



TURVALINE IT

Ain Jahhu



MIKS ON VAJA ANDMEID KAITSTA?

Mis on minu jaoks oluline

- Pangaandmed
- E-kirjad ja sõnumid
- Dokumendid
- Pildid

Muudes süsteemides

- Terviseandmed
- Asukoha ja liikumise andmed
- Ostuajalugu ja -harjumused

Mis võib juhtuda kui ei kaitse?

- Spämm
- Raha läheb kaotsi
- Andmed kaovad
- Sinu nimel tehtavad tegevused
 - Spämm ja õngitused
 - Laenud
 - SINA JÄÄD SÜÜDI!
- Täpsemad õngitsused

PAROOLID

- Kasuta iga konto jaoks erinevat parooli.
- Parool võiks olla pikk, näiteks vähemalt 15 tähemärki.
- Ära kasuta paroolina nime, sünniaega, lemmiklooma nime või lihtsat sõna.
- Kasuta võimalusel paroolihaldurit.
- Lülita sisse kaheastmeline autentimine ehk 2FA.
- Ära jaga oma paroole isegi sõpradega.
- Ära sisesta paroole tundmatule veebilehele.

[RIA juhend „Kuidas muuta oma kontod turvaliseks“](#)



ÕNGITSUS, PETTUSED JA PAHAVARA

Ohumärgid

- sõnum tekitab kiireloomulisuse või hirmu;
- lubatakse auhinda või raha;
- küsitakse parooli, PIN-koodi või pangainfot;
- veebiaadress on veidi muudetud või kahtlane;
- sõnum sisaldab kirjavigu;
- saatja aadress ei vasta väidetavale ettevõttele.

ÕNGITSUS, PETTUSED JA PAHAVARA (2)

Juhised käitumiseks

- Ära klõpsa kiirustades lingile.
- Kontrolli veebiaadressi eraldi brauseris.
- Ära ava tundmatuid manuseid.
- Ära sisesta PIN-koode ega paroole lingi kaudu avanenud lehele.
- Kahtluse korral küsi nõu õpetajalt, lapsevanemalt või teenuse ametlikust klienditoest.
- Pettusest või küberintsidendist võib teatada CERT-EE-le aadressil cert@cert.ee.

[IT-vaatlik: küberturvalisuse
juhendid eraisikule](#)



ISIKUANDMED, PRIVAATSUS JA DIGITAALNE JALAJÄLG

- Mõtle enne postitamist: kas sooviksin, et seda näeksid ka õpetaja või tulevane tööandja?
- Ära jaga avalikult kodust aadressi, telefoninumbrit ega igapäevast liikumisteed.
- Kontrolli sotsiaalmeedia privaatsusseadeid.
- Küsi teiselt inimeselt enne tema foto või video avaldamist luba.
- Ära anna rakendustele rohkem õigusi, kui need vajavad.
- Vaata aeg-ajalt üle vanad postitused, jälgijad ja ühendatud rakendused.
- Ära saada internetis võõrastele dokumentide või isikut tõendavate dokumentide fotosid.

[Andmekaitse Inspeksiooni juhend](#)



SEADMETE, TARKVARA JA ÜHENDUSTE TURVALISUS

- Uuenda operatsioonisüsteemi, rakendusi ja veebilehitsejat.
- Kasuta ekraanilukku, PIN-koodi või biomeetrilist autentimist.
- Ära paigalda rakendusi tundmatutest allikatest.
- Kontrolli, milliseid õigusi rakendus küsib.
- Välgi tundlike toimingute tegemist avalikus Wi-Fi-võrgus.
- Tee olulistest failidest varukoopia.
- Ära ühenda oma seadmega tundmatuid USB-mälupulki.
- Lukusta seade, kui jätab selle järelevalveta.

[IT-vaatlik: seadmete ja tarkvara
turvalisus](#)

SUHTLEMINE, SISU JAGAMINE JA ABI OTSIMINE

[Targalt internetis õppematerjalid](#)

- Suhtle teistega samasuguse viisakusega nagu päriselus.
- Ära jaga kontrollimata infot.
- Ära levita alandavaid fotosid, videoid ega sõnumeid.
- Salvesta probleemse olukorra tõendid: kuvatõmmised, kasutajanimi ja kuupäev.
- Blokeeri ja raporteeri kiusaja või võltskonto.
- Räägi juhtunust usaldusväärse täiskasvanuga.
- Kui konto on üle võetud, muuda parool kohe ja lõpeta aktiivsed seansid.
- Ära jää probleemiga üksi.