OLE IT-VAATLIK!

ÕPI KAITSMA ENNAST JA OMA ANDMEID

RIIGI INFOSÜSTEEMI AMET

Olulisemad terminid

Login – sisselogimine, sisenemine

Logout – väljalogimine, väljumine

MFA – mitmeastmeline sisselogimine

2FA, two-factor authentication – kaheastmeline autentimine (ka kaksikautentimine)

Password – parool, salasõna

IoT (Internet of Things) – asjade internet

Update – värskendamine

Backup – varukoopia loomine

Accept – aktsepteerimine, nõustumine

Cancel – tühistamine

Settings – sätted, häälestamine

Phishing – andmepüük

Malware – pahavara

Ransomware – lunavara

Firewall – tulemüür

Encryption – krüpteerimine

VPN (Virtual Private Network) – virtuaalne privaatvõrk

Spyware – nuhkvara

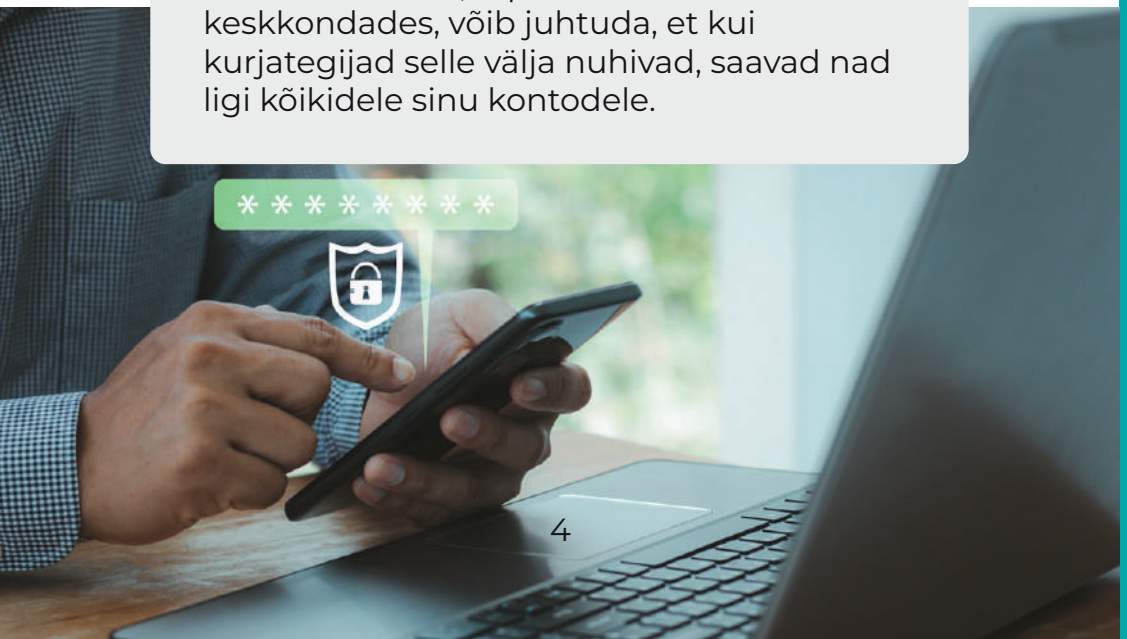
Social engineering – sotsiaalne manipuleerimine

Sisukord

1. Kasuta tugevaid unikaalseid paroole ja kaheastmelist autentimist

Paroolid on kasutusel selleks, et kaitsta sinu andmeid.

Kasutades ühte ja sama nõrka parooli sotsiaalmeedias, e-posti kontol või töö-keskkondades, võib juhtuda, et kui kurjategijad selle välja nuhivad, saavad nad ligi kõikidele sinu kontodele.



Pea meeles!

1. Kasuta erinevat parooli oma e-posti, sotsiaalmeedia ja töökonto jaoks.
2. **Tugeva parooli pikkus on vähemalt 12 tähemärki ning parool sisaldab nii suuri kui väikseid tähti, numbreid ja erimärke.**
3. Kasuta ka kaheastmelist sisselogimist kõikjal, kus võimalik, sest see pakub lisaks tugevale paroolile ühe lisakihi turvalisust.
4. Kuidas see aktiveerida? Enamikel platvormidel, nagu näiteks Facebook või Gmail, tuleb sul minna paremal ülemisse nurka, kus saad vaadata kontoseadeid. Vali sealt turvaseaded ning otsi üles kaheastmeline autentimine.
5. Vali endale sobiv meetod, näiteks SMS, seejärel sisesta oma telefoninumber ning kinnita oma number vastavalt juhistele.
6. Alternatiivina võid kasutada turvakoodide jaoks eraldi äppi.

2. Uuenda tarkvara erinevates seadmetes

Selleks, et oma seadmeid ja andmeid kaitsta, tuleb tarkvara pidevalt uuendada.

Uuendamata tarkvaraga arvuti või nutitelefon on küberkurjategijatele ahvatlevaks sihtmärgiks.

Turvaauke ära kasutades on võimalik seade pahavaraga nakatada ning jälgida kasutaja toiminguid, salvestada salasõnu või pääseda ligi teistele andmetele.

Pea meeles!

1. Enamasti on uuendamine tehtud nii lihtsaks, et ei nõua sinult suuremat pingutust kui paar hiireklikki.
Kui nutiseade või arvuti pakub uuendust, siis võta väike paus ja lase arvutil seda teha.
2. **Uuenda alati kõigis seadmes kõiki rakendusi.**
3. Aeg-ajalt vaata oma seadmesse paigaldatud rakendused kriitilise pilguga üle ning eemalda need, mida sa enam ei kasuta.

3. Suhtu ettevaatusega tundmatutesse linkidesse

Õpi ära tundma linke ja faile, mis võivad osutuda ohtlikuks.

Eelkõige pead teadma, et kahtlane link võib saabuda tuttavast kohast. Näiteks mõnelt ettevõttelt SMSi teel, sõbralt e-maili kaudu ja pereliikmelt Messengeri, WhatsAppi või mõne muu levinud suhtlusrakenduse teel.

Enamasti kutsub lingi juures olev tekst lingile klikkima ning sisestama oma panga-kaardiandmeid, paroole või paigaldama arvutisse pahavara.

Pea meeles!

1. **Ole umbusklik ja ära ava oma arvutis tundmatu kirjaga kaasa tulnud faile.**
2. Kui e-postis või SMS-is on link kuhugi sisenemiseks, ära kliki, vaid leia vajalik veebilehekülg ise otsimootorist. Kahtluse korral võid helistada kliendi-teenindusele.
3. Kui link saabub mõnelt tuttavalt inimeselt, kuid tavaliselt ta sellised asju ei saada, küsi mõnes muus kanalis temalt üle, millega tegu. Näiteks helista, sest tema konto võib olla kaaperdatud.
4. Kui juhtud siiski klikkima, ära sisesta kuskile tundlikku informatsiooni ega luba midagi paigaldada või alla laadida.

4. Vaata üle sotsiaalmeedia turvasätted

Pea meeles, et sotsiaalmeedias on vaikimisi kõik avalik.

Isegi kui postitamisest saadav vahetu emotsioon on tore, **kaob sul kontroll selle üle, kes su sisu näevad ja mida nad sellega peale hakkavad.**

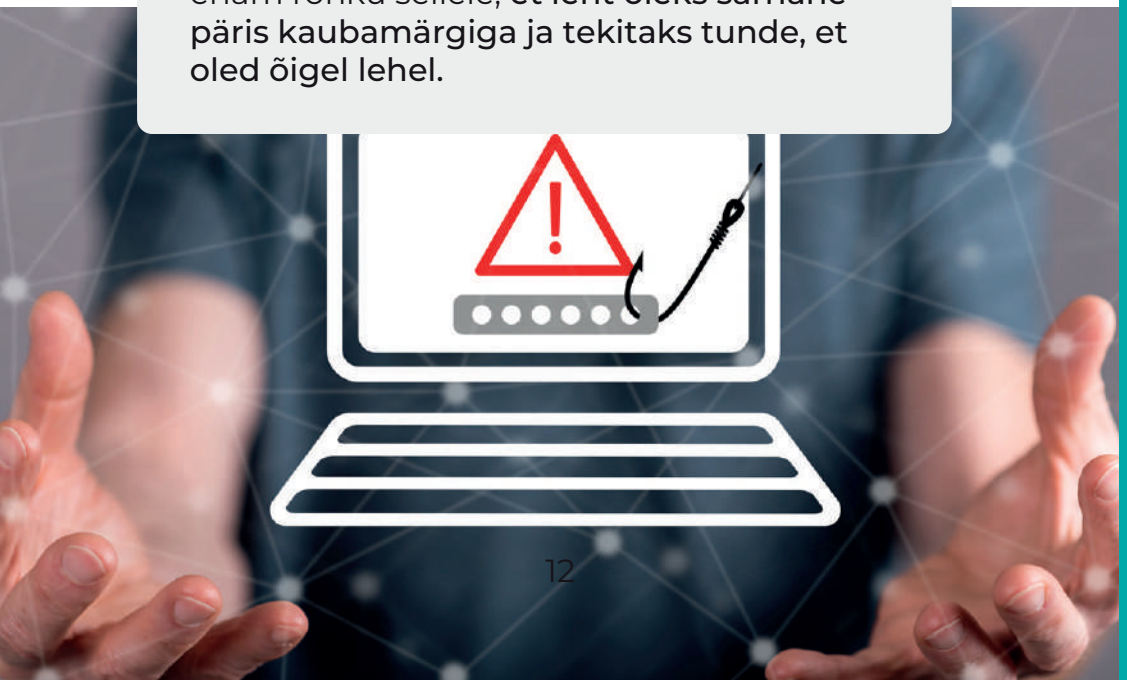
Pea meeles!

1. Kasuta sotsiaalmeedias kaheastmelist autentimist ja unikaalset salasõna.
2. **Piira, kes su postitusi näevad ja kes neid edasi saavad jagada.**
3. Võta sõpradeks ainult neid, keda päriselt tunned
4. Ära ava tundmatu päritoluga linke

5. Õpi ära tundma õngitsuslehti

Õngitsuslehtede eesmärk on varastada sinu kontode või krediitkaardi andmeid.

Õngitsuslehtede loomisel pannakse kõige enam rõhku sellele, **et leht oleks sarnane päris kaubamärgiga ja tekitaks tunde, et oled õigel lehel.**



Pea meeles!

1. Enne kui oma andmeid sisestama tõttad, veendu, et veebilehe aadress, millel oled, on täht-tähelt seesama, mis peaks olema (google.com vs g00gle.com).

2. Kui oled õnnetul kombel oma kasutajainfo õngitsuslehele sisestanud:

   - **vaheta kohe oma konto parool**
   - logi välja kõikidest seadmetest, kust on kasutajakontole sisse logitud.
   - veendu, et sul on aktiveeritud kaheastmeline autentimine.

6. Tee oma andmetest tagavarakoopiad

Võib juhtuda, et arvuti läheb katki, kaob ära või nakatub viirusega, mis muudab sinu tähtsad failid, näiteks perepildid ja videod, kasutuskõlbmatuks.

Ainus lihtne soovitus oma andmete kaitsmiseks on **tagavarakoopia**.

Andmeid on nimelt võimalik varundada. See tähendab, et saad oma dokumentidest või piltidest üsna lihtsasti teha varukoopiaid.

Pea meeles!

Andmete varundamiseks on kaks levinud võimalust.

1. **Üks võimalus on kõik tähtis kopeerida välisele andmekandjale. Näiteks mälupulgale või kõvakettale.**
2. Teine võimalus on varundada pilveteenusesse, mis automaatselt sinu faile varundavad
3. Tihti pakuvad pilveteenused ka tasuta salvestusruumi (näiteks Google Drive, Microsoft OneDrive jne).
4. Varunda kindlasti regulaarselt ja veendu, et kõik toimib.

7. Vaheta ära seadmete tehaseparoolid

Tänapäeval on väga levinud internetti ühendatud tolmuimejad, kellad, muruniidukid, printerid, telekad ja hulk muid nutikaid seadmeid.

Kõik need seadmed on internetti ühendatud ruuteri abil.

Kui sinu kodune ruuter kasutab tehaseparooli, võib mõni kurikael selle üle võtta ja printida välja tuhandeid kassipilte või panna sinu teleri suvalisel hetkel mängima ja häirida sellega sinu öörahu.

Halvemal juhul võib märkamatult sinu ruuterist ja sellega ühendatud seadmetest saada aga relv, millega rünnata kooli või kohalikku haiglat.

Pea meeles!

1. **Oluline on ära muuta ruuteri tehaseparool ja vaadata üle muud turvaseaded.**
2. Samuti on iga uue seadme puhul oluline kohe alguses üle vaadata turvasätted ja tehaseparoolid.
3. Kuidas seda teha? Selle info leiad seadme manuaalist. Kui manuaali kaasas ei ole, otsi internetist seadme nime ja mudeli järgi.

8. Õpi ära tundma petukõnesid

Erinevad petukõned on väga levinud, näiteks esitlevad petturid end politsei, panga või kullerteenuse pakkujana.

Enamasti on petturite eesmärk **varastada sinu kontode või krediitkaardi andmeid**.

Pea meeles!

1. **Panga- ja politseiametnikud sinu andmeid telefoni teel ei küsi.** Samuti ära võta vastu pakkumist teha tehinguid sinu eest ja siseneda mõne programmi abil üle võrgu sinu arvutisse.
2. Kahtluse korral katkesta kõne.
3. Sinu ID-kaardi PIN-koodid on kasutamiseks ainult sinule.

BCS Koolitus

Küberintsidendist teavita
cert@cert.ee

Vaata rohkem
www.itvaatlik.ee