Pedagoogika sissejuhatus vanematele

POSITIVE DIGITAL PARENTING

Co-funded by
the European Union

Project Number: 2023-2-LT01-KA210-ADU-000173746

Sissejuhatus

ÜRO lapse õiguste konventsioonis määratletakse positiivne vanemlus kui laste huve ja õigusi austav vanemlik käitumine. Interneti, uute digitaalsete tehnoloogiate ja sotsiaalmeedia tulekuga perekondadesse üle kogu maailma ei ole vanemate põhiroll ja lastekasvatuse eesmärgid muutunud: vanemad peavad endiselt oma lapsi kasvatama, kaitsma, ülal pidama, armastama, nendega suhtlema ja neid juhendama. On ka tõsi, et nii minevikus kui ka tänapäeval on vanemluspraktikad kõige tõhusamad, kui need põhinevad positiivsetel vanemluse väärtustel ja põhimõtetel, mis soodustavad avatud suhtlemist ja usaldust. Neid mudeleid ja väärtusi tuleb laiendada ka veebimaailmale, et ületada lõhe traditsiooniliste väärtuste ja veebimaailma vahel, samal ajal hallates ka veebimaailmaga seotud riske lastele. Digitaalne keskkond pakub lastele tohutuid eeliseid, avades uusi võimalusi hariduse, loovuse ja sotsiaalse suhtluse jaoks. Samas võib see kaasa tuua ka tõsiseid riske, nagu küberkiusamine, privaatsuse ohustamine, teiste tegevuste hülgamine, liikumatus ja veebisõltuvus.

Co-funded by
the European Union

Sissejuhatus

Erasmus+ projekti POSITIVE DIGITAL PARENTING eesmärk on anda vanematele meediapädevuse alased teadmised ja vahendid, et arendada lastes kriitilise mõtlemise oskusi digitaalmeediaga suhtlemisel: veebisisu analüüsimine, eelarvamuste äratundmine, valeinfo tuvastamine ja teadlike otsuste tegemine digikeskkonnas. Kriitilise mõtlemise ja meediapädevuse ühendamisega saavad vanemad oma lapsi paremini ette valmistada digitaalmaailmas vastutustundlikult ja mõistlikult liikuma. See koolitusprogramm pakub sissejuhatavat koolitust vanematele, kes on perekonnas peamised vastutajad ja kasvatajad. Selle lähenemisviisi eesmärk on harida vanemaid veebipõhise õppe ja dünaamiliste veebivahendite kasutamisega seotud teemadel, et nad saaksid integreeruda oma laste digitaalsesse ellu ja toetada oma vanemaid ja vanemaid inimesi perekonnas interneti ohtude ja lõksude kohta õppimisel. See õppematerjal edendab veebiturvalisust ja käsitleb perekonna eri põlvkondade vahelist digitaalset lõhet.

Co-funded by
the European Union

PARTNERID

IVAIGO

- Projektide arendamine sotsiaalteaduste uurimistöö kaudu, keskendudes tänapäeva ühiskonna peamistele probleemidele: sotsiaalne kaasatus, keskkonnaprobleemid, kõik diskrimineerimise vormid, digitaalne transformatsioon, füüsilise ja vaimse tervise teenused, naiste mõjuvõimu suurendamine, töötus, ettevõtlus jne.
- Teadmiste omandamine ning loovuse, kujutlusvõime ja kriitilise mõtlemise arendamine kõikide kunstivormide ja spordi kaudu
- Osalejate professionaalsete ja isiklike oskuste jätkusuutlik arendamine mitmekultuurilises kontekstis.
- Noorte, eriti vähemuste ja sotsiaalsete rühmade huvide esindamine.
- Noorte formaalse ja informaalse hariduse edendamine kohalike tegevuste ja rahvusvaheliste projektide kaudu. IVAIGO loob kaasava keskkonna, mis soodustab võrdsust ja võrdõiguslikkust.

Co-funded by
the European Union

POSITIVE DIGITAL PARENTING

PARTNERID

Incirliova Genclik Kultur Sanat ve Gelisim Dernegi

IOVA noorte kultuuri-, kunsti- ja arenguühing – IOVA on mittetulundusühing, millel on üle saja liikme, kes jagavad loomingulisi kodanikke, väärtusi, ideid, mõtteid, refleksioone ja visioone. IOVA on noor ja dünaamiline organisatsioon, mis loodi vastuseks vajadusele luua elav, kogukonnapõhine struktuur, mis suudab ära tunda võimalusi ja reageerida väljakutsetele, mis on seotud kohaliku kogukonna ja selle liikmete unikaalse iseloomuga. IOVA keskendub järgmistele valdkondadele: kodanikuaktiivsuse ja aktiivse osalemise edendamine laialdase hariduse kaudu;

- uute sotsiaalsete rakenduste kasutuselevõtt sellistes valdkondades nagu meediaohutus, valeuudised, sotsiaalmeedia vägivald, meediatehnoloogiate lähenemine jne;
- IKT-strateegiate väärtus digitaalse lõhe ületamise vahendina ja võimsa vahendina majandusliku ja sotsiaalse arengu edendamiseks kogu ELis;
- Digitaalse hariduse pakkumine noorsootöötajatele, täiskasvanuhariduse õpetajatele ja õpetajatele.

Co-funded by the European Union

PARTNERID

EESTI PEOPLE TO PEOPLE

Eesti People to People on 1997. aastal Eestis registreeritud mittetulundusühing, mis tegutseb alates 1993. aastast People to People Internationali vabaühenduse osana. People to People eesmärk on edendada rahvusvahelist mõistmist ja sõprust haridus-, kultuuri- ja humanitaartegevuse kaudu, mis hõlmab erinevate riikide ja kultuuride esindajate vahelist otsest ideede ja kogemuste vahetust. Eesti PTP on pühendunud kultuuridevahelise suhtluse arendamisele nii ühiskonnasiseselt kui ka ühiskondade ja rahvaste vahel. Selle peamised teemad on sallivus ja vastastikune mõistmine.

Co-funded by the European Union

Interneti kasutamine on muutunud tänapäeva pereelus sügavalt juurdunud, kus lapsed ja noored aktiivselt osalevad veebitegevustes ning vanemad inimesed liiguvad digikeskkonnas aeglasemalt. Kuna vanemad võtavad digikeskkonnas üha enam toetavat rolli, on äärmiselt oluline, et nad jääksid valvsaks interneti kasutamisega seotud riskide suhtes.

Kuigi internet pakub palju eeliseid, sealhulgas juurdepääsu teabele ja suhtlusplatvormidele, seab see kasutajad ka mitmesuguste ohtude ette, nagu sobimatu sisu, turvalisuse rikkumised, valeinfo ja küberkiusamine. Vanemad peaksid oma pereliikmeid proaktiivselt kaitsma, austades samal ajal nende privaatsust.

Vanematel on oluline võtta vastu väljakutse võimaldada lastel, noortel ja eakatel inimestel interneti eeliseid ohutult kasutada, selle asemel et suhtuda digitaaltehnoloogiasse negatiivselt. Käesoleva juhendi eesmärk on anda neile oskused ja teadmised veebiriskide ja -ohtude tuvastamiseks ja leevendamiseks.

Seetõttu on kõigi pereliikmete, sealhulgas laste, noorte, noorte täiskasvanute, vanemate ja eakate jaoks oluline põhjalik veebiturvalisuse alane haridus. Vanemad, kes on perekonna nurgakivi, on ainulaadses positsioonis, et pakkuda toetust, abi ja juhendamist kõige haavatavamatele pereliikmetele.

POSITIVE DIGITAL PARENTING Erasmus+ projekti A2 juhend ohutuks internetikasutuseks on mõeldud vanematele, et teavitada neid interneti ohtudest ja julgustada neid võtma ennetavat ja teadlikku lähenemisviisi, et maksimeerida internetikasutuse eeliseid ja tagada samal ajal oma perekonna turvalisus.

Co-funded by the European Union

İNTERNETİ TURVALİSUSE TÄHTSUS

Interneti- või veebiturvalisus on digitaalmaailmas vastutustundliku liikumise oluline aspekt. See hõlmab mitmesuguseid tavasid ja käitumismudeleid, mille eesmärk on kaitsta ennast ja teisi veebiohtude ja -ohu eest. See hõlmab isikuandmete kaitsmist, turvaliste suhtluskanalite tagamist ja positiivse digitaalse kodakondsuse edendamist.

Tänapäeva ühendatud maailmas, kus nutitelefonid, tahvelarvutid ja arvutid on igal pool, on veebis turvalisuse tagamine olulisem kui kunagi varem. Inimesed peaksid olema teadlikud veebitegevusega seotud riskidest, nagu küberkiusamine, pettused ja sobimatu sisu vaatamine. Olles informeeritud ja rakendades turvalisi tavasid, saavad inimesed neid riske vähendada ja nautida turvalisemat veebikogemust.

Laste turvalisuse tagamine internetis on vanematele ja hooldajatele äärmiselt oluline. See hõlmab laste tegevuste jälgimist internetis, vanusele vastavate piirangute kehtestamist ja laste harimist turvalise käitumise osas internetis. Lisaks sellele aitab avatud suhtlemise soodustamine internetikogemuste teemal lastel tunda end mugavamalt, kui nad arutavad muresid või probleeme, millega nad võivad internetikeskkonnas kokku puutuda.

Lõppkokkuvõttes on veebiturvalisuse eesmärk võimaldada inimestel teha teadlikke otsuseid ja liikuda digitaalses maailmas turvaliselt. Olles valvsad ja järgides head küberhügieeni, saame kõik aidata kaasa turvalisema ja ohutuma veebikeskkonna loomisele kõigile.

Co-funded by the European Union

DİGİTAALNE JALAJÄLG

Digitaalse jalajälje mõiste on sarnane internetis surfates jäetud „elektrooniliste leivapuru" jälgedega. Need jäljed koosnevad erinevatest tegevustest ja suhtlustest, näiteks külastatud veebisaitidest, üleslaaditud fotodest ja suhtlusest sotsiaalvõrgustikes. Nagu jalajäljed rannas, võib ka teie digitaalne jalajälg paljastada palju teie ja teie veebitegevuste kohta.

Erinevalt rannas jätvatest jälgedest, mis aja jooksul võivad kaduda, võib teie digitaalne jälg jääda püsima määramata ajaks. See tähendab, et kõik, mida te veebis teete või postitate, võib jääda püsima, isegi kui te selle hiljem kustutate. See püsivus rõhutab, kui oluline on olla teadlik sellest, mida te veebis jagate, ja teie digitaalsete tegevuste võimalikest tagajärgedest.

Teie digitaalses jalajäljes sisalduvat teavet saab kasutada teie kohta üksikasjaliku profiili loomiseks, sealhulgas teie huvide, harjumuste ja käitumise kohta. On äärmiselt oluline kaaluda, kes saab sellele teabele juurde pääseda, ja mõista, et isegi range privaatsusseadete korral on alati olemas võimalus, et sisu võidakse kopeerida ja jagada teie sihtrühmast väljaspool.

Digitaalse jalajälje haldamine tähendab põhimõtteliselt seda, et olete teadlik oma veebis jätvatest jälgedest ja võtate meetmeid, et need kajastaksid täpselt teie kavatsusi ja väärtusi. See hõlmab tähelepanu pööramist jagatavale sisule, privaatsusseadete mõistmist ja teadlikkust oma veebitegevuse võimalikest pikaajalistest tagajärgedest.

Co-funded by the European Union

DİGİTAALNE JALAJÄLG

Digitaalse jalajälje haldamine on tänapäeva digitaalajastul, kus veebitegevus võib avaldada pikaajalist mõju nii isiklikule kui ka tööelule, äärmiselt oluline. Siin on mõned näpunäited, mis aitavad teil oma digitaalset jalajälge tõhusalt hallata:

1. Olge teadlik sellest, mida jagate: mõelge enne postitamist. Kaaluge oma isikliku teabe, fotode või arvamuste jagamise võimalikke tagajärgi veebis. Pidage meeles, et kui midagi on avaldatud, võib seda olla raske täielikult eemaldada.

2. Kasutage privaatsusseadeid: tutvuge sotsiaalmeedia platvormide ja muude veebiteenuste privaatsusseadetega. Reguleerige neid seadeid, et kontrollida, kes saab teie postitusi ja teavet näha.

3. Vaadake regulaarselt üle oma veebipresents: vaadake perioodiliselt üle oma sotsiaalmeedia profiilid ja veebikontod. Eemaldage või uuendage aegunud või ebaoluline teave.

4. Piirangud isiklikule teabele: vältige tundliku isikliku teabe jagamist veebis, näiteks oma aadressi, telefoninumbrit või finantsteavet.

5. Kasutage tugevaid paroole: kasutage oma veebikontode jaoks tugevaid, unikaalseid paroole, et vältida volitamata juurdepääsu. Kaaluge paroolihalduri kasutamist, et oma paroole turvaliselt jälgida.

6. Olge tähelepanelik, millele klõpsate: olge ettevaatlik pettuste ja pahatahtlike linkide suhtes. Vältige tundmatutest või kahtlastest allikatest pärit linkide klõpsamist või manuste allalaadimist.

7. Jälgige oma veebipresentsi: kasutage otsingumootoreid, et regulaarselt kontrollida, milline teave teie kohta on veebis kättesaadav. Kui leiate ebaõiget või kahjulikku teavet, võtke meetmeid selle parandamiseks.

8. Harige ennast ja teisi: õppige parimaid tavasid veebiturvalisuse ja privaatsuse tagamiseks. Harige oma sõpru ja pereliikmeid digitaalse jalajälje haldamise tähtsuse osas.

Järgides neid nõuandeid, saate tõhusalt hallata oma digitaalset jalajälge ja kaitsta oma veebireputatsiooni. Pidage meeles, et teie veebipresents on teie peegelpilt, seega on oluline kontrollida, mida te jagate ja kuidas te end veebis esitate.

Co-funded by the European Union

POSITIVE DIGITAL PARENTING

VEEBİPÕHİNE PRİVAATSUS

Veebiprivatsus, tuntud ka kui internetiprivatsus või digitaalne privaatsus, viitab sellele, mil määral jääb isiku isiklik, finants- ja veebikasutuse teave privaatseks, kui ta on veebis. Seoses veebikeskkonnas jagatavate ja salvestatavate isikuandmete mahu suurenemisega on mure veebiprivatsuse pärast märkimisväärselt kasvanud.

Veebiprivatsuse kaitsmine on oluline mitmel põhjusel. Esiteks on isikutel õigus hoida oma isikliku elu üksikasjad privaatsena ja mitte jagada neid võõrastega. Lisaks, kuna ettevõtte kogutud andmeid võidakse jagada teistega teie teadmata või nõusolekuta, võib olla raske teada, millist isiklikku teavet kogutakse ja kes seda teeb.

Veebiprivatsust tuleks käsitleda sama tähtsana kui privaatsust reaalses maailmas. Nii nagu te peate privaatseid vestlusi suletud uste taga või jagate oma finantsteavet ainult pangaga, peaksite võtma meetmeid oma veebiprivatsuse kaitsmiseks. See hõlmab tugevate ja unikaalsete paroolide kasutamist, ettevaatlikkust veebis jagatava teabe suhtes ning sotsiaalmeedia ja muude veebiplatvormide privaatsusseadete regulaarse läbivaatamise.

Hinnates ja kaitstes oma veebiprivatsust, saate vähendada oma isikliku teabe väärkasutamise või teie nõusolekuta jagamise riski.

Co-funded by the European Union

ANDMETE KONFIDENTSIAALSUS

Andmete privaatsus on põhiõigus, mis on pälvinud märkimisväärset tähelepanu, eriti seoses Euroopa Liidus üldise andmekaitse määruse (GDPR) rakendamisega. 2018. aastal kehtestatud GDPR on loodud kaitseks iga ELi kodaniku privaatsust ja andmeid, kehtestades ranged eeskirjad isikuandmete kogumise, töötlemise ja säilitamise kohta.

GDPR koosneb 99 artiklist, mis võtavad kokku andmekaitse erinevad aspektid. Mõned olulisemad sätted on järgmised:

1. Juurdepääsuõigus: isikutel on õigus teada, milliseid andmeid ettevõte nende kohta hoiab ja kuidas neid kasutatakse.

2. Õigus andmete kustutamisele: see õigus, mida tuntakse ka kui „õigus olla unustatud", võimaldab isikutel teatavatel tingimustel taotleda oma isikuandmete kustutamist.

3. Nõusolek: ettevõtted peavad enne isikuandmete kogumist või töötlemist saama isikult selgesõnalise nõusoleku. See hõlmab selget ja selgesõnalist nõusolekut küpsiste ja sirvimisajaloo kohta.

4. Andmete minimeerimine: ettevõtted peaksid koguma ja töötlema ainult neid andmeid, mis on vajalikud andmete kogumise eesmärgi saavutamiseks.

5. Andmete ülekantavus: isikutel on õigus saada oma isikuandmeid ettevõttelt üldkasutatavas ja masinloetavas vormingus.

6. Andmekaitseametnikud: mõned organisatsioonid on kohustatud nimetama andmekaitseametniku, kes jälgib GDPR-i nõuete täitmist.

GDPR on oluliselt mõjutanud seda, kuidas ettevõtted isikuandmeid käitlevad, nõudes neilt rangemate andmekaitse meetmete rakendamist ja suuremat läbipaistvust oma andmetöötluspraktikate osas. GDPR on olnud tõhus andmekaitseõiguste edendamisel ja tagades üksikisikutele suurema kontrolli oma isikuandmete üle.

Co-funded by the European Union

POSITIVE DIGITAL PARENTING

VEEBİOHUD

Küberohtud on pahatahtlikud tegevused, mille eesmärk on kahjustada andmeid, varastada teavet või häirida digitaalseid toiminguid. Need ohud hõlmavad laia valikut tegevusi, sealhulgas küberrünnakuid, mis on suunatud infotehnoloogia varadele, arvutivõrkudele, intellektuaalomandile ja tundlikele andmetele. Küberohtud võivad pärineda nii sisemistest kui ka välistest

Sisemised ohud võivad pärineda usaldusväärsetelt kasutajatelt, kes kuritarvitavad oma õigusi või juurdepääsu tundlikule teabele organisatsiooni sees. Välised ohud pärinevad aga kaugemalt ja neid teostavad tavaliselt tundmatud isikud, kes soovivad ära kasutada digitaalsüsteemide turvaaukude nõrkusi.

Küberohtude näited on pahavara, lunavara, phishing-rünnakud ja teenuse keelamise (DoS) rünnakud. Nendel ohtudel võivad olla tõsised tagajärjed, nagu rahalised kahjud, andmete rikkumised ja organisatsiooni maine kahjustamine.

Küberohtude eest kaitsmiseks peavad organisatsioonid ja üksikisikud rakendama tugevaid küberturvalisuse meetmeid. Need meetmed hõlmavad tarkvara regulaarne uuendamine, tugevate paroolide kasutamine, tundlike andmete krüpteerimine ja kasutajate harimine potentsiaalsete ohtude ja nende vältimise kohta. Lisaks võib mitmefaktorilise autentimise rakendamine ja andmete regulaarne varundamine aidata leevendada küberrünnaku mõju.

Co-funded by the European Union

POSITIVE DIGITAL PARENTING

ONLINE-OHUD

Interneti ohud on kõik, mis võib internetikasutajale kahju tekitada. See kahju võib olla mitmesugune (nt füüsiline, emotsionaalne, psühholoogiline, rahaline, sotsiaalne ja maine kahju). Allpool on kokku võetud mitmesugused interneti ohud:

Interneti ohtude liigid:
Tänapäeval pakub internet juurdepääsu peaaegu kõigele, alates meelelahutusest, krediidi- ja finantsteenustest kuni toodeteni kõikjalt maailmast. Kuigi internet pakub teatud määral anonüümsust, suureneb oht, et kasutaja isikuandmed võivad sattuda ohtu.

1-Küberkiusamine: Küberkiusamine on kiusamise liik, mis toimub digitaalsete tehnoloogiate, nagu sotsiaalmeedia, sõnumivahetusplatvormid, mänguplatvormid ja mobiiltelefonid, abil. See hõlmab korduvat käitumist, mille eesmärk on hirmutada, vihastada või häbistada sihtmärgiks olevat isikut. Küberkiusamise näited on valede või kuulujuttude levitamine kellegi kohta sotsiaalmeedias, haavavate sõnumite või ähvarduste saatmine sõnumirakenduste kaudu ja kellegi identiteedi võltsimine pahatahtlike sõnumite saatmiseks.

Üks olulisemaid erinevusi näost-näkku kiusamise ja küberkiusamise vahel on see, et küberkiusamine jätab digitaalse jälje. See tähendab, et kiusamisest jääb jälg, mis võib olla kasulik tõendite kogumiseks, et kiusamine lõpetada. Inimestel on oluline olla teadlik oma digitaalsest jäljest ja mõista, et nende tegevusel internetis võivad olla reaalsed tagajärjed.

Küberkiusamise vastu võitlemiseks on oluline, et inimesed teavitaksid kõigist küberkiusamise juhtumitest asjaomasele platvormile või asutusele. Samuti on oluline harida noori vastutustundliku veebikäitumise ja küberkiusamise mõjude osas. Koostööd tehes saame luua kõigile turvalisema veebikeskkonna.

Co-funded by the European Union

ONLINE-OHUD

2- Küberkurjategijad: Küberkurjategija on tavaliselt täiskasvanud isik, kes kasutab internetti laste ja noorte ärakasutamiseks mitmesuguste kuritarvituste eesmärgil, sealhulgas seksuaalse, emotsionaalse, psühholoogilise või rahalise kahju tekitamiseks. Need kurjategijad otsivad haavatavaid isikuid erinevate veebipõhiste platvormide kaudu, nagu jututoad, kiirsõnumid, sotsiaalvõrgustikud ja videomängud.

Üks küberkurjategijate levinud taktika on luua vale identiteet, esitledes end lapsena või noorena. Nad kasutavad seda vale identiteeti, et luua suhe oma ohvritega, võita järk-järgult nende usaldus ja suunata neid kahjulikele tegevustele.

Grooming on küberkurjategijate kasutatav oluline strateegia, mille puhul nad manipuleerivad oma ohvreid aja jooksul aeglaselt ja kasutavad sageli ära nende nõrkusi ja ebakindlust. See protsess võib hõlmata näiliselt ehtsa sõpruse või suhte loomist ohvriga, enne kui teda oma kasuks ära kasutatakse.

Vanematel, hooldajatel ja õpetajatel on äärmiselt oluline õpetada lastele ja noortele internetiturvalisust ja küberkurjategijate poolt tekitatavaid ohte. Avatud suhtlemise soodustamine veebis ja piiride seadmine aitab kaitsta noori selliste kurjategijate ohvriks langemise eest. Lisaks aitab veebitegevuse jälgimine ja hoiatusmärkide teadmine tuvastada ja ennetada võimalikke kuritarvitusi.

3. Isikuandmete jagamine: Isikuandmete jagamise vältimine on oluline andmete kaitsmiseks, identiteedivarguse ennetamiseks ja turvalisuse tagamiseks internetis. See on oluline mitte ainult internetis surfates, vaid ka sotsiaalmeedia platvormidel teavet kasutades ja jagades.

Co-funded by the European Union

ONLINE-OHUD

Isikuandmete näited, mida tuleb kaitsta, on järgmised:
1. Nimed: täisnimi, perekonnanimi ja vanemate nimed.
2. Isikukoodid: riiklik kindlustusnumber, juhiloa number, passi number, patsiendi identifitseerimisnumber, maksukood, krediidikonto number või finantskontode numbrid.
3. Aadressid: tänava aadress ja e-posti aadress.
4. Biomeetrilised andmed: võrkkesta skaneeringud, sõrmejäljed, näo geomeetria või hääle allkirjad.
5. Sõiduki identifitseerimis- või registreerimisnumbrid.
6. Telefoninumbrid.
7. Tehnoloogiliste varade andmed: konkreetse isikuga seotud meediajuurdepääsu kontrolli (MAC) või internetiprotokolli (IP) aadressid.

Sotsiaalmeediat kasutades on oluline olla tähelepanelik jagatava teabe suhtes. Vältige oma täisnime, aadressi või telefoninumbri avalikku jagamist. Kasutage privaatsusseadeid, et kontrollida, kes saab teie postitusi ja teavet näha, ning olge ettevaatlik sõprade lisamise taotluste või sõnumite vastuvõtmisel inimestelt, keda te ei tunne. Olles ettevaatlik oma isikuandmete kaitsmisel, saate vähendada identiteedivarguse ja muude veebiohtude riski.

4- Phishing: Phishing-rünnakud on küberkurjategijate poolt kasutatavad petlikud taktikaid, mille abil meelitatakse inimesi avaldama tundlikku teavet, nagu krediitkaardi numbrid või sisselogimise andmed. Need rünnakud hõlmavad tavaliselt võltsitud suhtlust, näiteks e-kirju või sõnumeid, mis näivad pärinevat õiguspärastest allikatest. Phishing-rünnakute eesmärk on varastada isiklikku teavet või installida ohvri seadmesse pahavara.

Phishing-rünnakud võivad olla erinevad, sealhulgas e-kirjad, mis näivad pärinevat teie pangast või populaarse veebiteenuse pakkujalt. Need e-kirjad sisaldavad sageli linke, mis klõpsates suunavad edasi võltsitud veebisaitidele, mis jäljendavad õigete saitide välimust. Pärast võltsitud veebisaidile sisenemist palutakse ohvritel sisestada oma isiklikud andmed, mis seejärel küberkurjategijate poolt salvestatakse.

Co-funded by the European Union

ONLINE-OHUD

5-Pettuste ohvriks langemine: Internetipettused on küberkurjategijate poolt veebis läbi viidavad pettused. Need pettused võivad olla erinevad ja nende eesmärk on meelitada inimesi avaldama tundlikku teavet või raha. Interneti-pettused võivad toimuda mitmesuguste kanalite kaudu, näiteks phishing-kirjade, sotsiaalmeedia, SMS-sõnumite, võltsitud tehnilise toe telefonikõnede ja hirmutarkvara kaudu.
Interneti-pettuste peamine eesmärk on tavaliselt varastada isiklikku teavet, näiteks krediitkaardi andmeid või sisselogimise andmeid, või meelitada inimesi saatma raha petturitele. Mõned levinumad internetipettuste liigid on:

1. Pettusemeilid: meilid, mis näivad olevat pärit legitiimsetelt organisatsioonidelt, nagu pangad või valitsusasutused, kuid tegelikult püüavad meelitada inimesi andma isiklikku teavet või klõpsama pahatahtlikele linkidele.

2. Sotsiaalmeedia pettused: pettused, mis toimuvad sotsiaalmeedia platvormidel, näiteks võltsprofiilid või reklaamid, mis suunavad kasutajaid pettuslikele veebisaitidele või pahatahtliku tarkvara allalaadimise leht

3. SMS-pettused: pettuslikud sõnumid, mis saadetakse tekstisõnumina ja sisaldavad tavaliselt linke võltsitud veebisaitidele või isikuandmete küsimist.

4. Võltsitud tehnilise toe kõned: petturid, kes esinevad tehnilise toe esindajatena ja üritavad veenda inimesi, et nende arvutis on probleem, ning nõuavad seejärel makset või juurdepääsu arvutile, et probleem „lahendada”.

5. Hirmutarkvara: võltsitud tarkvara või hüpikaknad, mis väidavad, et arvuti on nakatunud viirusega, ja kutsuvad kasutajat üles ostma mittevajalikku tarkvara või teenuseid.

Interneti-pettuste eest kaitsmiseks on oluline olla ettevaatlik, kui saate soovimatuid sõnumeid või isikuandmete küsimisi. Enne mis tahes teabe edastamist või linkide klõpsamist kontrollige saatja või organisatsiooni õiguspärasust. Kasutage ka ajakohastatud turvatarkvara, mis aitab pettusi avastada ja ennetada.

Co-funded by the European Union

ONLINE-OHUD

6-Pahavara juhuslik allalaadimine: Pahavara juhuslik allalaadimine on levinud arvutiturbeoht, millel võivad olla tõsised tagajärjed. Pahavara, lühend sõnast malicious software, hõlmab viiruseid, usse, trooja hobuseid ja muid kahjulikke programme, mis on loodud teie arvutisüsteemi kahjustamiseks või häirimiseks.

Arvutiviirus on pahavara liik, mis suudab ennast paljundada ja levida teistesse arvutitesse. See võib sageli muuta teie arvuti tööd teie teadmata ja loata ning põhjustada mitmesuguseid probleeme, alates väikestest ebamugavustest kuni tõsiste kahjustusteni.

Et vältida pahavara juhuslikku allalaadimist, on oluline olla ettevaatlik tarkvara internetist allalaadimisel. Hinnake hoolikalt tasuta tarkvara ja vältige allalaadimist peer-to-peer failijagamise saitidelt, kuna need on levinud pahavara allikad. Olge ka ettevaatlik tundmatutelt saatjatelt saadud e-kirjade suhtes, kuna need võivad sisaldada pahatahtlikke manuseid või linke.

Enamikul tänapäevastel veebibrauseritel on sisseehitatud turvasätted, mis aitavad kaitsta veebiohtude eest. Oluline on hoida need sätted ajakohasena ja lubada täiendavaid turvaelemente, nagu hüpikakende blokeerijad ja pettustevastased tööriistad.

Kuid kõige tõhusam viis viiruste ja muu pahavara eest kaitsmiseks on kasutada usaldusväärse pakkuja ajakohastatud viirusetõrjetarkvara. Viirusetõrjetarkvara aitab tuvastada ja eemaldada pahavara teie arvutist ning pakub reaalajas kaitset uute ohtude eest. Viirusetõrjeprogrammi regulaarne uuendamine ja arvuti skaneerimine aitab hoida teie süsteemi pahavara nakkuste eest kaitstuna.

Co-funded by the European Union

POSITIVE DIGITAL PARENTING

OLULISED OSKUSED TURVALISEKS INTERNETIKASUTAMISEKS

Interneti-ohutus on üldmõiste, mida kasutatakse laste, noorte ja perekonna haavatavamate liikmete ohutuse edendamiseks internetiga ühendatud seadmete kasutamisel. Internetimaailm võib rikastada laste ja noorte elu mitmel moel, nii isiklikult kui ka haridusalaselt.
On oluline kokku võtta põhilised oskused, mis on õpilastel vaja veebikeskkonnas turvalisuse tagamiseks:

a**. Riskide tunnistamine:** veebitegevuse riskide tuvastamine on internetis turvalisuse tagamiseks ülioluline. Potentsiaalsete ohtude ja riskide tuvastamise abil saavad inimesed võtta ennetavaid meetmeid, et vähendada oma veebis viibimist ja kaitsta end kahju eest.

Alustuseks on oluline võtta kasutusele ennetav lähenemisviis veebiturvalisusele. See tähendab potentsiaalsete riskide teadvustamist ja meetmete võtmist nende leevendamiseks enne, kui need muutuvad probleemiks. Olles teadlikud levinud veebiohtudest, nagu phishing-pettused, pahavara ja identiteedivargus, saavad inimesed end paremini nende ohtude eest kaitsta.

Veebis ohutuse tagamise teine oluline aspekt on veebis avatuse vähendamine. See võib hõlmata sotsiaalmeedias ja muudel veebisaitidel jagatava isikuandmete hulga piiramist, privaatsusseadete kasutamist, et kontrollida, kes saab teie andmeid näha, ning ettevaatlikkust tundmatutest allikatest pärit linkide klõpsamisel või manuste allalaadimisel.

Digitaalmaailmas turvalisuse tagamiseks on oluline tunnistada veebitegevustega seotud riske ja võtta ennetavaid meetmeid nende vähendamiseks. Teadlikkus ja ennetav tegutsemine aitavad inimestel end veebiohtude eest kaitsta ja veebis turvaliselt liikuda.

b. Isikuandmete turvalisuse tagamine:
Isikuandmete turvalisuse tagamine on oluline ohutu veebikeskkonna säilitamiseks. Oluline on järgida teatud juhiseid, et kaitsta oma identiteeti ja tagada turvaline digitaalne elu endale ja oma perele:

1. Kasutage tugevaid ja unikaalseid paroole: Paroolid on teie digitaalse kodu võtmed. On oluline kasutada tugevaid, unikaalseid paroole kõigi oma kontode jaoks ja vältida kergesti äraarvatavaid paroole. Kaaluge usaldusväärse paroolihalduri kasutamist, et luua ja salvestada turvaliselt keerukaid paroole.

Co-funded by the European Union

2. Vältige paroolide jagamist: ärge jagage oma paroole kunagi kellegagi, isegi mitte usaldusväärsete isikutega. Paroolide jagamine võib ohustada teie kontode ja isikliku teabe turvalisust.

3. Tehke oma andmetest varukoopia: tehke oma olulistest andmetest regulaarselt varukoopiaid, et kaitsta neid kadumise või varguse eest. Selleks võite kasutada väliseid kõvakettaid, pilve salvestusteenuseid või muid varunduslahendusi. Varundatud andmed tuleks krüpteerida ja turvaliselt säilitada.

4. Hoidke oma tarkvara ajakohasena: veenduge, et kõik teie seadmetes olev tarkvara, sealhulgas operatsioonisüsteemid, brauserid ja rakendused, uuendatakse regulaarselt viimaste turvaparanduste ja uuendustega. See aitab kaitsta turvaaukude eest, mida küberkurjategijad võivad ära kasutada.

5. Kasutage turvatarkvara: installige oma seadmetesse usaldusväärne viirusetõrje- ja pahavaravastane tarkvara ning uuendage seda regulaarselt, et kaitsta end viiruste, pahavara ja muude veebiohtude eest.

6. Lülitage sisse kaheastmeline autentimine (2FA): võimaluse korral lülitage oma kontodel sisse 2FA, et lisada täiendav turvatase. See nõuab lisaks paroolile teist tüüpi kinnitust, näiteks teie telefonile saadetud koodi.

Järgides neid juhiseid, saate aidata kaitsta oma isiklikke andmeid ja tagada endale ja oma perele turvalisema veebikogemuse.

c. Ärge laadige alla tundmatuid faile: tundmatute failide allalaadimine võib seada teie arvuti ja isiklikud andmed mitmesugustesse ohtudesse, sealhulgas pahavara, viiruste ja muu pahatahtliku tarkvara ohtu. On oluline järgida neid juhiseid, et kaitsta ennast ja oma seadmeid:

1. Olge ettevaatlik e-kirjade manustega: ärge laadige alla manuseid tundmatutest või kahtlastest e-kirjadest. Need manused võivad sisaldada pahavara, mis võib kahjustada teie arvutit või varastada teie isiklikke andmeid.

Co-funded by the European Union

2. Kontrollige allikat: enne faili allalaadimist kontrollige allikat, et veenduda selle õiguspärasuses. Laadige faile alla ainult usaldusväärsetelt veebisaitidelt ja allikatest.

3. Kasutage usaldusväärset viirusetõrjetarkvara: installige oma arvutisse viirusetõrjetarkvara ja uuendage seda regulaarselt. See tarkvara aitab tuvastada ja eemaldada allalaaditud failidest pahavara.

4. Lubage faililaiendid: lubage oma operatsioonisüsteemis faililaiendid, et näha faili täisnime. See aitab teil tuvastada potentsiaalselt kahjulikke faile.

5. Vältige peer-to-peer (P2P) failide jagamist: olge ettevaatlik P2P failide jagamise teenuste kasutamisel, kuna need võivad teid pahavarale ja muudele ohtudele avada. Laadige faile alla ainult usaldusväärsetest allikatest.

6. Skaneerige faile enne nende avamist: kasutage viirusetõrjetarkvara, et skaneerida alla laaditud faile enne nende avamist. See aitab tuvastada failis oleva pahavara või viirused.

Järgides neid juhiseid, saate vähendada tundmatute failide allalaadimise riski ja kaitsta oma arvutit ja isiklikke andmeid veebiohtude eest.

d. Kasutage kriitilist mõtlemist, et analüüsida ja hinnata veebis leiduvat teavet.
Kriitilise mõtlemise oskuste kasutamine veebis leiduva teabe analüüsimiseks ja hindamiseks on äärmiselt oluline, et kaitsta end pettuste, andmepüügi katsete ja valeinfo eest. Siin on mõned juhised, mis aitavad teil turvalisust tagada:

1. Olge skeptiline: kahtlege veebis leitud teabe allika ja kehtivuse suhtes. Kui midagi tundub liiga hea, et olla tõsi, või ei tundu päris õige, on parem enne tegutsemist rohkem uurida.

2. Kontrollige õigekirja vigu ja kahtlasi e-posti aadresse: olge ettevaatlikud e-kirjade, sõnumite või veebisaitidega, mis sisaldavad õigekirja vigu või kasutavad ebaseaduslikke e-posti aadresse. Need võivad olla pettuse- või andmepüügi katsete tunnused.

Co-funded by the European Union

e. Veenduge, et külastatav veebisait on turvaline:
Veebisaidi turvalisuse kontrollimine on äärmiselt oluline, eriti kui sisestate tundlikku teavet, näiteks makseandmeid, et kaitsta end veebiohtude eest. Siin on mõned sammud veebisaidi turvalisuse kontrollimiseks:

1. Kontrollige URL-i: vaadake veebisaidi URL-i ja veenduge, et see algab „https://" asemel „http://". Täht „s" tähistab turvalisust ja näitab, et veebisaidil on SSL-sertifikaat, mis krüpteerib teie brauseri ja veebisaidi vahel edastatavaid andmeid.

2. Otsige tabaluku ikooni: kontrollige URL-i kõrval asuvat aadressiriba tabaluku ikooni olemasolu. See näitab, et veebisait on turvaline ja kasutab HTTPS-krüpteeringut.

3. Kontrollige veebisaidi õiguspärasust: enne isikliku või makseandmete sisestamist kontrollige veebisaidi õiguspärasust. Otsige kontaktandmeid, nagu füüsiline aadress ja telefoninumber, ning kontrollige teiste kasutajate kommentaare või hinnanguid.

4. Kasutage turvalist makseviisi: kui teete oste veebis, kasutage turvalist makseviisi, mis pakub ostja kaitset, näiteks PayPal või krediitkaart. Vältige deebetkaartide või pangaülekannete kasutamist, kuna need pakuvad vähem kaitset pettuste vastu.

5. Kasutage kõrge turvalisusega brauserit: kaaluge sellise brauseri kasutamist, mis pakub täiendavaid turvaelemente, nagu sisseehitatud pettuste ja pahavara kaitse. Mõned brauserid kuvavad ka rohelist aadressiriba või muid indikaatoreid, mis näitavad, et veebisait on turvaline.

6. Hoidke oma brauser ja turvatarkvara ajakohasena: hoidke oma brauser ja turvatarkvara ajakohasena, et kaitsta end uusimate ohtude ja turvaaukude eest.
Järgides neid juhiseid, saate aidata tagada, et veebisaidid, mida külastate, on turvalised, ja kaitsta end veebiohtude eest, kui teete oste või sirvite internetti.

f. Ole teadlik oma digitaalsest jalajäljest.
Kui oled kord võrgus, oled alati võrgus: kõik, mis võrgus avaldatakse, on kõigile nähtav, seega on oluline olla tähelepanelik isikuandmete kasutamisel sotsiaalmeedia profiilides ja veebisaitidel, mida külastatakse, kus registreeritakse või mis sisaldavad mis tahes tüüpi kasutaja isikuandmeid.

Co-funded by the European Union

ENNETAVAD MEETMED JA JUHISED VEEBITURVALISUSE TAGAMISEKS

Turvalisema lähenemisviisi kasutuselevõtt on oluline, et tagada turvalisus võrgus, kuna see aitab inimestel tunnistada potentsiaalseid riske ja võtta ennetavaid meetmeid enda kaitsmiseks. Siin on mõned olulised punktid, mida tuleks meeles pidada:

1. Olge ettevaatlikud vale turvatunde suhtes: isegi kui arvutid tunduvad turvalised, võivad nad olla haavatavad mitmesuguste võrguriskide suhtes. Oluline on meeles pidada, et küberkurjategijad võivad põhjustada reaalset kahju identiteedivarguse, rahalise kahju ja seadmete kahjustamise kaudu.

2. Püsige kursis: hoidke end kursis viimaste veebiohtude ja parimate turvapraktikatega. See aitab teil tunnistada potentsiaalseid riske ja võtta asjakohaseid meetmeid enda kaitsmiseks.

3. Järgige turvalisuse ettevaatusabinõusid: rakendage eespool kirjeldatud turvameetmeid, nagu tugevate ja unikaalsete paroolide kasutamine, tarkvara ajakohastamine ning kahtlaste linkide ja manuste vältimine.

4. Kasutage tervet mõistust: kasutage veebis suheldes tervet mõistust. Kui midagi tundub liiga hea, et olla tõsi, või ei tundu õige, on parem olla ettevaatlik ja sellest eemale hoida.

5. Olge proaktiivne: võtke proaktiivseid meetmeid, et end veebis kaitsta, näiteks varundage regulaarselt oma andmeid, kasutage turvatarkvara ja olge ettevaatlik veebis jagatava teabe suhtes.

6. Olge valvsad: Olge valvsad ja teadlikud oma veebikeskkonnast. Olge ettevaatlikud soovimatute e-kirjade, sõnumite või isikuandmete küsimiste suhtes ning kontrollige allikat enne mis tahes tegevuse alustamist.

Co-funded by the European Union

POSITIVE DIGITAL PARENTING

PROAKTIIVSED MEETMED JA JUHISED VEEBITURVALISUSE TAGAMISEKS

Võttes kasutusele turvalisema mõtteviisi ja järgides neid juhiseid, saate end kaitsta veebiohtude eest ja nautida turvalisemat veebikogemust.

-Looge tugevamad paroolid.
Tugev parool on üks parimaid viise oma kontode ja isikliku teabe kaitsmiseks häkkerite eest.

-Brauseri turvaomadused
Arvutid puutuvad veebis surfates kokku mitmesuguste ohtudega, sealhulgas viiruste, pahavara ja nuhkvaraga. Hea uudis on see, et teie veebibrauseril on palju sisseehitatud turvaomadusi, mis aitavad teie arvutit kaitsta.

-Spämmi ja phishing-tarkvara ennetamine
Et kaitsta end e-posti pettuste, pahavara ja identiteedivarguse eest, peate mõistma, kuidas tuvastada potentsiaalselt ohtlikku sisu ja kuidas seda vältida.

-Vältige pahavara viirusetõrje abil.
Pahavara on üks levinumaid ohte teie arvutile, kui olete võrgus, kuid seda on lihtne vältida. Teie arvuti turvalisuse tagamine ja õppimine, kuidas tuvastada ja vältida kahtlasi linke, on põhielemendid.

-Turvaline veebipood
Veebipood on mugav viis ostude tegemiseks oma kodust lahkumata. Kuigi sellel on palju eeliseid, on sellega seotud ka mõned riskid. On olemas viise, kuidas kaitsta oma finantsteavet ja tagada selle turvalisus, näiteks veebisaidi turvalisuse ja autentsuse kontrollimine.,

Co-funded by the European Union

ERİNEVATE VANEMLİKU KONTROLLİ LİİKİDE JAOTUS

Lapsevanemate kontroll pakub mitmesuguseid funktsioone, mis aitavad vanematel hallata oma laste veebitegevust. Siin on ülevaade erinevatest lapsevanemate kontrolli tüüpidest:

1. Filtreerimine ja blokeerimine: need funktsioonid piiravad juurdepääsu teatud veebisaitidele, sõnadele või piltidele, mida vanemad peavad sobimatuks. Need aitavad vältida laste juurdepääsu kahjulikule veebisisule.

2. Saadetud sisu blokeerimine: see funktsioon aitab kaitsta laste privaatsust ja turvalisust, takistades neil jagamast oma isiklikku teavet veebis ja e-posti teel.

3. Ajalised piirangud: vanemad saavad määrata ajalised piirangud, kui kaua lapsed võivad veebis viibida ja millistel kellaaegadel nad internetile juurde pääsevad. See aitab hallata ekraaniaega ja tagada, et lapsed ei viibi veebis sobimatutel aegadel.

4. Jälgimistööriistad: need tööriistad teavitavad vanemaid laste veebitegevusest, ilma juurdepääsu blokeerimata. Need võivad salvestada, milliseid veebisaite laps külastab, ja kuvada hoiatussõnumeid, kui laps külastab teatud saite. See võimaldab vanematel olla kursis laste veebikäitumisega.

Kuigi vanemlik kontroll aitab lapsi internetis kaitsta, on oluline meeles pidada, et see ei asenda haridust, vastutustunnet ja täiskasvanute järelevalvet. Vanemad peaksid õpetama oma lastele interneti võimalikke ohte ja kehtestama reeglid sobivate ja sobimatute veebisaitide kohta. Avatud ja ausad vestlused lastega on võtmeteguriks turvalise veebikeskkonna loomisel, kus nad tunnevad end mugavalt, arutades muresid või probleeme, millega nad võivad veebis kokku puutuda.

Co-funded by the European Union

POSITIVE DIGITAL PARENTING

VANEMLİKU JÄRELEVALVE PÕHİREEGLİD

Vanemlik järelevalve on laste turvalisuse tagamiseks internetis äärmiselt oluline. Siin on mõned põhireeglid tõhusa vanemliku kontrolli tagamiseks:

1. Veetke aega koos internetis: õpetage lastele sobivat käitumist internetis, veetes nendega aega internetis. See võimaldab teil jälgida nende tegevust ja arutada võimalikke riske.

2. Hoidke arvuti ühises ruumis: paigutage arvuti kodu ühisesse ruumi, näiteks elutuppa, kus saate selle kasutamist hõlpsasti jälgida. Vältige arvutite paigutamist eraldi magamistubadesse ja jälgige nutitelefonide või tahvelarvutite kasutamise aega.

3. Lisage laste lemmiksaitidele järjehoidjad: laste lemmiksaitidele järjehoidjate lisamine hõlbustab neile internetis turvalist surfamist ja vähendab sobimatu sisu avamise riski.

4. Kontrollige finantskontosid: kontrollige regulaarselt finantskontosid, kaardiväljavõtteid ja telefoniarveid, et avastada ebatavalisi kulutusi, mis võivad viidata volitamata veebioste.

5. Tutvuge veebiturvalisuse meetmetega: uurige, millised veebiturvalisuse meetmed on kasutusel teie lapse koolis, pärast kooli tegevuskeskuses, sõprade kodudes või muudes kohtades, kus lapsed võivad arvutit kasutada ilma järelevalveta.

6. Võtke teateid tõsiselt: kui teie laps teatab häirivast veebikogemusest või juhtumist, võtke seda tõsiselt ja uurige asja kohe. Julgustage avatud suhtlemist, et teie laps tunneks end mugavalt, kui ta oma muredest räägib.

Co-funded by the European Union

POSITIVE DIGITAL PARENTING

NÕUANDED VANEMLIKU JÄRELEVALVE KOHTA

Will Gardner, Suurbritannia turvalisema interneti keskuse direktor, pakub kasulikku teavet vanematele ja hooldajatele, kes soovivad hallata oma laste ja perekonna suhet internetiga. Juurdepääsu aadress: https://inews.co.uk/news/technology/tips-and-guidance-for-children-and-parents-for-staying-safe-online-254485

- Küsige oma pereliikmetelt (eriti lastelt), kuidas internet neid mõjutab
„Rääkige oma lapsega regulaarselt sellest, kuidas ta tehnoloogiat kasutab, ja uurige tema digitaalset elu, sealhulgas tema lemmiksaitide ja -teenustega seotud asju ning seda, kuidas interneti kasutamine teda mõjutab. Lapse kuulamine annab teile parima võimaliku ülevaate sellest, kuidas teda toetada."

- Laste ülekoormamine piirangutega ei ole abiks
„Vanematena on loomulik muretseda oma lapse internetikasutuse riskide pärast, kuid internetimaailm on noortele põnev ja lõbus, sest pakub neile palju võimalusi.
Pidage meeles, et teie laps kasutab tehnoloogiat ja internetti erineval viisil, sest ta kasvab üles maailmas, kus kõik on digitaalne. Püüdke vaadata nii internetikasutamise positiivseid kui ka negatiivseid aspekte ja andke oma lapsele võimalus teha ohutuid valikuid, selle asemel et teda piirangutega üle koormata."

- Tutvuge nende kasutatavate rakenduste ja teenustega.
„Võite oma last veebis toetada, kasutades selliseid funktsioone nagu sotsiaalmeedia privaatsusseaded ja mõistes, kuidas teatada erinevatest rakendustest, mängudest ja teenustest."

- Kasutage abiks olemasolevaid vahendeid.
„Teie perekonna kasutatavate seadmete haldamiseks on saadaval mitmed vahendid. Näiteks vanemliku kontrolli aktiveerimise ja kasutamise oskus aitab vältida, et teie laps näeks internetis sobimatut sisu."

Co-funded by the European Union

INTERNETİ TURVALİSUSE KONTROLLNİMEKİRİ

Norton Security Centre'i sõnul aitab turvaline käitumine internetis vältida teie ja teie pere kokkupuudet soovimatu teabe, materjalide või ohtudega, mis võivad kahjustada teie seadmeid, isiklikku teavet või perekonda. Oleks mõistlik õpetada lastele arvutiturvalisust, eelkõige selleks, et vältida nende langemist varem mainitud levinud ohtude ohvriks.

Siin on Norton Security Centre'i soovitustel põhinev internetiturvalisuse kontrollnimekiri:

1. Kasutage tugevaid, unikaalseid paroole: veenduge, et kõikidel kontodel on tugevad, unikaalsed paroolid, et kaitsta neid volitamata juurdepääsu eest.

2. Hoidke tarkvara ajakohasena: uuendage regulaarselt operatsioonisüsteeme, brausereid ja turvatarkvara, et kaitsta end turvaaukude eest.

3. Kasutage turvatarkvara: installige usaldusväärne viirusetõrje- ja pahavaravastane tarkvara, et kaitsta end viiruste ja muude ohtude eest.

4. Olge ettevaatlikud pettustega: olge ettevaatlikud e-kirjade, sõnumite või veebisaitidega, mis küsivad isiklikku teavet või sisaldavad kahtlaseid linke.

5. Lülitage sisse kaheastmeline autentimine: lülitage sisse kaheastmeline autentimine kontodel, mis seda pakuvad, et tagada täiendav turvatase.

6. Kasutage turvalisi võrke: vältige tundlike tegevuste jaoks avaliku Wi-Fi kasutamist ja kasutage vajaduse korral virtuaalset eravõrku (VPN).

7. Jälgige laste tegevust internetis: jälgige laste tegevust internetis ja õpetage neile turvalisi internetikasutuse tavasid.

8. Tehke olulistest andmetest varukoopiaid: tehke regulaarselt olulistest andmetest varukoopiaid, et kaitsta neid pahavara või riistvararikke tõttu andmete kaotuse eest.

9. Piirake isikuandmete jagamist: olge ettevaatlik isikuandmete jagamisel veebis ja tehke seda ainult turvalistel, usaldusväärsetel veebisaitidel.

10. Harige ennast ja oma peret: hoidke end kursis viimaste veebiohtudega ja õpetage oma perele turvalisi internetikasutuse tavasid.

Co-funded by the European Union

POSITIVE DIGITAL PARENTING

Kirjandus

Interneti turvalisuse näpunäited ja kontrollnimekiri, mis aitavad peredel internetis turvalisemalt käituda. Norton Security Centre. Juurdepääsu aadress: https://us.norton.com/internetsecurity-kids-safety-stop-stressing-10-internet-safety-rules-to-help-keep-your-family-safe-online.html

Kuidas kaitsta oma privaatsust internetis? Norton Security Centre (2021) https://us.norton.com/internetsecurity-privacy-protecting-your-privacy-online.html

Interneti turvalisus: rämpsposti ja andmepüügi vältimine. GCFGlobal (2021) Juurdepääsulink: https://edu.gcfglobal.org/en/internetsafety/avoiding-spam-and-phishing/1/

Lapsevanemate kontroll. Internetiteemad (2021) https://www.internetmatters.org/parental-controls/

5 küberturvalisuse nõuannet, mida iga lapsevanem peaks teadma. Norton Security Centre. Juurdepääsu aadress: https://us.norton.com/internetsecurity-kids-safety-5-cybersafety-tips-every-parent-should-know.html

Mis on veebiohud? Kaspersky (2021) Juurdepääsu aadress: https://thebossmagazine.com/internet-safety-tips/

Mis on digitaalne jalajälg? netsafe (2021) https://www.netsafe.org.nz/digital-footprint/

Mis on veebiturvalisus? National Online Safety (2021) Juurdepääsu aadress: https://nationalonlinesafety.com/wakeupwednesday/what-is-online-safety

Isikuandmete jagamise ohtlikkus sotsiaalmeedias.

Patel, D., mai 2020, PennToday. Juurdepääsu aadress: https://penntoday.upenn.edu/news/dangers-sharing-personal-information-social-media

STEGNER, Ben. (2017) Täielik juhend vanemliku kontrolli kohta. MUO: Tehnoloogia selgitus. Juurdepääsu aadress: https://www.makeuseof.com/tag/guide-parental-controls/

Turvalisus internetis: juhised vanematele ja noortele

https://inews.co.uk/news/technology/tips-and-guidance-for-children-and-parents-for-staying-safe-online-254485

Kuidas kaitsta oma isiklikke andmeid internetis? Norton Security Centre UK https://uk.norton.com/internetsecurity-how-to-8-ways-to-protect-your-private-information-online.html

Rahastatud Euroopa Liidu poolt. Käesolev töö kajastab ainult autori arvamust ning riiklik agentuur ja Euroopa Komisjon ei vastuta selles sisalduva teabe eest.

Co-funded by the Erasmus+ Programme of the European Union