandmeid, ärisaladusi või intellektuaalomandit, mille tagajärjeks võivad olla rahalised

	karistused, juriidilised kohustused ja kahju organisatsiooni mainele. Lunavararünnakud: küberturvalisuse tavade eiramine võib jätta üksikisikud ja ettevõtted lunavararünnakute suhtes haavatavaks. Kui lunavara ohustab süsteeme, saab väärtuslikke andmeid krüpteerida ja ründajad nõuavad dekrüpteerimisvõtme eest tasu. Lunaraha maksmine ei garanteeri andmete taastamist ning ohvritel võib tekkida andmete kadu või talitlushäireid. Mainekahju: küberkiusamise või sotsiaalmeedia rünnakute ohvriks langemine võib oluliselt kahjustada üksikisikute ja organisatsioonide mainet. Internetis levitatav valeteave, negatiivsed arvustused või kahjulik sisu võib kahjustada inimese või brändi mainet, mõjutades sotsiaalset positsiooni, töövõimalusi ja klientide usaldust. Privaatsuse kaotamine: privaatsusprobleemide eiramine võib viia privaatse teabe, sealhulgas isiklike vestluste, piltide või videote paljastamiseni. Sellel privaatsuse kaotamisel võivad olla emotsionaalsed ja psühholoogilised tagajärjed, aga ka võimalikud väljapressimisohud. Õiguslikud tagajärjed: Küberohtude mitteteadmisel ja vajalike turvameetmete rakendamata jätmisel võivad olla õiguslikud tagajärjed. Üksikisikute või organisatsioonide suhtes võidakse kohaldada õiguslikke meetmeid, trahve või regulatiivseid sanktsioone andmerikkumiste, privaatsuse rikkumiste või küberjulgeolekustandardite mittejärgimise eest. Teenuse katkemine: Interneti-ohte ignoreerivad ettevõtted võivad oma tegevust häirida. Küberrünnakud, nagu hajutatud teenuse keelamise (DDoS) rünnakud, võivad veebisaite või võrke üle koormata, muutes teenused klientidele kättesaamatuks ning viia tulude ja usaldusväärsuse kaotuseni. Sotsiaalne ja emotsionaalne mõju: küberkiusamise, võrguahistamise või röövelliku käitumise ignoreerimisel võivad olla ohvritele tõsised sotsiaalsed ja emotsionaalsed tagajärjed. See võib põhjustada ärevust, depressiooni, isolatsiooni ja isegi enesevigastamise mõtteid. Riiklikud julgeolekuprobleemid: Interneti-ohtude eiramine võib minna kaugemale üksikisiku või organisatsiooni tasandist ja muutuda riikliku julgeoleku probleemiks. Kriitilise infrastruktuuri või valitsussüsteemide vastu

	suunatud küberrünnakud võivad häirida olulisi teenuseid, ohustada tundlikku teavet ja kahjustada riigi stabiilsust. 3. ISIKUANDMETE KAITSE 3.1. PRIVAATSUSKAITSE TÄHTSUS Privaatsus on tänapäeva digiajastul tehnoloogia ja Interneti laialdase kasutuse tõttu ülimalt tähtis. See hõlmab üksikisiku isikuandmete, andmete ja võrgutegevuste kaitsmist volitamata juurdepääsu, väärkasutuse ja ärakasutamise eest. Privaatsuse kaitse olulisust saab mõista erinevate nurkade alt: Isiklik turvalisus: privaatsuskaitse tagab, et tundlikud isikuandmed, nagu sotsiaalkindlustuse numbrid, finantsandmed või kodused aadressid, jäävad konfidentsiaalseks ja turvaliseks. Sellele teabele volitamata juurdepääsu takistamine aitab ära hoida identiteedivargust, finantspettust ja muid küberkuritegevuse vorme, millel võivad olla üksikisikutele tõsised tagajärjed. Privaatsus ja andmete kontroll: üksikisikutel on õigus kontrollida, kuidas organisatsioonid nende andmeid koguvad, säilitavad ja kasutavad. Privaatsuskaitse tagab, et üksikisikud saavad teha teadliku valiku oma andmete jagamiseks ja anda nõusoleku nende kasutamiseks konkreetsetel eesmärkidel. Usalduse säilitamine: eraelu puutumatuse kaitsmine on üksikisikute ja organisatsioonide vahelise usalduse loomiseks ja säilitamiseks hädavajalik. Kui kasutajad on kindlad, et nende isikuandmeid käsitletakse vastutustundlikult ja turvaliselt, kasutavad nad suurema tõenäosusega veebiteenuseid, teevad tehinguid ja jagavad teavet enesekindlalt. Isikliku vabaduse säilitamine: privaatsuse austamine tähendab isikutele võimaldamist end vabalt väljendada, kartmata jälgimist või diskrimineerimist nende veebitegevuste või eelistuste tõttu. Eraelu puutumatuse kaitse on sõna- ja sõnavabaduse austamise seisukohast hädavajalik. Internetis ahistamise ja jälitamise ennetamine: privaatsuskaitse kaitseb inimesi võrgus ahistamise ja jälitamise eest. Isikuandmetele juurdepääsu piiramisega vähendavad privaatsuse kaitse meetmed sihitud rünnakute või küberkiusamise ohtu.

	Isiklike suhete kaitsmine: privaatsus võimaldab inimestel suhelda ja jagada teavet usalduslike suhete raames, tagades eravestluste ja suhtluse konfidentsiaalsuse. Andmete väärkasutuse vältimine: privaatsuse kaitsmine vähendab ohtu, et isikuandmeid kasutatakse muul eesmärgil kui üksikisik. See hõlmab soovimatute turunduskampaaniate, soovimatute meilide või isikupärastatud sisu vältimist, mis võib tungida isiklikku ruumi. Diskrimineerimise ja profiilide koostamise ennetamine: privaatsuskaitse võib aidata vältida isikute profiilide koostamist ja diskrimineerimist nende isikuandmete või veebikäitumise alusel. Andmete kogumine ilma piisava privaatsuskaitseta võib viia ebaõiglaste ja kallutatud otsuste tegemiseni. Küberturvalisus ja digitaalne usaldus: privaatsus ja küberturvalisus on omavahel seotud. Privaatsuse rikkumine võib põhjustada küberjulgeoleku intsidente ja vastupidi. Privaatsuse esikohale seadmisega saavad üksikisikud ja organisatsioonid edendada digitaalse usalduse ja turvalisuse kultuuri. 3.2. TURVALINE ONLINE KONTO HALDUS Turvaline veebikontohaldus on tavade ja strateegiate kogum üksikisiku veebikontode kaitsmiseks ja haldamiseks viisil, mis minimeerib volitamata juurdepääsu ja andmetega seotud rikkumiste riski. Nõuetekohane veebikonto haldamine on oluline isikuandmete privaatsuse säilitamiseks, identiteedivarguste ärahoidmiseks ja digitaalsete varade kaitsmiseks. Siin on mõned turvalise veebipõhise kontohalduse põhiaspektid ja parimad tavad. Tugevad ja kordumatud paroolid: kasutage iga võrgukonto jaoks tugevaid unikaalseid paroole. Vältige lihtsalt äraarvatavate paroolide (nt "123456" või "parool") kasutamist. Selle asemel looge keerukaid paroole, mis koosnevad suur- ja väiketähtedest, numbritest ja erimärkidest. Paroolihaldurid: kaaluge paroolide turvaliseks genereerimiseks, salvestamiseks ja haldamiseks usaldusväärse paroolihalduri kasutamist. Paroolihaldurid aitavad teil säilitada iga konto jaoks tugevaid ja kordumatuid paroole, ilma et peaksite neid kõiki meeles pidama.

	Lubage kahefaktoriline autentimine (2FA): võimaluse korral lubage oma veebikontode jaoks kahefaktoriline autentimine. Kahefaktoriline autentimine lisab täiendava turvakihi, nõudes lisaks paroolile ka teist kinnitusviisi, näiteks ühekordset koodi, mis saadetakse teie mobiilseadmesse. Jälgige oma kontotegevust: vaadake regulaarselt oma kontotegevust ja olge valvsa volitamata sisselogimiste või kahtlaste toimingute suhtes. Kui märkate ebatavalist tegevust, võtke kohe kasutusele meetmed oma konto kaitsmiseks, nt muutke parooli ja võtke ühendust konto pakkujaga. Vältige avalikke arvuteid ja WiFi-võrke: vältige avalikest arvutitest või turvamata WiFi-võrkudest juurdepääsu tundlikele kontodele, nagu meil või pangakontod. Avalikud arvutid võivad salvestada sisselogimismandaate ja turvamata WiFi-võrgud võivad teie andmeid potentsiaalselt pealt kuulata. Hoiduge andmepüügikatsete eest: olge ettevaatlik soovimatute meilide, sõnumite või linkide suhtes, mis küsivad tundlikku teavet või paluvad teil oma kontodele sisse logida. Enne teabe esitamist kontrollige saatja ja veebisaidi legitiimsust. Konto taasteteabe korrapärane värskendamine: hoidke oma konto taasteteavet (nt alternatiivsed e-posti aadressid või telefoninumbrid) ajakohasena. See aitab teil taastada juurdepääsu oma kontole, kui unustate parooli või kogete muid sisselogimisprobleeme. Privaatsus- ja turvaseadete ülevaatamine: vaadake regulaarselt üle oma võrgukontode privaatsus- ja turvaseaded. Kohandage seadeid vastavalt oma eelistustele ja vajadustele, et tagada hea tasakaal privaatsuse ja funktsionaalsuse vahel. Seadmete väljalogimine ja turvamine: logige alati oma kontodelt välja, kui olete nende kasutamise lõpetanud, eriti jagatud või avalikes seadmetes. Lisaks kaitske oma isiklikke seadmeid tugevate paroolide või biomeetrilise autentimise abil. Muutke oma paroole regulaarselt: kaaluge oma paroolide regulaarset muutmist, eriti kriitiliste kontode (nt meili- ja pangakontode) puhul. Paroolide regulaarne värskendamine lisab täiendava turvakihi.

	Konto taastamise valikute lubamine: seadistage konto taastamise valikud (nt turvaküsimused või varukoodid), et taastada juurdepääs oma kontole, kui see lukustatakse. 3.3. VASTUTUSTULINE SOTSIAALMEEDIA JAGAMINE Vastutustundlik sotsiaalmeedia jagamine viitab teadlikule ja läbimõeldud lähenemisele sisu jagamisele sotsiaalmeedia platvormidel viisil, mis austab privaatsust, soodustab positiivset suhtlust ning väldib valeinformatsiooni või kahju tekitamist. Vastutustundliku sotsiaalmeedia jagamise harjutamine on oluline digitaalse etiketi järgimiseks, positiivse veebikogukonna edendamiseks ning isikliku ja kollektiivse heaolu kaitsmiseks. Siin on mõned vastutustundliku sotsiaalmeedia jagamise põhiaspektid: **Kaitske isikuandmeid:** olge ettevaatlik, kui avaldate sotsiaalmeedias tundlikku isiklikku teavet, näiteks oma koduaadressi, telefoninumbrit või finantsteavet. Isikuandmete kaitsmine aitab kaitsta identiteedivarguse ja muude privaatsusriskide eest. **Privaatsusseadete kohandamine:** vaadake regulaarselt üle ja kohandage oma privaatsusseadeid sotsiaalmeedia platvormidel. Kohandage iga sõnumi vaatajaskonda, et teie sisu näeks ja sellega suhtleks ainult sihtrühm. **Austage nõusolekut:** hankige inimestelt nõusolek enne nende fotode või isikliku teabe jagamist sotsiaalmeedias. Võtke arvesse inimeste eelistusi postitustes märgistamise või sisus mainimise osas. **Kontrollige fakte ja vältige valeinformatsiooni:** enne artiklite, teabe või piltide jagamist kontrollige nende täpsust usaldusväärsetest allikatest. Vältige valeinformatsiooni või kontrollimata sisu levitamist, mis võib kaasa aidata kuulujuttude või valejuttude levikule. **Pöörake tähelepanu ajastusele ja sagedusele:** vältige liigset või sobimatut jagamist, kuna see võib teid jälgivate inimeste jaoks põhjustada teabe üleküllust. Arvestage postituste postitamisel erinevaid ajavööndeid ja publiku eelistusi. **Positiivse sisu reklaamimine:** jagage positiivset, informatiivset või inspireerivat sisu. Positiivne jagamine

	aitab luua tervislikumat veebikeskkonda ja edendab teid jälgivate inimeste seas kogukonnatunnet. **Käsitlege lahkarvamusi lugupidavalt:** osalege sotsiaalmeedias lugupidavates ja konstruktiivsetes aruteludes, isegi kui te ei nõustu teistega. Vältige võrguvestlustes osalemist ega isiklike rünnakute kasutamist. **Vältige kahjulikku või solvavat sisu:** hoiduge jagamast sisu, mis võib olla teistele inimestele solvav, diskrimineeriv või kahjulik. Olge teadlik oma sõnumite võimalikust mõjust erinevatele inimestele ja kogukondadele. **Autoriõiguste kaitse:** austage autoriõiguse seadusi ja vältige autoriõigusega kaitstud materjali jagamist ilma nõuetekohase loata või omistamiseta. Tunnustage algseid loojaid nende tööde jagamisel. **Jagatud sisu ülevaatamine:** vaadake oma jagatud sisu regulaarselt üle, veendumaks, et see on kooskõlas teie väärtuste ja pildiga, mida soovite veebis esitada. Kustutage või värskendage postitusi, mis ei kajasta enam teie praegust väljavaadet. **Edendage digitaalset lahkust:** näidake oma suhtluses sotsiaalmeedias lahkust ja empaatiat. Vältige küberkiusamise, vaenu õhutamise või mis tahes kahjuliku käitumise vormis osalemist või levitamist. **Julgustage positiivset veebikultuuri:** julgustage teisi jagama sotsiaalmeediat vastutustundlikult, näidates positiivset eeskuju. Osalege aruteludes digitaalse kodakondsuse ja vastutustundliku digikodaniku tähtsuse üle. 4. SIRVI SOTSIAALMEEDIAS OHUTULT 4.1. PRIVAATSUSSÄTETE KOHANDAMINE Privaatsusseadete kohandamine viitab isikuandmete juurdepääsutaseme ja nähtavuse kohandamise protsessile erinevatel platvormidel, veebisaitidel ja rakendustes. See tähendab teadliku valiku tegemist selle kohta, milliseid andmeid jagatakse, kellega neid jagatakse ja kuidas kolmandad osapooled neid kasutavad. Privaatsusseadeid kohandades saavad üksikisikud paremini kontrollida oma digitaalset jalajälge ja kaitsta oma isikuandmeid tarbetu kokkupuute eest. Siin on üksikasjalik selgitus privaatsusseadete kohandamise tähtsuse ja sammude kohta.

	Privaatsusseadete kohandamise tähtsus: Isikuandmete kaitse: privaatsusseadete kohandamine võimaldab inimestel piirata teistele nähtava isikliku teabe hulka, vähendades sellega identiteedivarguse, ahistamise või sotsiaalse manipuleerimise rünnakute ohtu. **Andmete jagamise juhtimine:** privaatsusseadeid kohandades saavad üksikisikud juhtida, milliseid andmeid nad sotsiaalmeedia platvormide, veebisaitide ja rakendustega jagavad, piirates oma teabe kogumist ja kasutamist. **Vältige sihitud reklaamimist:** privaatsusseaded võivad aidata inimestel sihitud reklaamidest ja isikupärastatud sisust loobuda, pakkudes privaatsemat ja vähem pealetükkivat veebikogemust. **Vältige andmete väärkasutust:** privaatsusseadete kohandamine vähendab volitamata kolmandate isikute poolt andmete väärkasutuse ohtu, aidates kaitsta võimalike rikkumiste ja volitamata juurdepääsu eest andmetele.tundlik teave. **Parandage võrguturvalisust:** isiklikule teabele juurdepääsu piiramine privaatsusseadete kaudu võib tugevdada võrguturvalisust ja minimeerida sotsiaalse manipuleerimise või andmepüügi rünnakute riski. **Toimingud privaatsusseadete kohandamiseks:** Kontrollige konto seadeid: sotsiaalmeedia platvormidel vaadake konto seadeid või privaatsusseadete jaotist, et pääseda juurde privaatsuseelistuste kohandamise valikutele. **Valige sõnumite vaatajaskond:** määrake, kes teie sõnumeid näevad, näiteks teie sõbrad, sõprade sõbrad või avalikkus. Valige oma sisu nähtavuse piiramiseks väiksem vaatajaskond. **Profiiliteabe haldamine:** otsustage, milline profiiliteave on teistele nähtav (nt teie e-posti aadress, telefoninumber või sünnikuupäev). Võimaluse korral vähendage tundlike andmete nähtavust. **Rakenduse lubade haldamine:** mobiilirakenduste puhul kontrollige ja hallake lubasid seadme seadetes. Lubage iga rakenduse jaoks ainult vajalikud load ja tühistage nende rakenduste load, mis neid ei vaja. **Andmete kogumisest keeldumine:** mõned platvormid ja veebisaidid pakuvad võimalust keelduda andmete

	kogumisest ja jagamisest reklaami eesmärgil. Kasutage neid võimalusi andmete jälgimise vähendamiseks. **Kohandage asukoha jagamist:** valige, millal ja kellega oma asukohta jagate. Lülitage asukoha jagamine välja, kui te seda ei vaja, või piirake seda kindlate usaldusväärsete rakendustega. **Kaaluge anonüümset sirvimist:** kasutage privaatset või inkognito sirvimisrežiimi, et vältida sirvimisajaloo ja küpsiste salvestamist teie seadmesse. **Kontrollige kolmanda osapoole rakenduste juurdepääsu:** vaadake üle ja hallake kolmandate osapoolte rakendusi, millel on juurdepääs teie kontoteabele. Tühistage juurdepääs rakendustele, mida enam ei kasutata või millele ei ole vaja juurde pääseda. **Olge vaikesätetega ettevaatlik:** paljudel platvormidel on privaatsusseaded, mis võivad olla lubavamad, kui soovitakse. Võtke aega, et kohandada neid seadeid vastavalt oma eelistustele. **Vaadake ja värskendage regulaarselt:** vaadake ja värskendage regulaarselt oma privaatsusseadeid, kuna platvormid ja rakendused võivad lisada uusi funktsioone või muudatusi, mis mõjutavad teie privaatsust. 4.2. HALDAGE SÕBRA TAOTLUSID JA SÕNUMID Sõbrakutsete ja sõnumite käsitlemine sotsiaalmeedia platvormidel ja sõnumsiderakendustes hõlmab teistega suhtlemisel ettevaatlikkust, otsustusvõimet ja austust. Oluline on säilitada isiklikke piire, kaitsta oma privaatsust ja edendada positiivset veebikogemust. Siin on mõned näpunäited sõbrakutsete ja sõnumite käsitlemiseks: Sõbrakutse haldamine: **Kinnitage identiteet:** enne sõbrakutse vastuvõtmist veenduge, et tunnete seda inimest või teil on ühiseid sõpru. Olge tundmatute või kahtlaste profiilide päringute vastuvõtmisel ettevaatlik. **Kontrollige privaatsusseadeid:** kohandage oma privaatsusseadeid, et määrata, kes saavad teile sõbrakutseid saata. Piirake sõbrakutsed sõprade sõpradele või kindlatele rühmadele, et vähendada võimalust saada taotlusi võõrastelt.

	Vältige võõraste vastuvõtmist: olge uute ühenduste lisamisel valiv. Vältige sõbrakutsete vastuvõtmist inimestelt, keda te isiklikult ei tunne, eriti kui neil pole vastastikuseid sidemeid. **Kahtlaste kontode blokeerimine või neist teatamine:** kui saate kahtlastelt või võltskontodelt sõbrakutseid, kaaluge nende blokeerimist või platvormi administraatoritele teatamist. **Vaadake üle profiiliteave:** enne sõbrakutse vastuvõtmist vaadake üle taotleja profiil, et veenduda, et see tundub autentne ning vastab teie väärtustele ja huvidele. **Austage piire:** kui te ei tunne end kellegi läheduses mugavalt, võite sõbrakutseid tagasi lükata. Austage oma piire ja ärge arvake, et peate iga taotlusega nõustuma. Sõnumi töötlemine: **Olge lugupidav:** vastake sõnumitele viisakalt ja lugupidavalt. Kohtle teisi veebivestluses nii, nagu soovid, et sinuga koheldaks. **Kontrollige saatjaid:** kui saate sõnumi tundmatult saatjalt, olge ettevaatlik. Vältige kahtlastel linkidel klõpsamist ega manuste allalaadimist tundmatutest allikatest. **Vältige tundliku teabe jagamist:** vältige tundliku isikuandmete, finantsandmete või paroolide jagamist sõnumsiderakenduste kaudu. Olge ettevaatlik, kui jagate privaatset teavet inimestega, keda te hästi ei tunne. **Ahistusest või väärkasutusest teatamine:** kui saate solvavaid, ähvardavaid või ahistavaid sõnumeid, teatage saatjast platvormi administraatoritele või sõnumirakenduse tugimeeskonnale. **Sõnumite privaatsuse määramine:** kohandage oma sõnumite privaatsusseadeid, et määrata, kes saavad teile sõnumeid saata. Piirake juurdepääsu sõnumitele oma sõpradele või kontaktidele. **Blokeeri funktsiooni kasutamine:** kui keegi häirib teid või saadab teile sobimatuid sõnumeid, kasutage funktsiooni Blokeerimine, et vältida edasist kontakti selle inimesega.

	Pöörake tähelepanu toonile ja kavatsusele: sõnumeid võib tooni ja näoilmete puudumise tõttu kergesti valesti tõlgendada. Olge oma suhtluses tähelepanelik ja püüdke vältida arusaamatusi. Tehke sõnumsides pause. Sõnumite saatmises ja sotsiaalmeedias on hea teha pause, et keskenduda muudele tegevustele ja vältida digitaalset ülekoormatust. 4.3. TEATA JA BLOKERI KURITAV KONTOD Kuritarvitavatest kontodest teatamine ja nende blokeerimine on turvalise ja positiivse veebikeskkonna säilitamisel üliloluline samm. Kuritarvitavad kontod võivad osaleda kahjulikus käitumises, nagu küberkiusamine, ahistamine, vihakõne ja muud võrgus kuritarvitamise vormid. Nendest kontodest teatamine ja nende blokeerimine aitab kaitsta ennast ja teisi nende kahjulike tegude eest. Siin on selgitus selle kohta, kuidas aruandlus ja blokeerimine toimivad ning miks need on olulised. Kuritavast kontost teavitamine: Kahjuliku käitumise tuvastamine: kui avastate konto, mis on kuritahtlik või kahjulik (nt ahistamine, ähvardused või vaenu õhutamine), on oluline see ära tunda. **Teata kontost:** enamikul sotsiaalmeedia platvormidel ja võrguteenustel on aruandlusmehhanism. Kasutage platvormi aruandlusfunktsiooni, et teavitada administraatoreid või moderaatoreid kuritahtlikust käitumisest. **Esitage tõendeid:** kuritahtlikust kontost teatamisel võib olla abiks tõendite esitamine, nagu ekraanipildid või lingid solvavale sisule, et teie teadet toetada. **Valige sobiv kategooria:** sotsiaalmeediaplatvormid pakuvad sageli erinevaid aruandluskategooriaid. Valige kategooria, mis vastab kõige paremini selle väärkasutuse tüübile, millest teatate. **Järgige aruandlusjuhiseid:** tutvuge platvormi aruandlusjuhistega, et tagada kontode aruandlus mõjuvatel põhjustel. Vältige valeteateid, kuna need võivad kahjustada aruandlussüsteemi tõhusust. Kuritarvitavate kontode blokeerimine:

	Kaitske ennast: kuritahtliku konto blokeerimine takistab sellel kontol teiega suhtlemist. See võib aidata kaitsta teie vaimset heaolu ja luua teile turvalise veebiruumi. **Soovimatu kontakti vältimine:** kui blokeerite konto, ei saa selle konto taga olev kasutaja teid enam jälgida, teile sõnumeid saata ega teie postitusi kommenteerida. **Anonüümsus:** blokeerimine on üldiselt privaatne toiming. Kasutaja, kelle blokeerite, ei saa teavitust, et ta on blokeeritud. **Ei mingit suhtlemist:** pärast konto blokeerimist ei näe te enam selle sisu ega tegevusi ning nemad ei näe enam teie oma. Miks on teavitamine ja blokeerimine oluline? **Kahju ennetamine:** kuritahtlikest kontodest teavitamine võib võimaldada kõnealuse konto suhtes meetmeid võtta, mis võib ära hoida edasist kahju teile või teistele. **Platvormi juhiste jõustamine:** kuritahtlikust käitumisest teavitamine aitab jõustada platvormi teenusetingimusi ja kogukonna juhiseid, luues turvalisema keskkonna kõigile kasutajatele. **Kogukonna tervise toetamine:** kuritahtlikest kontodest teatades ja blokeerides aitate edendada tervet ja lugupidavat veebikogukonda. **Kasutajate mõjuvõimu suurendamine:** teavitamine ja blokeerimine võimaldavad inimestel oma veebikogemust kontrollida ja kaitsta end kuritahtliku või kahjuliku suhtluse eest. 5. KÜBERTURVASED JA MOBIILSEADMED 5.1. TURVALINE NUTITELEFONID JA TABLETTID Nutitelefonide ja tahvelarvutite turvalisus on tänapäeva mobiilimaailmas hädavajalik, kuna need seadmed salvestavad hulgaliselt isiklikku teavet ja tundlikke andmeid. Nende seadmete turvalisus aitab kaitsta volitamata juurdepääsu, andmetega seotud rikkumiste ja pahavara rünnakute eest. Siin on mõned peamised sammud nutitelefonide ja tahvelarvutite turvalisuse tagamiseks.

	Lukustusekraani turvalisuse lubamine: seadistage turvaline ekraaniluku meetod, nt PIN-kood, muster, parool või biomeetriline meetod (sõrmejälg või näotuvastus). See aitab vältida volitamata juurdepääsu teie seadmele kaotsimineku või varguse korral. **Hoidke tarkvara ajakohasena:** värskendage regulaarselt oma seadme operatsioonisüsteemi ja rakendusi. Tootjad annavad turvaaukude parandamiseks välja värskendusi. Seetõttu on oluline hoida oma seadet ajakohasena, et olla kaitstud võimalike ärakasutamise eest. **Installige ainult usaldusväärsed rakendused:** laadige rakendused alla ametlikest rakenduste poodidest (nt Google Play Store, Apple App Store) ja vältige tundmatutest allikatest pärit rakenduste installimist. Mitteametlikest allikatest pärit pahatahtlikud rakendused võivad kahjustada teie seadme turvalisust ja privaatsust. **Rakenduse lubade ülevaatamine:** olge rakendustele lubade andmisel ettevaatlik. Vaadake üle iga rakenduse taotletud load ja vaadake, kas need on selle tööks vajalikud. Vältige tarbetute lubade andmist, mis võivad teie privaatsust ohustada. **Kasutage avalikes WiFi-võrkudes VPN-i:** avalike WiFi-võrkude kasutamisel kaaluge oma Interneti-liikluse krüptimiseks ja andmete kaitsmiseks võimaliku pealtkuulamise või luuramise eest virtuaalse privaatvõrgu (VPN) kasutamist. **Turvaline mobiilisirvimine:** kasutage turvalisi brausereid, mis pakuvad veebisaitidele krüptitud ühendusi (HTTPS). Vältige juurdepääsu tundlikule teabele, näiteks Interneti-pangale, turvamata või avalike võrkude kaudu. **Varundage oma andmeid regulaarselt:** varundage oma seadme andmeid regulaarselt turvalisse pilveteenusesse või välisseadmesse. Seega on teie oluline teave turvaline isegi siis, kui teie seade on kadunud, kahjustatud või lähtestatud. **Vältige kahtlastel linkidel klõpsamist:** olge ettevaatlik, kui klõpsate tundmatutest allikatest pärit meilides, sõnumites või hüpikakendes olevatel linkidel. Pahatahtlikel linkidel klõpsamine võib viia andmepüügikatseteni või pahavara installimiseni. Rakenduste load ja juurdepääs andmetele viitavad õigustele, mida mobiilirakendused (rakendused) taotlevad, et pääseda

	ligi kasutaja seadme erinevatele funktsioonidele ja andmetele. Kui kasutajad installivad ja kasutavad rakendusi oma nutitelefonidesse või tahvelarvutitesse, võivad need rakendused nõuda õigeks toimimiseks juurdepääsu teatud seadmeressurssidele ja isiklikule teabele. Need load võimaldavad rakendustel pakkuda konkreetseid funktsioone ja parandada kasutajakogemust. Siiski on oluline, et kasutajad mõistaksid ja hallaksid neid õigusi, et kaitsta oma privaatsust ja turvalisust. Siin on rakenduste load ja andmetele juurdepääs lähemalt. **Rakenduste lubade tüübid:** kasutusload sõltuvad rakenduse funktsioonidest ja platvormist (Android või iOS). Levinumad load on juurdepääs kaamerale, mikrofonile, asukohale, kontaktidele, kalendrile, salvestusruumile, SMS-idele, kõnelogidele jne. seadmest. Mõned rakendused võivad taotleda luba ka muude ühendatud seadmete (nt Bluetoothi seadmete) kasutamiseks. **Loataotlused:** kui kasutajad rakenduse installivad, võib see taotleda konkreetseid lube, mida see toimimiseks vajab. Loataotlused esitatakse tavaliselt rakenduse installiprotsessi ajal või siis, kui rakendus proovib esimest korda teatud funktsioonile juurde pääseda. Kasutajad saavad neid õigusi anda või keelata. **Kasutuslubade eesmärk:** kasutusload on vajalikud rakenduse teatud funktsioonide lubamiseks. Näiteks vajab fototöötlusrakendus fotode jäädvustamiseks ja salvestamiseks juurdepääsu seadme kaamerale ja mälule. Navigeerimisrakendus vajab täpsete juhiste andmiseks juurdepääsu asukohale. **Privaatsus:** kuigi load on rakenduste tööks sageli hädavajalikud, peaksid kasutajad olema ettevaatlikud, et nad ei annaks lubasid, arvestamata rakenduse eesmärki ja kaalumata, kas taotletud load on mõistlikud. Ülemääraste lubade andmine võib ohustada privaatsust või lubada rakendustel pääseda juurde tundlikele andmetele ilma õiguspärase vajaduseta. **Rakenduse lubade haldamine:** enamik kaasaegseid operatsioonisüsteeme võimaldavad kasutajatel hallata rakenduse lubasid. Kasutajad saavad vaadata ja muuta rakenduse lubasid seadme seadetes, võimaldades neil igal ajal anda või tühistada konkreetsetele rakendustele konkreetseid õigusi.

Co-funded by the European Union

	Lubage hoolikalt läbi: enne lubade andmist peaksid kasutajad rakenduse taotletud load hoolikalt läbi lugema. Kui rakendus taotleb lubasid, mis ei tundu selle funktsionaalsuse jaoks asjakohased, on see punane lipp ja kasutajad peaksid olema ettevaatlikud või kaaluma muude rakenduste kasutamist. **Rakenduse load ja värskendused:** rakenduse värskendamisel on oluline kontrollida uusi või muudetud lubasid. Mõnikord võivad rakenduse värskendused lisada täiendavaid õigusi ja kasutajad peaksid veenduma, et need vastavad nende eelistustele ja vajadustele. **iOS-i ja Androidi rakenduste loataotlused:** kuigi iOS ja Android käitlevad lubasid erinevalt, pakuvad mõlemad platvormid kasutajatele võimalust hallata õigusi oma vastavates seadetes. iOS-is saavad kasutajad vaadata ja hallata lubasid rakenduse seadetes jaotises „Privaatsus". Androidis saavad kasutajad lube hallata, minnes seadme seadetes jaotisse „Rakendused ja teatised" või „Rakenduste haldur". 5.2. KAITSKE MOBIILSEADMEID VARGUSE JA KAOTUSE EEST Mobiilseadmete kaitsmine varguse ja kaotsimineku eest on oluline isikuandmete kaitsmiseks, identiteedivarguste vältimiseks ja tundlike andmete konfidentsiaalsuse säilitamiseks. Mobiilseadmed, nagu nutitelefonid ja tahvelarvutid, on sageli varaste sihtmärgiks oma kaasaskantavuse ja neis sisalduva väärtusliku teabe tõttu. Turvameetmete rakendamine võib oluliselt vähendada varguse või kaotsiminekuga seotud riske. Siin on mõned olulised sammud mobiilseadmete kaitsmiseks. **Lukustusekraani turvalisuse seadistamine:** lubage turvaline ekraaniluku meetod, nagu PIN-kood, muster, parool või biomeetriline meetod (sõrmejälg või näotuvastus). See aitab vältida volitamata juurdepääsu teie seadmele, kui see satub valedesse kätesse. **Kasutage Leia minu seade teenuseid:** lubage oma seadmes Leia minu seade või Leia minu iPhone. Need teenused võimaldavad teil kaugjuhtimisega seadme asukohta leida, lukustada või kustutada, kui see kaob või varastatakse. **Hoidke tarkvara ja rakendused ajakohasena:** värskendage regulaarselt oma seadme operatsioonisüsteemi ja rakendusi, et tagada uusimad turvapaigad ja

	veaparandused. Tootjad annavad välja värskendusi, et parandada turvaauke ja parandada seadme turvalisust. **Vältige oma seadmete järelevalveta jätmist:** ärge jätke oma mobiilseadet järelevalveta avalikesse kohtadesse, nagu restoranid, ühistransport või spordisaalid. Varguse ohu vähendamiseks hoidke seadet enda peal või turvalises kohas. **Olge rahvarohketes kohtades tähelepanelik:** pöörake tähelepanu oma ümbrusele tiheda liiklusega kohtades, eriti seal, kus taskuvargused ja vargused on kõige tõenäolisemad. Olge ettevaatlik, kui kasutate seadet rahvarohketes kohtades. **Hoidke seadet turvaliselt kodus:** hoidke mobiilseadet turvalises kohas, kui seda ei kasutata, eriti kodus. Vältige selle jätmist letile, avatud akna lähedusse või kergesti ligipääsetavasse kohta. **Rakenduste lukkude kasutamine tundlike rakenduste jaoks:** kaaluge rakenduse lukkude või külalisrežiimi funktsioonide kasutamist, et piirata juurdepääsu seadme tundlikele rakendustele või sisule. See lisab täiendava turvakihi, eriti kui jagate oma seadet teistega. **Seadme andmete krüptimine:** kui teie seade seda võimaldab, lubage krüpteerimine, et kaitsta oma andmeid volitamata juurdepääsu eest, isegi kui keegi teine seadmele füüsiliselt juurde pääseb. **Vältige avalikke laadimisjaamu:** vältige avalike laadimisjaamade või USB-portide kasutamist, kuna need võivad sattuda ohtu ja põhjustada andmete varguse või pahavara installimise ohtu. **Varundage oma andmeid regulaarselt:** varundage oma seadme andmeid regulaarselt turvalisse pilveteenusesse või välisseadmesse. Seega on teie oluline teave turvaline isegi siis, kui teie seade on kadunud, kahjustatud või lähtestatud. **Kasutage privaatsust kaitsvaid ekraanikaitsmeid:** kaaluge ekraanikaitsmete kasutamist, et välistada uudishimulikud silmad teie ekraani avalikes kohtades nägemast. **Seadmete registreerimine ametiasutustes:** registreerige oma mobiilseadmed kohalikes ametiasutustes või asjakohastes andmebaasides. See võib varguse korral taastamise protsessi lihtsamaks muuta.

Sõnastik:	1. Interneti-turvalisus Jõustamisjuhiste järgimine, kaasaegse tehnoloogia mõistmine ja digiseadmete kaitsmine võrgumaailma pahatahtlike elementide eest. 2. Interneti-turvalisus Arvutite, võrkude ja andmete kaitsmiseks küberohtude eest, nagu pahavara, viirused ja volitamata juurdepääs, võetud meetmed ja tavad. 3. Digitaalne privaatsus Õigus kontrollida ja kaitsta isikuandmeid ja andmeid ilma nõusolekuta juurdepääsu, kasutamise või jagamise eest. 4. Küberturvalisus Digiseadmete, võrkude ja infosüsteemide kaitsmine küberohtude, sealhulgas häkkimise, andmerikkumiste ja küberrünnakute eest. 5. Turvalised võrgutavad Juhiste ja käitumisviiside kogum, mida üksikisikud peaksid järgima, et tagada oma võrgutegevuste turvalisus ja kaitsta oma privaatsust. 6. Isikuandmete kaitse Tundlike ja isikuandmete kaitsmine volitamata juurdepääsu või väärkasutuse eest, identiteedivarguste ja pettuste vältimine. 7. Sotsiaalmeedia etikett Sobiv ja lugupidav käitumine, mida inimesed peaksid sotsiaalmeediaplatvorme kasutades omaks võtma. 8. Andmete turvalisus Digitaalsete andmete kaitsmiseks volitamata juurdepääsu, muutmise või hävitamise eest võetud meetmed ja protokollid. 9. Identiteedivarguste ennetamine Meetodid ja tavad isikuandmete kaitsmiseks ja kurjategijate selle kasutamise vältimiseks isikuna esinemiseks. 10. Paroolihaldus Vastutustundlik praktika tugevate unikaalsete paroolide loomisel ja nende turvalisel haldamisel, et kaitsta võrgukontosid. 11. Interneti-ähvardused

	Erinevad Interneti kasutamisel kokku puutuvad riskid ja ohud, nagu andmepüük, pahavara, pettused ja küberkiusamine. 12. Andmepüügiteadlikkus Võimalus ära tunda andmepüügikatseid ja neid vältida, mille puhul ründajad meelitavad inimesi hankima tundlikku teavet, sageli petturlike meilide või veebisaitide kaudu. 13. Privaatsusseaded Veebiplatvormide kohandatavad valikud, mis võimaldavad kasutajatel kontrollida oma isikliku teabe nähtavust ja sisu vaatajaskonda. 14. Väärkasutusest teatamine Protsess, mille käigus teavitatakse platvormi administraatoreid või moderaatoreid kuritahtlikust või kahjulikust käitumisest platvormil, nagu ahistamine või vihakõne. 15. Konto blokeerimine Toiming, mis takistab kuritahtlikul või soovimatul kontol teiega suhtlemist või teie sisu vaatamist sotsiaalmeedia platvormidel. 16. Turvalised veebitehingud Pettuste vältimiseks veebitehingute (nt ostud või finantstehingud) turvaline sooritamine. 17. Digitaalne jalajälg Andmete ja teabe jälg, mis on jäänud üksikisiku võrgutegevusest, sealhulgas sotsiaalmeedia postitustest, otsinguajalugu ja võrgusuhtlusest. 18. Küberkiusamise ennetamine Internetis toimuva ahistamise, hirmutamise või kiusamise peatamiseks ja ennetamiseks võetud meetmed. 19. Kahefaktoriline autentimine (2FA) Täiendav turvakiht, mis nõuab kasutajatelt kontole juurdepääsu saamiseks kahte identifitseerimisvormi (nt parool ja telefoni saadetud kordumatu kood). 20. Ohutu sirvimisharjumused Tavad ja juhised, mille eesmärk on tagada ohutu ja turvaline Internetis sirvimine, vältides riskantseid saite ja sisu.

Bibliograafia:	Interneti-ohutuse nõuanded ja reeglid (kaspersky.com) Veebiohutus (teismelistele) – Nemours KidsHealth Mis on võrguturvalisus? | SWGfL Online ohutusvestlus | LearnEnglish teismelised (britishcouncil.org) Interneti turvalisus – Vikipeedia Veebiohutus – näpunäiteid laste abistamiseks | Internet on oluline Interneti-turvalisus: Interneti-turvalisuse sissejuhatus (gcfglobal.org) indianjournals.com/ijor.aspx?target=ijor:ijie&volume=8&issue=2&article=001 "Interneti turvalisus" ajakirjas: The International Encyclopedia of Online Media Literacy (researchgate.net) Google'ist teabe otsimine – Google Güvenlik Merkezi (safety.google) Veebiturve – e-turvalisuse volinik Kuidas võrgus turvaliselt püsida: Interneti-ohutuse nõuanded ja ressursid (reviews.org)
Ressursid (videod, viitelink)	https://www.youtube.com/watch?v=qZE45J-MIUg&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=aO858HyFbKI&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=HxySrSbSY7o&pp=ygULc2FmZSBvbmxpbmU%3D https://www.youtube.com/watch?v=EyQeUwqCDWg&pp=ygULc2FmZSBvbmxpbmU%3D