# KÜBEROHUD VÄIKEETTEVÕTJATELE

***Mis on päriselt oluline – ja miks lihtsalt ettevaatusest enam ei piisa?***

## Sissejuhatus: Kas sina oled liiga väike, et olla sihtmärk?

Kui sa oled väikeettevõtja, oled sa arvatavasti ettevõtte juht, turundaja, müügijuht ja raamatupidaja ühes isikus. Sa ise oled oma klientidele klienditugi, võib-olla oled ainus töötaja (või üks vähestest). Ja kõigele lisaks oled sa tehnika seadistaja-parandaja: printer, arvuti, telefon, ja kõiksugu muu kontori ja ettevõtlusega seonduvad vidinad. Seda on palju.

Arusaadavalt läheb sinu aeg ja energia sinna, kus on kliendid, raha ja igapäevased tulekahjud. See tähendab, et küber- ehk digiturvalisus jääb enamasti tähelepanuta või tahaplaanile. Sul pole tõenäoliselt väga palju aega mõelda paroolipoliitika või andmelekete peale. Ja seegi on täiesti arusaadav. Mitte sellepärast, et see poleks tähtis, vaid sellepärast et see tundub ebamäärane, tehniline, ja natuke liiga kauge. Võib-olla isegi midagi mustkunsti laadset. Ja võib-olla sa arvad et „Mul pole ju midagi nii olulist, mida keegi tahaks varastada.“

Siin tuleb mängu üks suur ja levinud müüt:

> “Minu ettevõte on nii väike, et mind see ei puuduta.”

Tegelikult on just mikro, väikesed ja keskmised ettevõtted kõige lihtsam saak küberkurjategijatele. Ja seda mitte sellepärast, et nad oleksid rumalad, vaid sellepärast, et nad ei mõtle reeglina üldse küberturvalisusele ja nad ei ole võimalikeks ohtudeks lihtsalt valmis. Neil ei ole IT-osakonda, kes jälgiks logisid või kontrolliks ligipääse, neil ei ole loodud varunduspoliitikat või kriisireageerimisplaani. Ja päris tihti juhtub, et keegi ei tea täpselt, kes millele ligi pääseb või milliseid keskkondi ja kontosid üldse kasutatakse.

### Statistika räägib enda eest

- Euroopas on küberrünnakute sihtmärgiks langenud üle 50% väikese ja keskmise suurusega ettevõtetest (ENISA, 2023).

- Eestis läbiviidud uuringu järgi ei ole ligikaudu 70% mikroettevõtetest mitte kunagi teinud küberturvalisuse riskianalüüsi (RIA, 2022).

- Vähem kui kolmandik väikestest ettevõtetest kasutab kaheastmelist autentimist, kuigi see on tegelikult väga tõhusamaid kaitsemeede.

- Aastal 2021 Eestis registreeritud andmeleketest ligi 40% puudutasid väikeettevõtteid, sageli nende endi teadmata.

### Elulised näited

- **Väike e-pood** kaotas 4000 € pärast seda, kui nende PayPali konto kaaperdati – parool oli „firma2020“ ja 2FA puudus. Nad ei saanud oma raha kunagi tagasi, PayPal konto tagasi saamisega läks palju aega.
- **Väike põllumajandusettevõte** kaotas kogu oma kliendisuhtluse, klientide nimekirja, raamatupidamise ja palju muud, kui nende Gmaili konto kaaperdati. Nad ei saanud kunagi oma andmeid tagasi ja pidid kõike nullist alustama.
- **Koolitusteenuse pakkuja** ei teadnud, et Google Drive'is olev kliendinimekiri oli kogemata “avalik kõigile” lingiga. Leke avastati alles pärast seda, kui üks klient mainis, et leidis guugeldades enda nime. Tekkis mainekahju.
- **Ehitusvaldkonnas tegutsev mikroettevõte** sai petukirja väidetavalt koostööpartnerilt, kus paluti kiiret ettemakset summas 2390 EUR uuele kontole. Ettevõte kandis raha üle. Ja alles pärast üle helistamist selgus, et tegemist oli petuskeemiga. Raha tagasi ei saadud.

Sellised väikesed asjad teevadki väikeettevõtted haavatavaks. Keegi ei sihtinud just neid konkreetseid ettevõtteid, vaid need rünnakud said toimuda tänu kurjategijatel olemas olevatele (või väga kergelt soetatavatele) vahenditele mis aitavad neil vähese vaevaga läbi viia massilisi ja automatiseeritud rünnakuid. Suurt osa ründeid tehaksegi automatiseeritult, võib isegi öelda et neid teevad robotid. Ja robotid ei vali ohvreid nimepidi - nad otsivad uksi, mis on lukust lahti või natuke paokil. Ja kahjuks on just väiksemate ettevõtete digitaalsed uksed sageli lukustamata või natuke lahti. Ja tihti  lihtsalt sellepärast, et kellelgi polnud aega neid sulgeda. Või see keegi lükkas sulgemist pidevalt edasi.

Sellised asjad ei tee sind halvaks ettevõtjaks. Need teevad sind inimeseks, kellel on palju rolle ja kelle tähelepanu on jagatud kümne erineva suuna vahel. Loodetavasti just selle pärast loed sa praegu seda raamatut. Loodetavasti on sul piisavalt teadlikkust, et küsida küsimusi ja piisavalt tahtmist, et otsida vastuseid.

See ei ole tehniline käsiraamat. See ei ole ka müügipakkumine. See on kerge lugemine, selge ja aus sissevaade sellesse, kus võivad sinu digitaalsed nõrkused päriselt peituda, ja isegi siis, kui kõik tundub korras olevat.

Kui oled valmis ausaks sisse vaatamiseks oma ettevõtte turvapeeglisse, siis loe edasi. Sest päriselt turvaline ettevõte ei alga keerukatest tehnilistest lahendustest, vaid eelkõige teadlikkusest ja väga lihtsatest sammudest.

# 1. peatükk: 7 levinud müüti, mis võivad su ettevõtte ohtu seada

Küberrünnakud ei alga alati tehnoloogiast, seadmete vastu suunatud rünnetest või keerulistest häkkimistest. Väga sageli algavad need millestki palju lihtsamast – valedest uskumustest. Paljud inimesed ja ettevõtted arvavad et „kes küll mind peaks ründama“, „ma pole üldse tähtis”, „mu ettevõte on nii väike” või „mul ei ole mingit tundlikku informatsiooni“.

Need uskumused tunduvad loogilised. Mõned neist põhinevad varasematel kogemustel („meil pole kunagi midagi juhtunud”) või lihtsalt igapäevatöös kujunenud harjumusel. Aga just sellised uskumused on põhjuseks, miks väikesed ettevõtted sageli haavatavad on. Ja see on ka põhjuseks, miks nad ei märka ohtu enne, kui on juba hilja.

Selles peatükis vaatame lähemalt seitset kõige levinumat mõttemustrit, mida olen oma töös väikeettevõtjatega korduvalt kuulnud. Ma ei räägi seda sõrmega näitamiseks. Need müüdid kahjuks levivad - mitte rumalusest, vaid selle pärast et need tunduvad loogilised, inimlikud ja mõistlikud.

Kahjuks on need müüdid kübermaailmas täiesti valed. Kui mõni neist kõlab tuttavalt, siis tea: sa ei ole üksi, ja nii arvab enamus inimesi ja ettevõtteid (kuni nendega midagi juhtub). Aga võib-olla on just nüüd õige aeg neid müüte enda peas murda, et hakata mõtlema mida saab teha enne kui midagi päriselt juhtub.

Vaatame lähemalt.

## 1. *“Mul ei ole tundlikke andmeid.”*

See on ilmselt kõige levinum uskumus, mida väiksemate ettevõtete juhtidelt võib kuulda. „Ma ei kogu isikuandmeid ega krediitkaardinumbreid - mis mõttes mul oleks midagi tundlikku?“

Aga vaata asjale veidi teise nurga alt:

- Kas sul on klientide nimed, e-posti aadressid ja telefoninumbrid?
- Kas sa koostad neile hinnapakkumisi, arveid, lepinguid?
- Kas su arvutis või pilves on nende aadress, ostuajalugu või erisoovid?
- Kas sul on ligipääs äripartnerite või koostöövõrgustike kontaktidele?

Kui vastasid vähemalt ühele küsimusele „jah“, siis pead tunnistama: SUL ON TUNDLIKKE ANDMEID.

Need ei pruugi olla „kõrge riskiga“ delikaatsed andmed seaduse mõttes (nt terviseandmed),

aga need on siiski väärtuslikud – nii sulle kui potentsiaalsele ründajale. Ja eriti sulle endale. Kui sina need kaotad, jääb su äri seisma. Andmed ei pea olema seaduse silmis tundlikud või

delikaatsed andmed. Aga kui sa neid kogud, töötled või salvestad (isegi kui teed seda ajutiselt) pead sa neid ka kaitsma.

Miks on need andmed väärtuslikud kurjategijatele?

Klientide andmeid saab kasutada petukirjade saatmiseks nende nimel. Ligipääs e-postile või failidele annab ründajale võimaluse jäljendada sind**.** Ja seeläbi küsida raha, muuta saadetaval arvel sinu pangaarve andmeid, levitada valeinfot, võtta üle sinu ettevõtte veebileht, või esineda sinu nimel sotsiaalmeedias.

## 2. *“Ma kasutan ainult turvalisi teenuseid.”*

See on ilmselt paljude inimeste jaoks rahustav mõte. Mõtleme „Mu e-post on Gmailis, failid Google Drive’is, raamatupidamine pilves / need on ju turvalised.“ Ja see ongi osaliselt tõsi. Google ja teised suured teenusepakkujad kulutavad miljoneid, et tagada oma teenuste turvalisus. Seda teevad ka väiksemad teenuspakkujad, näiteks raamatupidamisprogrammid. Aga see ei tähenda, et *sinu konto* oleks turvaline. Teenus on suure tõenäosusega igati turvatud. Aga kui sina ise kasutad sama parooli mitmes kohas, kaheastmeline autentimine pole sisse lülitatud, seadmel pole ekraanilukku või parooli, või jagad oma parooli kolleegi, assistendi või pereliikmega, teed end ise haavatavaks. Ja kui sinu konto kaudu saadetakse petukiri või sinu draivist lekivad andmed, ei süüdista ohver Googlet.

## 3. *“Ma pole kunagi midagi kaotanud, või: minuga pole kunagi midagi juhtunud.”*

See, et siiani ei ole midagi juhtunud, ei tähenda, et mitte midagi mitte kunagi ei juhtu. Rünnakud on automatiseeritud. Kurjategijad ei vali sihtmärke käsitsi. Tihtilugu ei saa ohver isegi aru, et keegi on tema kontole sisse pääsenud. Või on keegi juba faili jaganud, ja ohver seda ei teagi. Või kasutab keegi kusagil sinu nime, ja sa veel ei tea. See et siiani pole midagi juhtunud, ei tähenda et seda lähiajal ei juhtu. Eriti arvestades et kurjategijad ei vali oma ohvreid käsitsi, vaid otsivad lihtsalt nõrkusi. Ja nad ei saa vaadata, et „sellest inimesest on kahju, teda ma ei ründa”.

## 4. *“Ma ei usu, et keegi mind sihib.”*

Põhimõtteliselt on see õige. Enamasti ei sihigi keegi sind isiklikult. Aga sa lihtsalt satud suurde võrku, mis otsib ohvreid automaatselt. Sind sihib robot, paljude teiste sihtmärkide hulgas. Suuremas osas toimuvad küberrünnakud automaatselt. Kurjategijatel on tööriistad, mis skännivad sadu tuhandeid veebilehti, kontosid ja seadmeid samaaegselt. Need tööriistad otsivad nõrku paroole, uuendamata tarkvara, turvaauke, jagatud faile, ja isegi kasutajanimesid, domeeninimesid ja muud sellist. Ja sinu e-post võib saada osaks kellegi petuskeemist ilma et sa midagi isegi tähele paneksid. See pole isiklik. Ja kui kaitse puudub, võid sattuda küberkurjategija ohvriks.

## 5. *“Meil on väike ettevõte ja ma ei usu et keegi eksib.”*

Väikestes ettevõtetes kasutavad erinevad inimesed tihti samu sisselogimisandmeid, jagatakse paroole omavahel ja e-posti teel. Enamasti ei mõelda sellele mis võib juhtuda,

vaid seda tehakse lihtsalt mugavusest või kiire tegutsemise eesmärgil, et äri toimiks. Aga sellised väikesed mugavusest tulenevad seaded võivad põhjustada kahju, mille hind on äri seiskumine lühemaks või pikemaks ajaks. Rääkimata võimalikust rahalisest või mainekahjust.

### 6. *“Ma ei tunne kedagi, keda oleks rünnatud.”*

Kindlasti tunned, isegi kui keegi sellest ei räägi. Sellest ei taheta rääkida, sest see tundub piinlik. Ohvreid enamasti naeruvääristatakse, ja küsitakse kuidas sai keegi nii rumal olla. Või siis jääb märkamatuks et üldse midagi pahatahtlikku on juhtunud ja arvatakse et tegemist oli hoopis tehnilise veaga. Eestis meil head ja täpset statistikat pole, kuid Euroopas ja mujal maailmas on seda rohkem uuritud. Erinevate uuringute järgi on umbes 70% väiksematest ettevõtetest langenud küberrünnakute ohvriks. Ja pole mingit põhjust arvata, et Eestis oleks olukord sellest erinev. Edukaid (aga ka edutuid) rünnakuid toimub rohkem kui oskame arvata**.**

### 7. *“Mul on viirusetõrje ja sellest piisab.”*

Viirusetõrje on nagu lukk välisuksel. Aga kui aken on lahti, ei ole lukust alati kasu. Ohuks ei ole ainult pahavara (mille vastu suuremas osas aitab tõesti viirustõrje), vaid ohud tulenevad ka näiteks avaliku WiFi kasutamisest, korduvatest salasõnadest, uuenduste edasi lükkamisest ja paljust muust. Veel kasutatakse ära inimpsühholoogiat (sotsiaalne manipuleerimine, identiteedivargus, ja õngitsuskirjad või SMS-d. Viirusetõrje on ainult üks osa turvalisusest. Lisaks peab veel tegelema paroolide, varunduse, uuenduste ja teadliku käitumisega. Ilma teadlikkuse ja harjumusteta ei ole ainult viirustõrje täna enam piisav.

## Lühike kokkuvõte:

Kui sa tundsid ära mõne enda mõtte – siis see raamat on sulle.
Aga ära muretse – teadlikkus on esimene ja kõige tähtsam samm, mida käesoleva raamatuga püüame ka saavutada.

## 2. peatükk: Mis tegelikult juhtub, kui midagi läheb valesti

Küberrünnak ei alga nagu filmis. Arvuti või telefon ei anna häiret. Ekraanile ei ilmu suured tähed „HÄKITUD”. Tegelikkuses toimub kõik palju vaiksemalt, mis teeb ka küberründed palju ohtlikumaks. Sa ei märka kohe, et midagi on juhtunud. Aga mõni tund peale kahtlases e-mailis olnud lingile vajutamist võib keegi juba olla sinu kontole sisse loginud, mõni päev pärast faili jagamist (õigele inimesele) võib selle seadete tõttu link liikuda valesse kohta. Või mõne vana parooli taaskasutusele võtmisel (isegi kui see on väga turvaline) võib keegi automaatse skännimisega vanade lekkinud paroolide andmebaasi kasutades saada ligi sinu uuele kontole. Tihti võib juhtuda, et märkad midagi alles siis, kui keegi teine sulle midagi

ütleb. Näiteks, et su saadetud Google Drive link ei tööta ja näitab mingit veidrat lehte. Või küsib, miks mingi imeliku kirja saatsid. Või küsib, miks su pangaarve andmed on muutunud.

Allpool on mõned päriselulised olukorrad, mis on juhtunud mikro- ja väikeettevõtetega. Nad ei olnud hooletud – nad lihtsalt ei teadnud, mida nad ei teadnud.

## Näide 1: “Meie klient sai minu nimelt vale arve.”

Mari on väikese disainiagentuuri omanik. Ta saatis tavapärase kuu lõpu arve kliendile. Mõni päev hiljem kirjutas klient:

> “Miks te oma panka vahetasite? Kas see uus pangakonto on nüüd teie oma?”

Mari ei olnud midagi muutnud. Aga keegi oli saanud ligipääsu tema meilikontole, ootas sobivat hetke ja asendas arvesüsteemis pangakonto andmed ja IBAN-i. Klient maksis arve õigel ajal ära aga raha läks ründajale. Mari jäi rahast ilma ja pidi seletama, kuidas see juhtus.

**Miks see juhtus?**

- Parool oli vana ja kasutusel ka mujal.
- Kaheastmeline tuvastus puudus.
- Rünnak oli aeglane, sihitud ja suunatud, mitte massiline.

## Näide 2: “Google Drive’i kaust lekkis kogemata kõigile.”

OÜ Pilvex kasutas Google Drive’i pakkumiste ja lepingute salvestamiseks. Nad jagasid tiimis lingi kaudu kaustu: *“Anyone with the link can view”*. Üks töötaja jagas kogemata selle lingi avalikku foorumisse ja linki nägi sadu inimesi.

Mõni nädal hiljem ilmus ühe kliendi pakkumine konkurendi hinnakirjas. Juhus?

**Kus oli nõrkus?**

- Jagamisõigused olid kontrollimata.
- Ei olnud ülevaadet, kes millele ligi pääseb.
- Töötajad ei teadnud, kuidas jagada turvaliselt.

## Näide 3: “Töötaja telefon läks kaduma, koos sellega ka ettevõtte postkast”

Mikroettevõttes “Raamat & Ruum” kasutas raamatupidaja oma isiklikku telefoni ka töömeiliks. Telefon jäi kohvikusse. Ekraanilukku polnud. Meilikontole pääses ligi igaüks, kes telefoni oma kätte sai. Ja keegi pääseski. Mis edasi sai? E-postilt saadeti pahatahtlik kiri koostööpartnerile, See kiri sisaldas pahavaraga linki, mille kaudu üritati varastada sisselogimisandmeid.

**Miks see polnud lihtsalt “ups”?**

- Isiklikud seadmed ei olnud kaitstud elementaarsete seadetega.
- Ettevõttes polnud juhiseid, mida teha, kui seade kaob. Ja inimene ei teinud mitte midagi.

## Mida need lood näitavad?

- Küberintsident ei pea olema “häkkimine” – piisab inimlikust eksimusest.
- Väike ettevõte olemine ei tähenda et võimalikul ründel on väike mõju. Raha, usaldus ja maine on ikkagi löögi all.
- Tihti ei saa sa isegi aru, et midagi on juhtunud enne kui kahju on käes.

## Tee väike enesetest: kas sul on…

- Eri tasemega ligipääsud failidele?
- Reeglid tööseadmete ja isiklike seadmete kasutuseks?
- Reeglid töökontode ja isiklike kontode kasutuseks?
- Plaan, mida teha, kui klient ütleb “midagi on valesti”?

Kui vastasid vähemalt ühe korra „ei“ – siis oled täpselt õigel ajal õigel lehel. Reeglid ei tähenda midagi suurt ja bürokraatlikku. Aga reeglid peavad olema läbi mõeldud, lihtsad ja rakendatavad.

# 3. peatükk: Millised on sinu digitaalsed nõrkused?

*Digitaalsed nõrkused ei tähenda "IT-spetsialisti puudumist". See tähendab lihtsat: kus võivad tekkida ootamatud haavatavused ja turvaaugud.*

Enamik mikro- ja väikeettevõtteid ei ole meelega hooletud. Nad lihtsalt *ei tea*, millised kohad on kõige haavatavamad. Nad teevad seda, mida enamus inimesi: usaldavad, et kõik „lihtsalt töötab“.

See peatükk aitab sul näha oma hetkeolukorda. Vaatame praegust olukorda mitte testina, vaid *päriseluliste küsimustena*, millele on raske otsesõnu vastata „jah“ või „ei“. Ja just see ongi mõte.

## 1. Kes omab kontrolli sinu digivara üle?

- Kas kõik su kontod on loodud sinu nimele, või on mõni teenusepakkuja kunagi loonud su eest “ajutise” meilikonto?
- Kas keegi teine (nt töötaja, partner, arendaja) võib veel pääseda mõnele kontole, mida sa pole ammu kontrollinud?
- Kui sina homme puhkusele lähed, kas keegi teine pääseb ligi sellele, millele peaks?

## 2. Kuhu su ettevõtte andmed „elama“ on jäänud?

- Kas kasutad mitut pilveteenust korraga (nt Google Drive, Dropbox, iCloud)? Kas tead, mis ja kus on?
- Kas dokumente on jagatud „lingiga kõigile“ lihtsalt mugavuse pärast?
- Kas mõni vana fail (nt klientide andmed või hinnapakkumised) on avatud ligipääsuga netis, kuigi sina arvad, et see on kustutatud?

## 3. Kuidas liiguvad paroolid ja ligipääsud?

- Kas paroolid liiguvad meili või messengeri kaudu?
- Kas keegi teine teab mõnda sinu töömeilide või sotsiaalmeedia parooli?
- Kas mõni endine töötaja võiks teoreetiliselt veel pääseda kuskile, kuhu sa ei tea et ta sisse või ligi pääseb?

## 4. Kui seadmega juhtub midagi, mis juhtub sinu äriga?

- Mis juhtub, kui su arvuti või telefon kaob või kukub vette? Kas seal oli meilikonto? Facebook? Google Authenticator?
- Kas kõik su failid ja kontaktid on salvestatud ainult arvutisse?
- Kui homme peaksid oma sülearvutist või telefonist ilma jääma, mitu päeva su töö seisaks?

### 5. Kui keegi „teeks sinu nime alt midagi“, kuidas sa seda teada saaksid?

- Kui keegi saadaks sinu nimel vale arve või petukirja, kas keegi annaks sulle teada?
- Kas su kliendid usaldavad su brändi nii palju, et ei kahtlusta midagi?
- Kas sul on harjumus aeg-ajalt kontrollida: mida sinu ettevõtte kohta leida saab?

## Peegeldus, mitte süüdistus

Need küsimused ei ole mõeldud selleks, et sind süüdistada. Need on mõeldud selleks, et sul tekiks teadlikkus. Sest kõige suurem risk ei ole pahatahtlik ründaja vaid teadmatus ja sellest tulenev hooletus. Kui need küsimused panevad sind korraks mõtlema, siis on see hea.

## Mis edasi?

Kui sa soovid:

- viia oma ettevõtte turvalisuse **käegakatsutava tasemeni** (mitte ainult mõttetasandile),
- saada **töölehti, plakateid, tegevusplaane** ja juhiseid,
- õppida, **kuidas reageerida küberintsidendile**,

siis järgmine samm on:

**Küberkindel äri” raamatu täisversioon: praktiline juhend ja tööriistad väikeettevõtjale.** Koos kontrollnimekirjade, kriisijuhendi ja isetäidetavate töölehtedega.

Vaata lähemalt ja osta: www.sinuleht.ee/kuberraamat

## Lõppsõna: Turvalisus algab ausast pilgust praegusele olukorrale

Kui sa oled selle raamatu lõpuni lugenud, siis oled juba teinud esimese ja kõige olulisema sammu. Sa oled suurendanud oma teadlikkust, et päriselt küberturvaline ettevõte ei teki niisama lihtsalt. Turvalisus ei ole mingi tehniline üllatus, mis ilmub siis, kui palgata IT-inimene. See on igapäevaste väikeste otsuste kogum, mida teed sina, ja mille mõjusid koged samuti sina.

Ja kuigi kõik see võib tunduda esmapilgul veidi ehmatav, siis tegelikult on sõnum lihtne:

> **Sa ei pea kõike oskama. Sa pead lihtsalt teadma, kus on su riskid ja olema valmis nendega midagi ette võtma.**

# “Aga mida ma nüüd tegema pean?”

Kui see küsimus juba tekkis, siis suurepärane. Sest järgmine samm ongi TEGEMINE.

Kui soovid:

✅ kontrollnimekirju ja töölehti,
✅ küberintsidendi esmaabi juhendit,
✅ lihtsat kriisiplaani ja meeskonnaga jagatavaid visuaale,
✅ samm-sammulisi juhiseid, kuidas oma ettevõtet päriselt turvalisemaks muuta

…siis oled oodatud lugema täisversiooni:

📘 **“KÜBERKINDEL ÄRI”**
*Kuidas kaitsta oma ettevõtet ilma IT-osakonnata.*

🧰 Sisaldab tööriistu, juhiseid ja palju elulisi näiteid.

👉 Laadi alla siit või hoia silma peal uutel osadel: www.sinuleht.ee/kuberraamat

## Meelespea:

**Iga väike samm loeb.**
Sa ei pea kõike tegema korraga. Aga sa pead alustama. Ja kui alustad täna, oled homme juba turvalisem.

Kohtume järgmises peatükis,
**[Sinu nimi]**
*küberturvalisuse koolitaja & mikroettevõtjate kaaslane*