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

POSITIIVNE DIGITAALNE KASVATAMINE

POSITIVE DIGITAL PARENTING

Co-funded by the European Union

SISSEJUHATUS LAPSEVANEMATELE PEDAGOOGIKASSE

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the National Agency. Neither the European Union nor National Agency can be held responsible for them.

Co-funded by the European Union

SİSSEJUHATUS ✳

UNCRC määratleb positiivse vanemluse kui ; vanemlik käitumine, mis austab laste huve ja nende õigusi. Interneti, uute digitehnoloogiate ja sotsiaalmeedia kasutuselevõtuga peredele üle kogu maailma jäävad vanemate põhiroll ja lapsevanemaks kasvamise eesmärgid muutumatuks: vanemad peavad endiselt hoolitsema, kaitsma, hoolitsema, armastama, ühendama. oma lastega ja neid juhendada. Samuti kehtib see, et vanemlikud tavad minevikus ja tänapäeval on kõige tõhusamad, kui need põhinevad positiivse vanemluse väärtustel ja põhimõtetel, mis soodustavad avatud suhtlemist ja usaldust. Neid mudeleid ja väärtusi tuleb laiendada veebimaailma, et luua seos traditsiooniliste väärtuste ja veebimaailma vahel, aga ka ohjeldada sellega seotud riske lastele. Digikeskkond pakub lastele tohutult kasu, avades uusi kanaleid hariduse, loovuse ja sotsiaalse suhtluse jaoks. Kuid see võib kujutada endast ka tõsiseid riske, sealhulgas küberkiusamine, privaatsusriskid, muude tegevuste eiramine, istuv käitumine, võrgusõltuvus jne.

Co-funded by
the European Union

SİSSEJUHATUS ✳

POSITIIVNE DIGITAALNE KASUTAMINE Erasmus+ projekti eesmärk on anda vanematele meediapädevuse teadmised ja tööriistad, et arendada oma lastes kriitilise mõtlemise oskusi digimeediaga suhtlemisel: veebisisu analüüsimisel, eelarvamuste äratundmisel, valeinformatsiooni tuvastamisel ja teadlike otsuste tegemisel digitaalses keskkonnas. Kombineerides kriitilist mõtlemist meediapädevusega, saavad vanemad oma lapsi paremini ette valmistada vastutustundlikult ja tähelepanelikult digimaailmas navigeerimiseks. See õppeprogramm pakub sissejuhatavat koolitust vanematele, kuna nemad on peres peamised hooldajad ja koolitajad. Selle lähenemisviisi eesmärk on õpetada vanemaid mõistma veebipõhise õppimise ja dünaamiliste veebitööriistade kasutamisega seotud probleeme, et nad saaksid integreeruda oma laste digitaalse eluga ning toetada oma vanemaid ja eakaid pereliikmeid ohtude ja lõkse tundmaõppimisel. Internetist. See õppematerjal julgustab veebiturvalisust ja tegeleb perekonna eri põlvkondade vahel valitseva digitaalse lõhega.

Co-funded by the European Union

PARTNERID

ASOCİACİJA IVAIGO

- Projektide arendamine läbi sotsiaaluuringute, keskendudes peamistele probleemidele, millega ühiskond praegu silmitsi seisab: sotsiaalne kaasatus, keskkonnaprobleemid, igasugune diskrimineerimine, digitaalne transformatsioon, füüsiline ja vaimne tervishoid, naiste mõjuvõimu suurendamine, töötus, ettevõtlus jne.
- Teadmiste omandamine ning loovuse, kujutlusvõime ja kriitilise mõtlemise edendamine kõigi kunsti- ja spordialade kaudu.
- Osalejate professionaalsete ja isiklike oskuste jätkusuutlik parandamine mitmekultuurilises kontekstis.
- Noorte, eriti vähemuste ja sotsiaalsete rühmade huvide esindamine.
- Formaal- ja mitteformaalse hariduse edendamine noorte seas läbi kohalike tegevuste ja rahvusvaheliste projektide. IVAIGO loob kaasavaid keskkondi, mis soodustavad võrdsust ja võrdsust.

Co-funded by the European Union

PARTNERID

INCİRLİOVA GENCLİK KULTUR SANAT VE GELİSİM DERNEGİ

- İ.ova Gençlik Kültür , Sanat ve Gelişim Derneği -IOVA on mittetulunduslik organisatsioon, mille liikmeteks on enam kui sada (100) inimest, loovad kodanikud, inimesed, kes jagavad väärtusi, ideid, mõtteid, mõtteid ja nägemust. IOVA on noor ja dünaamiline organisatsioon, mis loodi vastuseks vajadusele elujõulise kogukonnapõhise formatsiooni järele, mis suudaks ära tunda võimalusi ja vastata väljakutsetele, mis on seotud kohaliku kogukonna ja selle liikmete ainulaadse iseloomuga. IOVA fookus on:
- Soodustada kodanikuosalust ja aktiivset kaasamist mitteformaalse hariduse kaudu;
- Uute sotsiaalsete tavade rakendamine meediaohutuse, võltsuudiste, sotsiaalvõrgustiku vägivalla, meediatehnoloogiate lähenemise jms valdkonnas;
- IKT strateegiate väärtus digitaalse lõhe kaotamise vahendina ning majandusliku ja sotsiaalse arengu võimsa vahendina kogu ELis;
- Digihariduse pakkumine noorsootöötajatele, täiskasvanute koolitajatele. ja õpetajad

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 MTÜ People to People rahvusvahelise MTÜ peatükina. Inimesed inimesele eesmärk on edendada rahvusvahelist mõistmist ja sõprust läbi haridus-, kultuuri- ja humanitaartegevuse, mis hõlmab ideede ja kogemuste vahetamist otse eri maade ja erinevate kultuuride rahvaste vahel. Eesti PTP on pühendunud kultuuridevahelise suhtluse edendamisele iga kogukonna sees ning kogukondade ja rahvuste vahel. Keskseks teemaks on sallivus ja vastastikune mõistmine.

Co-funded by the European Union

SISU

Co-funded by the European Union

Interneti kasutamine on tänapäevases pereelus sügavalt juurdunud – lapsed ja noored täiskasvanud võtavad aktiivselt omaks veebitegevusi ning pensionärid liiguvad järk-järgult digitaalsel maastikul. Kuna vanemad võtavad üha enam digitaalse abistaja rolli, on ülioluline, et nad oleksid teadlikud Interneti kasutamisega kaasnevatest riskidest.

Kuigi Internet pakub hulgaliselt eeliseid, sealhulgas juurdepääsu teabe- ja suhtlusplatvormidele, seab see kasutajad ka mitmesuguste ohtude eest, nagu sobimatu sisu, turvarikkumised, desinformatsioon ja küberkiusamine. Vanemad peavad ennetavalt kaitsma oma pereliikmeid, austades samas nende privaatsust.

On oluline, et vanemad ei võtaks digitehnoloogia suhtes heidutavat hoiakut, vaid võtaksid omaks väljakutse tagada, et lapsed, noored ja pensionärid saaksid turvaliselt Interneti hüvesid nautida. See hõlmab neile oskuste ja teadmiste andmist riskide ja ohtude tuvastamiseks ja maandamiseks võrgus.

Seetõttu on igakülgne veebiohutusalane koolitus hädavajalik kõigile pereliikmetele, sealhulgas lastele, teismelistele, noortele täiskasvanutele, vanematele ja pensionäridele. Perekonna tugipunktina on vanematel ainulaadne positsioon, et pakkuda kõige haavatavamatele liikmetele tuge, abi ja juhiseid.

Projekti POSITIIVNE DIGITAALNE KASUTAMINE Erasmus+ projekti A2 juhiste ohutuks veebikasutamiseks eesmärk on tutvustada vanemaid veebis esinevate ohtudega, võimaldades neil kasutada ennetavat ja teadlikku lähenemisviisi, et maksimeerida Interneti kasutamisest saadavat kasu, tagades samal ajal oma pereüksuse turvalisuse.

Co-funded by the European Union

INTERNETİS TURVALİSE OLEMİSE TÄHTSUS

Interneti-turvalisus või Interneti-ohutus on vastutustundliku navigeerimise oluline aspekt. See digimaailmas hõlmab mitmesuguseid tavasid ja käitumisviise, mille eesmärk on kaitsta ennast ja teisi võrguohtude ja -ohtude eest. See hõlmab isikuandmete kaitsmist, turvaliste suhtluskanalite tagamist ja positiivse digitaalse kodakondsuse edendamist.

Tänapäeva omavahel ühendatud maailmas, kus nutitelefonid, tahvelarvutid ja arvutid on kõikjal, on võrgus turvalisus olulisem kui kunagi varem. Üksikisikud peavad olema teadlikud võrgutegevusega seotud riskidest, nagu küberkiusamine, andmepüügipettused ja kokkupuude sobimatu sisuga. Olles kursis ja rakendades ohutuid tavasid, saavad inimesed neid riske maandada ja nautida turvalisemat veebikogemust.

Vanemate ja hooldajate jaoks on laste turvalisuse tagamine veebis ülimalt tähtis. See hõlmab nende veebitegevuste jälgimist, eakohaste piirangute seadmist ja turvalise veebikäitumise õpetamist. Lisaks võib veebikogemuste osas avatud suhtlemise edendamine aidata lastel end mugavalt tunda, kui nad saavad veebis kokku puutuda murede või probleemide üle.

Lõppkokkuvõttes seisneb veebiohutus inimeste volitamises teha teadlikke otsuseid ja navigeerida digitaalses maailmas enesekindlalt. Olles valvsad ja järgides head küberhügieeni, saame kõik kaasa aidata turvalisema ja turvalisema veebikeskkonna loomisele kõigi jaoks.

Co-funded by
the European Union

DIGITAALNE JALAJÄLG

Digitaalse jalajälje kontseptsioon sarnaneb Internetis navigeerimisel „elektroonilise leivapuru" jälje jätmisega. See rada koosneb erinevatest tegevustest ja suhtlustest, nagu külastatavad üleslaaditavad fotod ja suhtlus suhtlusvõrgustikes. veebisaidid, Sarnaselt jalajälgedega rannas võib teie digitaalne jalajälg paljastada palju teie ja teie veebitegevuste kohta.

Kuid erinevalt rannajälgedest, mis võivad aja jooksul tuhmuda, võib teie digitaalne jalajälg jääda määramata ajaks. See tähendab, et kõik, mida teete või postitate veebis, võib jääda püsivaks, isegi kui selle hiljem kustutate. See püsivus rõhutab, kui oluline on olla teadlik sellest, mida veebis jagate, ja oma digitaalsete toimingute võimalikke tagajärgi.

Teie digitaalses jalajäljes sisalduvat teavet saab kasutada teie üksikasjaliku profiili koostamiseks, sealhulgas teie huvid, harjumused ja käitumised. Oluline on kaaluda, kes sellele teabele juurde pääseb, ja mõista, et isegi rangete privaatsusseadete korral on alati võimalus sisu kopeerida ja jagada väljaspool teie sihtrühma.

Sisuliselt tähendab oma digitaalse jalajälje haldamine seda, et olge teadlik sellest, mis jälje te võrgus maha jätate, ja astute samme tagamaks, et see kajastab täpselt teie kavatsusi ja väärtusi. See hõlmab jagatava sisu suhtes tähelepanelikkust, privaatsusseadete mõistmist ja ettevaatust võrgutoimingute võimalike pikaajaliste tagajärgede suhtes.

Co-funded by the European Union

DIGITAALNE JALAJÄLG

Digitaalse jalajälje haldamine on praegusel digiajastul ülioluline, kus võrgutegevusel võib olla pikaajaline mõju teie isiklikule ja tööelule. Siin on mõned näpunäited, mis aitavad teil oma digitaalset jalajälge tõhusalt hallata.

1. Pöörake tähelepanu sellele, mida jagate: mõelge enne postitamist. Mõelge isikliku teabe, fotode või arvamuste veebis jagamise võimalikele tagajärgedele. Pidage meeles, et kui midagi on postitatud, võib selle täielik eemaldamine olla keeruline.

2. Kasutage privaatsusseadeid: tutvuge sotsiaalmeedia platvormide ja muude võrguteenuste privaatsusseadetega. Kohandage neid seadeid, et juhtida, kes teie postitusi ja teavet näevad.

3. Vaadake regulaarselt üle oma kohalolek võrgus: vaadake perioodiliselt üle oma sotsiaalmeedia profiilid ja veebikontod. Eemaldage või värskendage aegunud või ebaoluline teave.

4. Piirake isikuandmeid: vältige tundliku isikuandmete (nt aadressi, telefoninumbri või finantsandmete) jagamist võrgus.

5.Kasutage tugevaid paroole: volitamata juurdepääsu vältimiseks kasutage oma veebikontode jaoks tugevaid unikaalseid paroole. Paroolide turvaliseks jälgimiseks kaaluge paroolihalduri kasutamist.

6. Olge klõpsamisel ettevaatlik: olge andmepüügipettuste ja pahatahtlike linkide suhtes ettevaatlik. Vältige linkidel klõpsamist ega manuste allalaadimist tundmatutest või kahtlastest allikatest.

7. Jälgige oma mainet veebis: kasutage otsingumootoreid, et regulaarselt kontrollida, milline teave teie kohta on Internetis saadaval. Kui leiate ebatäpset või kahjulikku teavet, võtke kasutusele meetmed selle lahendamiseks.

8. Harige ennast ja teisi: olge kursis veebiohutuse ja privaatsuse parimate tavadega. Õpetage oma sõpru ja perekonda nende digitaalse jalajälje haldamise tähtsusest.

Neid nõuandeid järgides saate tõhusalt hallata oma digitaalset jalajälge ja kaitsta oma mainet veebis. Pidage meeles, et teie veebipõhine kohalolek peegeldab teid, seega on oluline võtta kontroll selle üle, mida jagate ja kuidas end veebis esitlete.

Co-funded by the European Union

INTERNETİS PRİVAATSUS

Interneti-privaatsus, tuntud ka kui Interneti-privaatsus või digitaalne privaatsus, on see, mil määral jääb isiklik, finants- ja sirvimisteave konfidentsiaalseks, kui keegi on võrgus. Internetis jagatud ja salvestatud isikuandmete suureneva hulgaga on mure veebipõhise privaatsuse pärast märkimisväärselt kasvanud.

Interneti-privaatsuse kaitsmine on mitmel põhjusel ülioluline. Esiteks on inimestel õigus oma isikliku elu üksikasju privaatseks jätta ja mitte jagada neid võõrastega. Lisaks võib olla keeruline teada, milliseid isikuandmeid ja kes kogub, kuna ühe ettevõtte kogutud andmeid võidakse jagada teistega ilma teie teadmata või nõusolekuta.

Interneti-andmete privaatsust tuleks käsitleda sama tähtsana kui privaatsust füüsilises maailmas. Nii nagu peaksite pidama konfidentsiaalset vestlust suletud uste taga või jagate pangaga ainult finantsandmeid, peaksite võtma meetmeid oma veebipõhise privaatsuse kaitsmiseks. See hõlmab tugevate unikaalsete paroolide kasutamist, ettevaatlikkust võrgus jagatava teabe suhtes ning oma privaatsusseadete regulaarset ülevaatamist sotsiaalmeedias ja muudel veebiplatvormidel.

Väärtustades ja kaitstes oma veebipõhist privaatsust, saate vähendada riski, et teie isikuandmeid väärkasutatakse või jagatakse ilma teie nõusolekuta.

Co-funded by
the European Union

ANDMETE PRİVAATSUS

Andmete privaatsus on põhiõigus, mis on pälvinud märkimisväärset tähelepanu eelkõige seoses isikuandmete kaitse üldmääruse (GDPR) rakendamisega Euroopa Liidus. 2018. aastal jõustunud GDPR eesmärk oli kaitsta iga ELi kodaniku privaatsust ja andmeid, kehtestades ranged reeglid isikuandmete kogumise, töötlemise ja säilitamise kohta.

GDPR sisaldab 99 artiklit, mis kirjeldavad andmekaitse erinevaid aspekte. Mõned põhisätted hõlmavad järgmist:

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

2. Õigus kustutada: tuntud ka kui "õigus olla unustatud", võivad üksikisikud teatud tingimustel taotleda oma isikuandmete kustutamist.

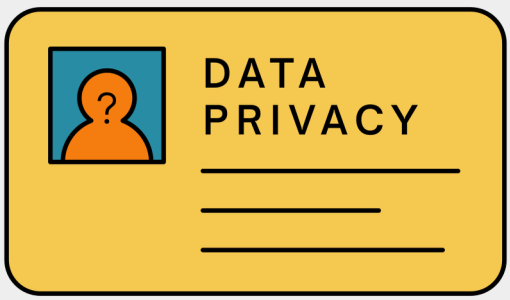
3. Nõusolek: ettevõtted peavad enne nende isikuandmete kogumist või töötlemist saama üksikisikutelt selgesõnalise nõusoleku. See hõlmab selget ja ühemõttelist nõusolekut küpsiste ja sirvimisajaloo kasutamiseks.

4. Andmete minimeerimine: ettevõtted peaksid koguma ja töötlema ainult andmeid, mis on vajalikud nende kogumise eesmärgil.

5.Andmete teisaldatavus: üksikisikutel on õigus saada ettevõttelt oma isikuandmeid üldkasutatavas ja masinloetavas vormingus.

6. Andmekaitseametnikud: mõned organisatsioonid peavad määrama andmekaitseametniku, kes jälgib GDPR-i järgimist.

GDPR on oluliselt mõjutanud seda, kuidas ettevõtted isikuandmeid käitlevad, nõudes neilt rangemate andmekaitsemeetmete rakendamist ja andmetöötlustavade suuremat läbipaistvust. GDPR on aidanud kaasa andmete privaatsusõiguste suurendamisele ja andnud inimestele võimaluse omada rohkem kontrolli oma isikuandmete üle.



Co-funded by
the European Union

INTERNETİS ÄHVARDUSED

Küberohud on pahatahtlikud tegevused, mille eesmärk on andmete kahjustamine, teabe varastamine või digitaalsete toimingute häirimine. Need ohud hõlmavad suurt hulka tegevusi, sealhulgas küberrünnakuid, mis on suunatud infotehnoloogia varadele, arvutivõrkudele, intellektuaalomandile ja tundlikele andmetele. Küberohud võivad pärineda nii sisemistest kui ka välistest allikatest.

Sisemised ohud võivad tekkida organisatsiooni usaldusväärsetest kasutajatest, kes kuritarvitavad oma õigusi või juurdepääsu tundlikule teabele. Välised ohud aga pärinevad kaugetest kohtadest ja sageli panevad neid toime tundmatud osapooled, kes soovivad ära kasutada digitaalsete süsteemide haavatavusi.

Küberohtude näideteks on pahavara, lunavara, andmepüügirünnakud ja teenuse keelamise (DoS) rünnakud. Nendel ohtudel võivad olla tõsised tagajärjed, sealhulgas rahalised kaotused, andmetega seotud rikkumised ja organisatsiooni maine kahjustamine.

Küberohtude eest kaitsmiseks peavad organisatsioonid ja üksikisikud rakendama jõulisi küberjulgeolekumeetmeid. See hõlmab tarkvara regulaarset värskendamist, tugevate paroolide kasutamist, tundlike andmete krüptimist ning kasutajate harimist võimalike ohtude ja nende vältimise kohta. Lisaks võib mitmefaktorilise autentimise rakendamine ja andmete korrapärane varundamine aidata leevendada küberrünnaku mõju.

Co-funded by
the European Union

INTERNETİS OLEVAD OHUD

Interneti-ohtu võib määratleda kui kõike, mis võib Interneti-kasutajat kahjustada. See kahju võib esineda mitmel kujul (nt füüsiline, emotsionaalne, psühholoogiline, rahaline, sotsiaalne ja maine). Allpool on kirjeldatud paljusid Interneti-ohtude tüüpe.

Interneti-ohtude tüübid:
Tänapäeval on Internetis juurdepääs peaaegu kõigele, alates meelelahutusest, krediidi- ja finantsteenustest kuni toodeteni kõikjalt maailmast. Kuigi Internet pakub teatud tasemel anonüümsust, on üha rohkem viise, kuidas kasutaja isikuandmed võivad ohtu sattuda.

1-Küberkiusamine : küberkiusamine on kiusamise vorm, mis toimub digitaaltehnoloogiate, näiteks sotsiaalmeedia, sõnumiplatvormide, mänguplatvormide ja mobiiltelefonide abil. See hõlmab korduvat käitumist, mille eesmärk on sihikule suunatud isiku hirmutamine, vihastamine või häbistamine. Küberkiusamise näideteks on valede või kuulujuttude levitamine kellegi kohta sotsiaalmeedias, solvavate sõnumite või ähvarduste saatmine sõnumsiderakenduste kaudu ning kellegi teisena esinemine, et saata alatuid sõnumeid.

Üks peamisi erinevusi näost näkku kiusamise ja küberkiusamise vahel on see, et küberkiusamine jätab digitaalse jalajälje. See tähendab, et kiusamiskäitumine on registreeritud, mis võib olla kasulik tõendite esitamisel kuritarvitamise peatamiseks. On oluline, et inimesed oleksid teadlikud oma digitaalsest jalajäljest ja mõistaksid, et nende võrgutoimingutel võivad olla tegelikud tagajärjed.

Küberkiusamise vastu võitlemiseks on oluline, et inimesed teavitaksid igast küberkiusamise juhtumist vastavat platvormi või ametiasutust. Samuti on oluline harida noori vastutustundliku veebikäitumise ja küberkiusamise mõju kohta. Koos töötades saame luua turvalisema veebikeskkonna kõigile.

Co-funded by
the European Union

INTERNETİS OLEVAD OHUD

2- Küberkiskjad : küberkiskja on isik, tavaliselt täiskasvanu, kes kasutab Internetti laste ja teismeliste ärakasutamiseks väärkohtlemise vormide, sealhulgas seksuaalse, mitmesuguste emotsionaalse, psühholoogilise või rahalise kahju tekitamiseks. Need röövloomad sihivad haavatavaid inimesi erinevate veebiplatvormide, näiteks jututubade, kiirsõnumite, suhtlusvõrgustike ja videomängude kaudu.

Üks levinud taktika, mida küberkiskjad kasutavad, on valeidentiteedi loomine, teeseldes end lapse või teismelisena. Nad kasutavad seda võltsidentiteeti oma ohvritega suhete loomiseks, saavutades järk-järgult nende usalduse ja manipuleerides neid kahjulike tegevustega.

Hoolitsemisprotsess on Cyber Predatorsi põhistrateegia, mille käigus nad manipuleerivad oma ohvritega aja jooksul aeglaselt, kasutades sageli ära nende haavatavust ja ebakindlust. See protsess võib hõlmata näiliselt tõelise sõpruse või suhte loomist ohvriga, enne kui teda omakasu eesmärgil ära kasutatakse.

Lapsevanemate, hooldajate ja pedagoogide jaoks on ülioluline harida lapsi ja teismelisi veebiohutuse ja küberkiskjate ohtude kohta. Avatud suhtlemise julgustamine võrgusuhtluse teemal ja piiride seadmine võib aidata kaitsta noori nende kiskjate ohvriks langemise eest. Lisaks võib võrgutegevuste jälgimine ja hoiatusmärkidest teadlik olemine aidata tuvastada ja ära hoida võimalikku kuritarvitamist.

Co-funded by the European Union

INTERNETİS OLEVAD OHUD

3- Privaatse teabe postitamine Isikuandmete jagamise vältimine on andmete kaitsmiseks, identiteedivarguste ärahoidmiseks ja võrgus turvalisuse tagamiseks ülioluline. See on oluline mitte ainult veebis surfamisel, vaid ka sotsiaalmeedia platvormidel teabe kasutamisel ja jagamisel.

Näited isikuandmetest, mida tuleks kaitsta, on järgmised:
1. Nimed: täisnimi, perekonnanimi ja vanemate nimed.
2. Isikukoodid: sotsiaalkindlustuse number, juhiloa number, passi number, patsiendi ID number, maksumaksja ID number, krediidikonto number või finantskonto number.
3. Aadressid: tänav ja e-posti aadress.
4. Biomeetria: võrkkesta skaneeringud, sõrmejäljed, näo geomeetria või häälallkirjad.
5. Sõiduki ID või tiitlinumbrid.
6. Telefoninumbrid.
7. Tehnoloogiavarateave: meedia juurdepääsu juhtimise (MAC) või Interneti-protokolli (IP) aadressid, mis on seotud teatud isikuga.

Sotsiaalmeediat kasutades on oluline olla tähelepanelik jagatava teabe suhtes. Vältige isiklike andmete, nagu täisnimi, aadress või telefoninumber, avalikult postitamist. Kasutage privaatsusseadeid, et juhtida, kes teie postitusi ja teavet näevad, ning olge ettevaatlik tundmatutelt isikutelt pärit sõbrakutsete või sõnumite vastuvõtmisel.
Olles oma isikuandmete kaitsmisel valvas, saate vähendada identiteedivarguste ja muude võrguohtude riski.

Co-funded by the European Union

INTERNETİS OLEVAD OHUD

4- Andmepüük: andmepüügirünnakud on petlik taktika, mida küberkurjategijad kasutavad, et meelitada inimesi välja andma tundlikku teavet, näiteks krediitkaardinumbreid või sisselogimisandmeid. Need rünnakud hõlmavad tavaliselt võltsitud suhtlust, näiteks e-kirju või sõnumeid, mis näivad olevat pärit seaduslikest allikatest. Andmepüügirünnakute eesmärk on varastada isikuandmeid või installida ohvri seadmesse pahavara.

Andmepüügirünnakud võivad esineda erineval kujul, sealhulgas meilid, mis näivad olevat pärit teie pangast või populaarsest veebiteenusest. Need meilid sisaldavad sageli linke, millel klõpsamine suunab võltsveebisaitidele, mis jäljendavad seadusliku saidi välimust. Võltsveebisaidile sattudes palutakse ohvritel sisestada oma isiklikud andmed, mille seejärel küberkurjategijad kinni püüavad.

Kui andmepüügirünnakuid on traditsiooniliselt seostatud meilidega, siis küberkurjategijad kasutavad nüüd ohvrite sihtimiseks muid meetodeid. See hõlmab tekstisõnumeid, telefonikõnesid, võltsrakendusi ja sotsiaalmeedia viktoriinid. Need taktikad on loodud selleks, et meelitada inimesi oma isikuandmeid esitama või pahatahtlikel linkidel klõpsama.

Andmepüügirünnakute eest kaitsmiseks on oluline olla ettevaatlik e-kirjade või tundmatute saatjate kirjade avamisel. Kontrollige e-kirjade autentsust, kontrollides saatja e-posti aadressi ja vältides linkidel klõpsamist ega kahtlastest allikatest manuste allalaadimist. Lisaks kasutage andmepüügirünnakute tuvastamiseks ja ärahoidmiseks turvatarkvara ja hoidke seda ajakohasena

Co-funded by the European Union

INTERNETİS OLEVAD OHUD

5- Pettustele langemine: Interneti-pettused on petturlikud skeemid, mida küberkurjategijad Internetis läbi viivad. Need pettused võivad esineda erineval kujul ja nende eesmärk on petta üksikisikuid, et nad esitaksid tundlikku teavet või raha. Interneti-pettused võivad toimuda erinevate kanalite kaudu, sealhulgas andmepüügimeilid, sotsiaalmeedia, SMS-id, võltsitud tehnilise toe telefonikõned ja hirmutusvara. Interneti-pettuste peamine eesmärk on sageli varastada isikuandmeid, nagu krediitkaardiandmed või sisselogimisandmed, või petta inimesi petturile raha saatma. Mõned levinumad Interneti-pettuste tüübid on järgmised:

1. Andmepüügimeilid: meilid, mis näivad olevat pärit seaduslikelt organisatsioonidelt, nagu pangad või valitsusasutused, kuid tegelikult püütakse inimesi petta, et nad esitaksid isikuandmeid või klõpsaksid pahatahtlikel linkidel.
2. Sotsiaalmeedia pettused: sotsiaalmeedia platvormidel toimuvad pettused, nagu võltsprofiilid või reklaamid, mis viivad andmepüügiveebisaitidele või pahavara allalaadimiseni.

3. SMS-pettused: tekstisõnumiga saadetud pettused, mis sisaldavad sageli linke võltsitud veebisaitidele või isikuandmete päringuid.

4. Võltstehnilise toe kõned: petturid, kes esinevad tehnilise toe esindajatena, kes püüavad veenda inimesi, et nende arvutis on probleem, ja seejärel taotlevad makset või juurdepääsu arvutile, et probleem "parandada".

5. Hirmutusvara: võltstarkvara või hüpikaknad, mis väidavad, et arvuti on viirusega nakatunud, ja õhutavad kasutajat ostma tarbetut tarkvara või teenuseid.

Interneti-pettuste eest kaitsmiseks on oluline olla ettevaatlik soovimatute sõnumite või isikuandmete päringute saamisel. Enne teabe esitamist või linkidel klõpsamist kontrollige saatja või organisatsiooni õiguspärasust. Lisaks kasutage pettuste tuvastamiseks ja ärahoidmiseks ajakohast turvatarkvara.

Co-funded by the European Union

INTERNETİS OLEVAD OHUD

6- Pahavara kogemata allalaadimine: pahavara kogemata allalaadimine on tavaline arvutiturbeoht, millel võivad olla tõsised tagajärjed. Pahavara ehk pahatahtliku tarkvara lühend hõlmab viiruseid, usse, troojalasi ja muid kahjulikke programme, mis on loodud teie arvutisüsteemi kahjustama või häirima.

Arvutiviirus on teatud tüüpi pahavara, mis on võimeline ennast paljunema ja levima teistesse arvutitesse. See võib muuta teie arvuti tööviisi, sageli teie teadmata või loata, ning põhjustada mitmesuguseid probleeme, alates väiksematest tüütustest kuni tõsiste kahjustusteni.

Pahavara kogemata allalaadimise vältimiseks on oluline olla Internetist tarkvara allalaadimisel ettevaatlik. Hinnake hoolikalt tasuta tarkvara ja vältige allalaadimist peer-to-peer failijagamise saitidelt, kuna need on levinud pahavara allikad. Lisaks olge ettevaatlik tundmatutelt saatjatelt pärit meilide suhtes, kuna need võivad sisaldada pahatahtlikke manuseid või linke.

Enamikul tänapäeva veebibrauseritel on sisseehitatud turvaseaded, mis aitavad kaitsta võrguohtude eest. Oluline on hoida neid sätteid ajakohasena ja lubada täiendavaid turvafunktsioone, nagu hüpikakende blokeerijad ja andmepüügivastased tööriistad.
Kõige tõhusam viis viiruste ja muu pahavara eest kaitsmiseks on aga kasutada maineka pakkuja ajakohast viirusetõrjetarkvara. Viirusetõrjetarkvara aitab tuvastada ja eemaldada teie arvutist pahavara ning pakkuda reaalajas kaitset uute ohtude eest. Viirusetõrjetarkvara regulaarne värskendamine ja arvuti kontrollimine aitab kaitsta teie süsteemi pahavara nakatumise eest.

Co-funded by
the European Union

VÕTMEPÄDEVUSED VEEBİS TURVALİSEKS OLEMİSEKS

Veebiohutus on kõikehõlmav sõna, mis julgustab lapsi, noori ja haavatavamaid pereliikmeid Internetiga ühendatud seadmete kasutamisel turvaliselt. Internetimaailm võib laste ja teismeliste elu rikastada mitmel viisil, nii isiklikult kui ka hariduslikult.
Oluline on kokku võtta õppijate võtmepädevused, et veebis turvaliselt püsida:

a.Tunnistage riske: Interneti-tegevusega seotud riskide teadvustamine on Internetis turvalisuse tagamiseks üliloluline. Tuvastades võimalikud ohud ja ohud, saavad üksikisikud astuda ennetavaid samme, et vähendada oma kokkupuudet veebis ja kaitsta end kahju eest.

Alustuseks on oluline omaks võtta ennetav lähenemine veebiturvalisusele. See tähendab, et tuleb olla teadlik võimalikest riskidest ja võtta meetmeid nende maandamiseks enne, kui need muutuvad probleemiks. Olles kursis levinud veebiohtudega, nagu andmepüügipettused, pahavara ja identiteedivargused, saavad üksikisikud end nende ohtude eest paremini kaitsta.

Veebis kokkupuutumise vähendamine on võrgus turvalise püsimise teine oluline aspekt. See võib hõlmata sotsiaalmeedias ja muudel veebisaitidel jagatava isikliku teabe hulga piiramist, privaatsusseadete kasutamist, et kontrollida, kes teie teavet näevad, ning olla ettevaatlik linkidel klõpsamisel või tundmatutest allikatest manuste allalaadimisel.

Interneti-tegevusega seotud riskide mõistmine ja ennetavate meetmete võtmine kokkupuute vähendamiseks on digitaalmaailmas turvalisuse tagamiseks hädavajalik. Olles kursis ja tegutsedes ennetavalt, saavad inimesed end võrguohtude eest kaitsta ja nautida turvalisemat veebikogemust.

Co-funded by
the European Union

VÕTMEPÄDEVUSED VEEBİS TURVALİSEKS OLEMİSEKS

b. Hoidke isikuandmeid turvaliselt:
Isikuandmete turvaline hoidmine on turvalise veebis kohaloleku säilitamiseks hädavajalik. Oma identiteedi kaitsmiseks ja turvalise digitaalse elu tagamiseks nii teile kui teie perele on oluline järgida teatud juhiseid.

1.Kasutage tugevaid unikaalseid paroole: paroolid on teie digimaja võtmed. Väga oluline on kasutada iga konto jaoks tugevaid unikaalseid paroole ning vältida kergesti äraarvatavate paroolide kasutamist. Kaaluge usaldusväärse paroolihalduri kasutamist keerukate paroolide turvaliseks genereerimiseks ja salvestamiseks.

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

3. Andmete varundamine. Varundage regulaarselt olulisi andmeid, et kaitsta neid kaotsimineku või varguse eest. Seda saab teha väliste kõvaketaste, pilvesalvestusteenuste või muude varunduslahenduste abil. Varundusandmed tuleks krüpteerida ja turvaliselt salvestada.

4. Hoidke tarkvara ajakohasena: veenduge, et kogu teie seadmete tarkvara, sealhulgas operatsioonisüsteeme, brausereid ja rakendusi, värskendataks regulaarselt uusimate turvapaikade ja värskendustega. See aitab kaitsta haavatavuste eest, mida küberkurjategijad võivad ära kasutada.

5. Turvatarkvara kasutamine: installige oma seadmetesse mainekas viiruse- ja pahavaratõrjetarkvara ning värskendage neid regulaarselt, et kaitsta end viiruste, pahavara ja muude võrguohtude eest.

6. Lubage kahefaktoriline autentimine (2FA): lisaturvakihi lisamiseks lubage oma kontodel võimaluse korral 2FA. See nõuab lisaks paroolile teist kinnitusviisi, näiteks teie telefoni saadetud koodi.

Neid juhiseid järgides saate aidata kaitsta oma isikuandmeid ja tagada teile ja teie perele turvalisema veebikogemuse.

Co-funded by
the European Union

VÕTMEPÄDEVUSED VEEBİS TURVALİSEKS OLEMİSEKS

c.Ärge laadige alla tundmatuid faile : tundmatute failide allalaadimine võib teie arvuti ja isikliku teabe ohustada mitmesuguseid riske, sealhulgas pahavara, viirused ja muu pahatahtlik tarkvara. Enda ja oma seadmete kaitsmiseks on oluline järgida järgmisi juhiseid.

1. Olge e-kirjade manuste suhtes ettevaatlik: ärge laadige alla tundmatute või kahtlaste meilide manuseid. Need manused võivad sisaldada pahavara, mis võib teie arvutit kahjustada või teie isikuandmeid varastada.

2. Kontrollige allikat: enne mis tahes faili allalaadimist kontrollige allikas veendumaks, et see on õigustatud. Laadige faile alla ainult usaldusväärsetelt veebisaitidelt ja allikatest.

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

4. Luba faililaiendid: lubage oma operatsioonisüsteemis faililaiendid, et näeksite faili täisnime. See võib aidata tuvastada potentsiaalselt pahatahtlikke faile.

5. Vältige P2P (peer-to-peer) failide jagamist: olge P2P-failide jagamise teenuste kasutamisel ettevaatlik, kuna need võivad teid paljastada pahavara ja muude riskide eest. Laadige faile alla ainult usaldusväärsetest allikatest.

6. Kontrollige faile enne avamist: kasutage allalaaditud failide enne avamist kontrollimiseks viirusetõrjetarkvara. See võib aidata tuvastada failis leiduvat pahavara või viirusi.

Neid juhiseid järgides saate vähendada tundmatute failide allalaadimise ohtu ning kaitsta oma arvutit ja isiklikku teavet võrguohtude eest.

Co-funded by the European Union

VÕTMEPÄDEVUSED VEEBİS TURVALİSEKS OLEMİSEKS

d. Kasutage kriitilise mõtlemise oskusi teabe analüüsimiseks ja hindamiseks veebis; Kriitilise mõtlemise oskuste kasutamine teabe analüüsimiseks ja hindamiseks veebis on oluline, et kaitsta end pettuste, andmepüügikatsete ja valeinformatsiooni eest. Siin on mõned juhised, mis aitavad teil end turvaliselt hoida.

1. Olge skeptiline: seadke kahtluse alla võrgus leiduva teabe allikas ja kehtivus. Kui miski tundub liiga hea, et tõsi olla, või ei tundu päris õige, on parem enne mis tahes toimingu tegemist põhjalikumalt uurida.

2. Kontrollige õigekirjavigu ja kahtlasi e-posti aadresse: olge ettevaatlik kirjade, sõnumite või veebisaitide suhtes, mis sisaldavad õigekirjavigu või kasutavad ebaõigeid e-posti aadresse. Need võivad olla andmepüügikatsete või pettuste märgid.

3. Kontrollige allikat: enne mis tahes linkidel klõpsamist või manuste allalaadimist kontrollige teabe allikat. Otsige ametlikke veebisaite või usaldusväärseid allikaid, et tagada teabe õiguspärasus.

4. Enne klõpsamist mõelge: vältige klõpsamist tundmatutest või kahtlastest allikatest pärit meilides või sõnumites olevatel linkidel või manustel. Hõljutage kursorit linkide kohal, et näha enne klõpsamist tegelikku URL-i.

5. Olge ebatavalise suhtluse suhtes ettevaatlik: kui saate sõbralt või tuttavalt sõnumi, mis tundub ebaloomulik või ootamatu, kontrollige enne toimingu allikat. Nende konto võib olla rikutud.

6. Turvatarkvara kasutamine: installige oma seadmetesse viiruse- ja pahavaratõrjetarkvara ning värskendage neid regulaarselt. See võib aidata tuvastada pahatahtliku tarkvara teie seadet ja vältida selle nakatamist.

Kriitilise mõtlemise oskusi kasutades ja neid juhiseid järgides saate end kaitsta võrguohtude ja valeinformatsiooni eest.

Co-funded by the European Union

VÕTMEPÄDEVUSED VEEBİS TURVALİSEKS OLEMİSEKS

e. Veenduge, et veebisait, millel viibite, on ohutu: Veebisaidi ohutuse kontrollimine on veebiohtude eest kaitsmiseks ülioluline, eriti tundliku teabe, näiteks makseteabe sisestamisel. Siin on mõned sammud veebisaidi ohutuse kontrollimiseks.

1. Kontrollige URL-i: vaadake veebisaidi URL-i ja veenduge, et selle alguses oleks "https://", mitte ainult "http://". "S" tähistab turvalist ja näitab, et veebisaidil on SSL- sertifikaat, mis krüpteerib teie brauseri ja veebisaidi vahel edastatavad andmed.

2. Otsige tabaluku ikooni: otsige URL-i kõrval aadressiribal tabaluku ikooni. See näitab, et veebisait on turvaline ja kasutab HTTPS-i krüptimist.

3. Veebisaidi legitiimsuse kontrollimine: enne isikliku või makseteabe sisestamist kontrollige veebisaidi legitiimsust. Otsige kontaktteavet, nagu füüsiline aadress ja telefoninumber, ning vaadake teiste kasutajate arvustusi või hinnanguid.

4.Kasutage turvalist makseviisi. Internetis ostlemisel kasutage turvalist makseviisi, nagu PayPal või krediitkaart, mis pakub ostjale kaitset. Vältige deebetkaartide või pangaülekannete kasutamist, kuna need pakuvad vähem kaitset pettuste eest.

5.Kasutage kõrge turvalisusega brauserit: kaaluge brauseri kasutamist, mis pakub täiendavaid turvafunktsioone, nagu sisseehitatud andmepüügi- ja pahavarakaitse. Mõned brauserid kuvavad ka rohelist aadressiriba või muid indikaatoreid, mis näitavad, et veebisait on ohutu.

6. Värskendage oma brauserit ja turvatarkvara: hoidke oma brauser ja turbetarkvara ajakohasena, et kaitsta end uusimate ohtude ja haavatavuste eest.
Järgides neid juhiseid, saate tagada, et külastatavad veebisaidid on turvalised ja kaitsta end ostlemise või veebi sirvimise ajal võrguohtude eest.

f. Olge teadlik oma digitaalsest jalajäljest. Olles võrgus, alati võrgus: kõik, mis on veebis postitatud, on seal kõigile nähtav, tuleb olla ettevaatlik sotsiaalmeedia profiilides ja külastatud, registreeritud või mis tahes tüüpi kasutajate andmeid sisaldava identifitseeriva teabega. isiklik informatsioon.

Co-funded by
the European Union

ENNETAVAD MEETMED JA JUHISED VÕRGUOHUTUSE TAGAMISEKS

• Turvalisema mõtteviisi omaksvõtt on võrgus turvalisuse tagamiseks üliioluline, kuna see aitab inimestel ära tunda võimalikke riske ja võtta ennetavaid meetmeid enda kaitsmiseks. Siin on mõned põhipunktid, mida meeles pidada.

1. Olge vale turvatunde suhtes ettevaatlik: kuigi arvutid võivad tunduda turvalised, võivad need olla haavatavad erinevate võrguohtude suhtes. Oluline on meeles pidada, et küberkurjategijad võivad Interneti kaudu tekitada tõelist kahju, näiteks identiteedivargust, rahalist kahju ja teie seadmeid kahjustada.

2. Olge kursis: hoidke end kursis viimaste veebiohtude ja turvalisuse parimate tavadega. See võib aidata teil võimalikke riske ära tunda ja võtta asjakohaseid meetmeid enda kaitsmiseks.

3. Järgige ohutusmeetmeid: rakendage ülalkirjeldatud ohutusmeetmeid , nagu tugevate unikaalsete paroolide kasutamine, tarkvara ajakohasena hoidmine ja kahtlastel linkidel või manuste klõpsamise vältimine.

4.Kasutage tervet mõistust: kasutage võrgus suheldes tervet mõistust. Kui miski tundub liiga hea, et tõsi olla, või ei tundu õige, on parem olla ettevaatlik ja seda vältida.

5. Olge ennetav: astuge ennetavaid samme, et kaitsta end võrgus, nt regulaarselt varundada andmeid, kasutada turvatarkvara ja olla võrgus jagatava teabe suhtes ettevaatlik.

6. Olge valvs: olge valvs ja olge teadlik oma võrgukeskkonnast. Olge soovimatute e-kirjade, sõnumite või isikuandmete päringute suhtes ettevaatlik ning kontrollige allikat enne mis tahes toimingu tegemist.

Co-funded by
the European Union

ENNETAVAD MEETMED JA JUHISED VÕRGUOHUTUSE TAGAMISEKS

Kui võtate kasutusele turvalisema mõtteviisi ja järgite neid juhiseid, saate kaitsta end võrguohtude eest ja nautida turvalisemat võrgukogemust.

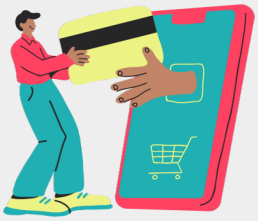
• Loo tugevamad paroolid.
Tugev parool on üks parimaid viise oma kontode ja privaatsete andmete kaitsmiseks häkkerite eest.

• Brauseri turvafunktsioonid Arvutid seisavad veebi sirvimisel silmitsi erinevate ohtudega, sealhulgas viiruste, pahavara ja nuhkvaraga. Hea uudis on see, et teie veebibrauseril on palju sisseehitatud turvafunktsioone, mis aitavad teie arvutit kaitsta.

• Rämpsposti ja kalapüügi vältimine
Meilipettuste, pahatahtliku tarkvara ja identiteedivarguse eest kaitsmiseks on vaja mõista, kuidas potentsiaalselt ohtlikku sisu tuvastada ja vältida.

•Vältige viirusetõrjega pahavara. Pahavara on võrgus olles üks levinumaid ohte teie arvutile, kuid seda on lihtne vältida. Põhialuseks on arvuti turvamine ning kahtlaste linkide tuvastamise ja vältimise õppimine.

•Ohutu veebipõhine ostlemine Internetis ostlemine on mugav viis mugavalt kodust ostlemiseks. Ja kuigi sellel on palju eeliseid, on ka mõned riskid. Oma finantsandmete kaitsmiseks ja turvalisuse tagamiseks on olemas viise, näiteks veebisaidi turvalisuse ja õigsuse kontrollimine.



Co-funded by
the European Union

VANEMLİK KONTROLL

Vanemlik kontroll on oluline tööriist teie lapse turvalisuse tagamiseks võrgus. Siin on mõned põhipunktid, mida kaaluda:

1. Sisu filtreerimine: vanemlik järelevalve võimaldab teil filtreerida sisu, millele teie laps võrgus juurde pääseb, blokeerides sobimatud veebisaidid ja materjalid.

2. Ajapiirangud: määrake oma lapse võrgutegevusele ajapiirangud, et ta ei veedaks liiga palju aega võrgus.

3. Rakenduste ja mängude juhtnupud: saate juhtida, milliseid rakendusi ja mänge teie laps saab alla laadida ja neile juurde pääseda, tagades, et need on vanusele sobivad.

4. Privaatsusseaded: veenduge, et teie lapse privaatsusseaded on tema isikuandmete kaitsmiseks õigesti konfigureeritud.

5.Jälgimine ja jälgimine: mõned vanemliku kontrolli tööriistad võimaldavad jälgida oma lapse veebitegevusi ja jälgida tema asukohta.

6. Haridus ja suhtlemine: oluline on õpetada oma last veebiohutuse ja vastutustundliku interneti kasutamise olulisuse kohta. Julgustage avatud suhtlemist, et nad tunneksid end mugavalt kõigi probleemide või probleemide üle, millega nad veebis kokku puutuvad.

7. Seadete korrapärane ülevaatamine: vaadake regulaarselt üle ja värskendage oma vanemliku järelevalve seadeid, et tagada nende vastavus teie lapse vanusele ja küpsusastmele.

Pidage meeles, et kuigi vanemlik kontroll on väärtuslik tööriist, ei ole see lollikindel. Samuti on oluline õpetada oma lapsele kriitilise mõtlemise oskusi ja vastupidavust, et ta saaks veebimaailmas turvaliselt ja enesekindlalt navigeerida.

Co-funded by
the European Union

ERİNEVAT TÜÜPİ VANEMLİKU JÄRELEVALVE JAOTUS

Vanemlik järelevalve pakub erinevaid funktsioone, mis aitavad vanematel oma laste võrgutegevusi hallata. Siin on eri tüüpi vanemliku järelevalve jaotus.

1. Filtreerimine ja blokeerimine: need funktsioonid piiravad juurdepääsu teatud veebisaitidele, sõnadele või piltidele, mida vanemad peavad sobimatuks. Need võivad aidata lapsi kaitsta kahjuliku veebisisu juurdepääsu eest.

2. Väljuva sisu blokeerimine: see funktsioon takistab lastel isiklikku teavet võrgus ja meili teel jagamast, aidates kaitsta nende privaatsust ja turvalisust.

3. Aja piiramine. Vanemad saavad määrata ajapiirangud, kui kaua nende lastel on lubatud Internetis olla ja millisel kellaajal nad saavad internetti kasutada. See võib aidata hallata ekraaniaega ja tagada, et lapsed ei oleks sobimatutel aegadel võrgus.

4. Jälgimistööriistad: need tööriistad hoiatavad vanemaid nende laste võrgutegevusest ilma juurdepääsu blokeerimata. Nad saavad salvestada, milliseid veebisaite laps on külastanud, ja kuvada hoiatussõnumeid, kui ta külastab teatud saite. See võimaldab vanematel olla kursis oma laste veebikäitumisega.

Oluline on märkida, et kuigi vanemlik kontroll võib aidata lapsi võrgus kaitsta, ei asenda see haridust, vastutust ega täiskasvanute järelevalvet. Vanemad peaksid oma lapsi teavitama Interneti võimalikest ohtudest ning kehtestama reeglid sobivate ja sobimatute veebisaitide kohta. Avatud ja ausad vestlused lastega on turvalise veebikeskkonna loomisel võtmetähtsusega, kus nad tunnevad end mugavalt, et arutada kõiki probleeme või probleeme, millega nad veebis kokku puutuvad.

Co-funded by
the European Union

VANEMLIKU JÄRELEVALVE PÕHIJUHISED

Vanemlik järelevalve on laste turvalisuse tagamisel võrgus üliioluline. Siin on mõned tõhusa vanemliku järelevalve põhijuhised:

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

2.Hoidke arvutit ühises ruumis: asetage arvuti maja üldkasutatavasse kohta, näiteks elutuppa, kus saate selle kasutamist hõlpsalt jälgida. Vältige arvutite paigutamist üksikutesse magamistubadesse ja jälgige nutitelefonides või tahvelarvutites veedetud aega.

3.Laste lemmiksaitide lisamine järjehoidjatesse: laste lemmiksaitide lisamine järjehoidjatesse, et neil oleks lihtne juurdepääs, aitab neil Internetis turvaliselt liikuda ja vähendab sobimatule sisule juurdepääsu ohtu.

4. Kontrollige finantskontosid: kontrollige regulaarselt finantskontosid, kaardiväljavõtteid ja telefoniarveid tundmatute tasude suhtes, mis võivad viidata volitamata veebiostudele.

5. Küsige veebikaitse kohta: uurige, millised võrgukaitsemeetmed on teie lapse koolis, koolijärgses keskuses, sõprade kodudes või mujal, kus lapsed võivad arvutit ilma järelevalveta kasutada.

6. Võtke aruandeid tõsiselt: kui teie laps teatab ebamugavast võrguvahetusest või juhtumist, võtke seda tõsiselt ja uurige probleemi viivitamatult. Julgustage avatud suhtlemist, et teie laps tunneks end mugavalt oma murede arutamisel.

Co-funded by
the European Union

NÕUANDED VANEMLİKUKS JÄRELEVALVEKS

Ühendkuningriigi turvalisema Interneti keskuse direktor Will Gardneril on kasulikku teavet vanemate või karjääri kohta, kes soovivad hallata oma laste ja pere suhteid Internetiga. Välja otsitud aadressilt: https://inews.co.uk/news/technology/tips-and-guidance-for-children-and-parents-for-staying-safe-online-254485

• Küsige oma pereliikmetelt (eriti lastelt), milliseid tundeid internet neis tekitab „Rääkige oma lapsega regulaarselt, kuidas ta tehnoloogiat kasutab, ja uurige, milline on tema digitaalne elu, sealhulgas millised on tema lemmiksaidid ja -teenused ning kuidas võrgus olemine teda tunneb. Oma lapse kuulamine annab teile parima võimaliku ettekujutuse, kuidas saate teda toetada.

• Laste ülekoormamine piirangutega ei ole kasulik „Lapsevanematena on loomulik, et tunnete muret ohtude pärast, mida teie laps võrgus viibimisega kaasnevad, kuid noorte jaoks on võrgumaailm põnev ja lõbus, kuna see pakub neile palju võimalusi. „Pidage meeles, et teie laps kasutab tehnoloogiat ja internetti erinevalt, kuna ta kasvab üles maailmas, mis on sukeldunud kõigesse digitaalsesse. Püüdke vaadata nii võrgus viibimise positiivseid kui ka negatiivseid külgi ja andke oma lapsele võimalus teha turvalisi valikuid, selle asemel, et piirangutega koormata.

• Õppige tundma rakendusi ja teenuseid, mida nad kasutavad. "Saate astuda samme oma lapse toetamiseks võrgus, kasutades selliseid funktsioone nagu sotsiaalmeedia privaatsusseaded ja mõista, kuidas mitmesuguste rakenduste, mängude ja teenuste kohta aruannet koostada."

• Kasutage abistamiseks olemasolevaid tööriistu. "Pere kasutatavate seadmete haldamiseks on palju tööriistu. Näiteks teadmine, kuidas vanemlikku järelevalvet aktiveerida ja kasutada, aitab kaitsta teie last veebis sobimatu sisu nägemise eest.

Co-funded by the European Union

INTERNETİ-OHUTUSE KONTROLL-LEHT

Nortoni turvakeskuse andmetel võib võrgus ohutu mängimine aidata vältida teie ja teie pere kokkupuudet soovimatu teabe, materjalide või Interneti-riskidega, mis võivad kahjustada teie seadmeid, isiklikku teavet või perekonda. Arukas on õpetada spetsiaalselt lastele arvutiohutust, et nad ei langeks mõne levinud ohu ohvriks, mida me varem mainisime.

Siin on Interneti-ohutuse kontroll-loend, mis põhineb Nortoni turvakeskuse nõuannetel:

1. Kasutage tugevaid unikaalseid paroole. Veenduge, et kõigil kontodel oleksid tugevad kordumatud paroolid, et kaitsta neid volitamata juurdepääsu eest.

2. Hoidke tarkvara ajakohasena: turvaaukude eest kaitsmiseks värskendage regulaarselt operatsioonisüsteeme, brausereid ja turbetarkvara.

3. Turvatarkvara kasutamine: installige hea mainega viiruse- ja pahavaratõrjetarkvara, et kaitsta end viiruste ja muude ohtude eest.

4. Olge andmepüügipettuste suhtes ettevaatlik: olge ettevaatlik meilide, sõnumite või veebisaitide suhtes, mis küsivad isikuandmeid või sisaldavad kahtlasi linke.

5. Lubage kahefaktoriline autentimine: lubage kahefaktoriline autentimine kontodel, mis seda pakuvad täiendava turvalisuse tagamiseks.

6.Kasutage turvalisi võrke: vältige avaliku WiFi kasutamist tundlike tegevuste jaoks ja kasutage vajadusel virtuaalset privaatvõrku (VPN).

7.Jälgige laste veebitegevusi: hoidke laste võrgutegevustel silm peal ja õpetage neid turvalise interneti kasutamise kohta.

8. Varundage olulised andmed: varundage regulaarselt olulisi andmeid, et kaitsta neid pahavara või riistvararikkest tingitud andmete kadumise eest.

9. Piirake isikuandmete jagamist: olge isikliku teabe jagamisel võrgus ettevaatlik ja tehke seda ainult turvalistel ja hea mainega veebisaitidel.

10. Harige ennast ja oma perekonda: olge kursis viimaste veebiohtudega ja teavitage oma perekonda turvalise Interneti-tegevuse kohta.

Co-funded by
the European Union

VIITED

Interneti-ohutuse nõuanded ja kontroll-loend, mis aitavad peredel võrgus turvalisemalt püsida. Nortoni turvakeskus. Välja otsitud aadressilt: 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 võrgus. Nortoni turvakeskus (2021) https://us.norton.com/internetsecurity-privacy-protecting-your-privacy-online.html

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

Vanemlik kontroll. Interneti küsimused (2021) https://www.internetmatters.org/parental-controls/

5 küberohutuse nõuannet, mida iga vanem peaks teadma. Nortoni turvakeskus. Välja otsitud aadressilt: https://us.norton.com/internetsecurity-kids-safety-5-cybersafety-tips-every-parent-should-know.html

Mis on veebiohud? Kaspersky (2021) Välja otsitud aadressilt: https://thebossmagazine.com/internet-safety-tips/

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

Mis on võrguohutus? Riiklik võrguohutus (2021) Laaditud aadressilt: https://nationalonlinesafety.com/wakeupwednesday/what-is-online-safety

Isikuandmete jagamise ohud sotsiaalmeedias.

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

STEGNER, Ben. (2017) Vanemliku kontrolli täielik juhend. MUO: Tehnoloogia selgitatud. Välja otsitud aadressilt: https://www.makeuseof.com/tag/guide-parental-controls/

Turvalisus võrgus: juhised vanematele ja teismelistele

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

Kuidas kaitsta oma privaatset teavet võrgus. Ühendkuningriigi Nortoni turvakeskus https://uk.norton.com/internetsecurity-how-to-8-ways-to-protect-your-private-information-online.html

Co-funded by the European Union