

HYÖKKÄYKSEN ANATOMIA

Antti Laatikainen, Johtava konsultti

WithSecure Consulting

W / T H
secure

ÄLÄ HÄTÄILE

Valmistautumalla näistä selviää

Hyökkäyksen anatomia

Erään murren tarina

Puolustuksen työkalut

Arkipäivän vinkit



Miksi tietoturva on tärkeää?

Rahaa, henkilöllisyys,
arkaluontoista tietoa

- - Rikollinen tavoittelee kaikkea rahanarvoista.

Nettiyhteys tai
tietokoneesi

- - Nettiyhteyttäsi tai laitteitasi käytetään rikolliseen toimintaan.

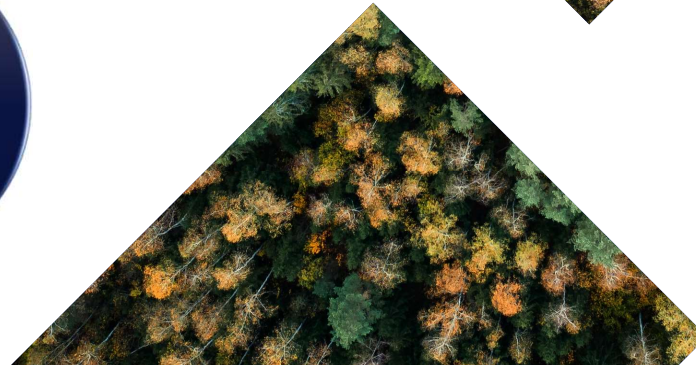
Maine

- - Nimelläsi tehtäillut rikokset ja vahingonteot ovat kiusallisia ja haitallisia.

Identiteettivarkauksien jälkien korjaaminen on työlästä ja kallista.
Kaikkea varastettua ei välttämättä saa koskaan takaisin.

Yritysmaailmassa riskit

“Riski = epävarmuuden vaikutus tavoitteisiin” - ISO 31000



Hyökkäyksen anatomia

Jokainen joka haluaa vaikuttaa tietojärjestelmiin, salakuunnella liikennettä tai kaapata laitteita, käyttää samoja tekniikoita kuin puolustajat.

Loppujen lopuksi kyseessä on lasten “lipunryöstö”.

VOITTAAKSESI PELIN SINUN TARVITSEE TIETÄÄ

- ✓ Missä lippu on.
- ✓ Miten sen luo pääsee.
- ✓ Miten vältellä puolustajia.
- ✓ Miten päästä lipun kanssa karkuun.



Hyökkäys on palapeli

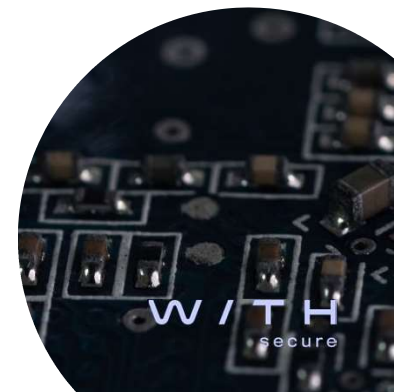
Tiedusteluvaiheessa kaikki tieto on hyvää tietoa.

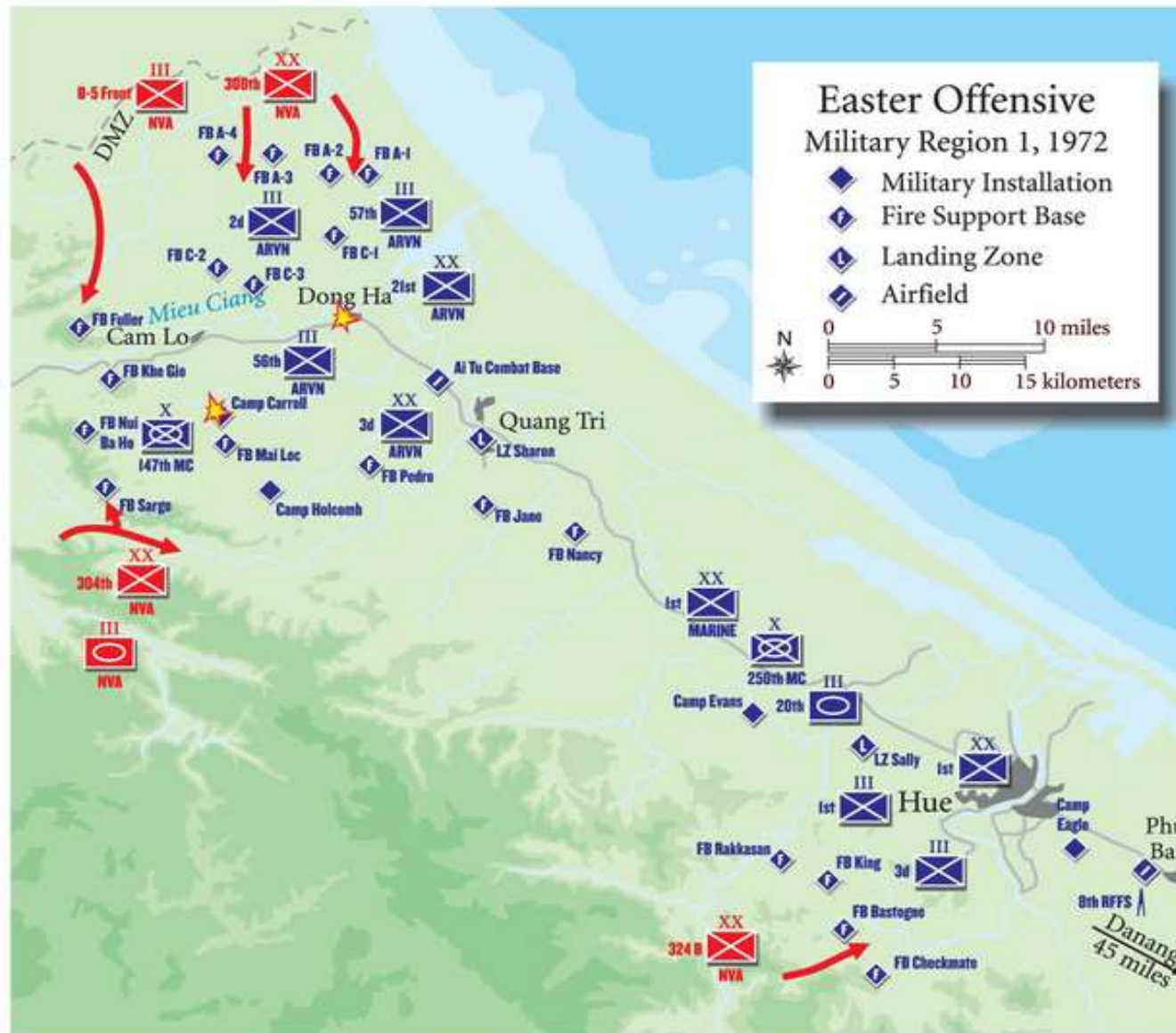
Murto on yleensä nopea, hyvin suunniteltu ja pistemäinen.

Sisäinen levittäytyminen tehdään harkiten ja mahdollisimman hiljaa.

Todellinen vahinko tehdään kun maalit on tunnistettu ja ajoitus oikea.

Mahdollisuuksien mukaan jäljet pyyhitään.



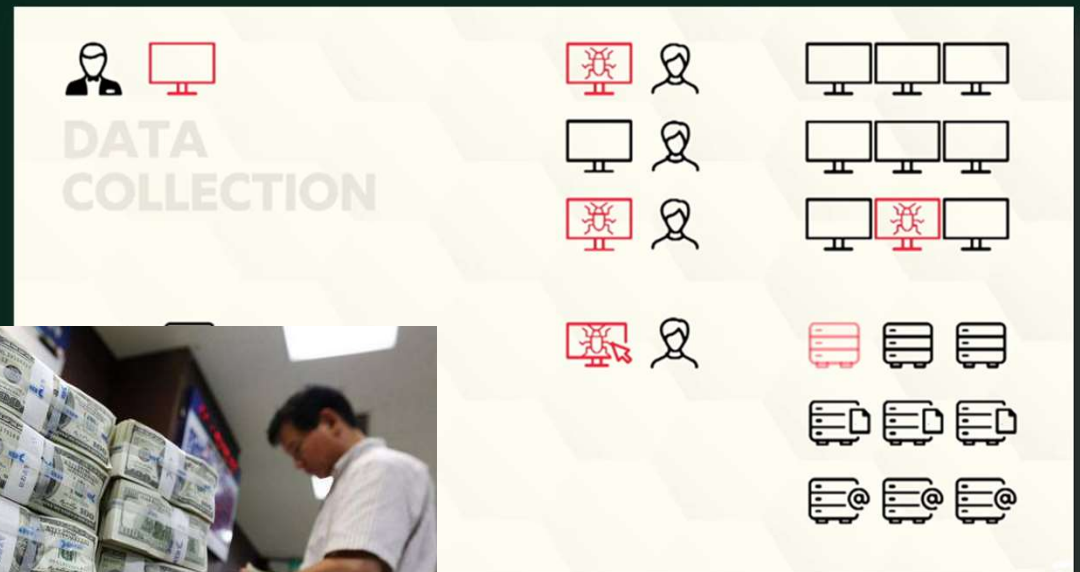


Hämärää bisnestä

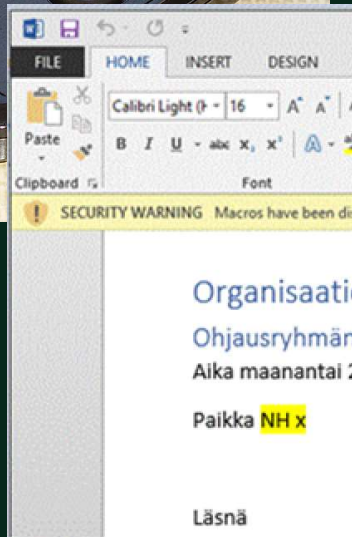
Kohdennettu hyökkäys ei tarkoita että olit kohde alusta asti.

Opportunistisen sisäänpääsyn jälkeen kohteet arvotetaan ja etenemisestä päätetään.

Toiminta kuin yrityksessä.
Contileaksissa HR huolia



Erään murron tarina



Lähettäjä: ext-migratic
Lähetetty: keskiviikkona 11. toukokuuta 2010
Vastaanottaja:
Aihe: TÄNÄÄN: Tietojen siirto WebSync-järjestelmään

Terve!

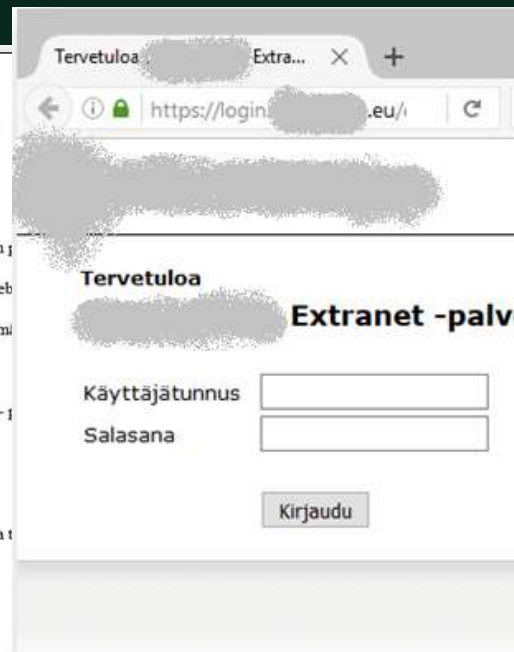
Osana käynnissä olevaa kommunikaatiojärjestelmien ja nykyisten kontaktitietojen siirtoa pilvipohjaiseen WebSync-järjestelmään tulee korvaamaan kaikki nykyiset pikaviestijärjestelmät.

Siirtymän helpottamiseksi synkronoimme WebSync-järjestelmään nykyisistä järjestelmistä.

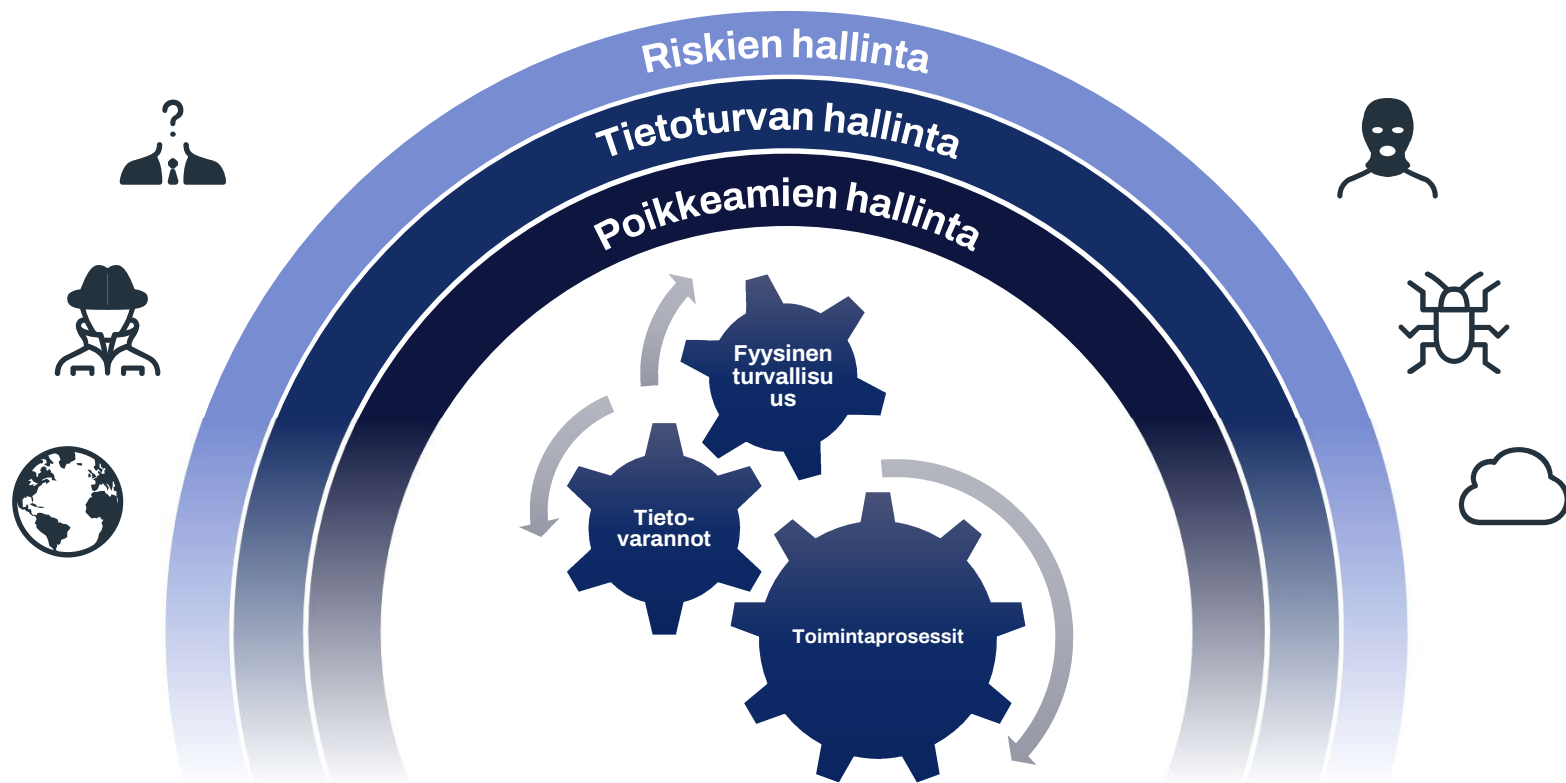
Tämä prosessi vaatii autentikoinnin käyttäjän omilla tunnuksilla ja yksityisyydensuojattuihin tietoihin.

Sinun käyttäjätunnuksesi on migraatiovuorossa tälle palvelimelle.

Kun migraatiojonossa on tilaa, ottaa ylläpitomme sinuun yhteyttä puhelimella ja neuvoo tarvittavat vaiheet läpi kohta kohdalta.



Puolustuksen työkalut



Puolustuksen työkalut

Turvallisuus on kuin laatu – se syntyy oikeista arkipäivän teoista.

Turvallisuuden täytyy olla kulttuurissa.

Vanhan koulun IT ei ole mennyt mihinkään.

Kybersietoisuus.

Sirpaloitunut IT tuottaa haasteita

Oman elämän kyberturva

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työkaluihin

4: Vältä huijaukset

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi

- ✓ Käyttäjän tunnistautuminen usein ainoa suojaus.
- ✓ Ihmiselle vaikea salasana ei ole sitä tietokoneelle.
- ✓ Pidempi on parempi, voi olla lause.
- ✓ Salasanageneraattorit ja lompakot.

<https://www.lastpass.com/>

<https://bitwarden.com>

<https://1password.com/>

<https://www.f-secure.com/en/home/products/id-protection>

Oman elämän kyberturva

1: Salasanat

2: **Klikkaile harkiten**

3: Kiinnitä huomiota työkaluihin

4: Vältä huijaukset

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi

- ✓ Suurin osa haittaohjelmista vaatii käyttäjältä aktiivista osallistumista.
- ✓ Sähköpostien liitetiedostot.
- ✓ Linkit viesteissä, myös SoMe ja tekstiviestit.
- ✓ Ponnahdussivustot ja mainokset.



Erja Tuomisto <dicleSheena7513@h
otmail.com>

Sun 2/7/2021 21:07

To: You

Oman elämän kyberturva

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työkaluihin

4: Vältä huijaukset

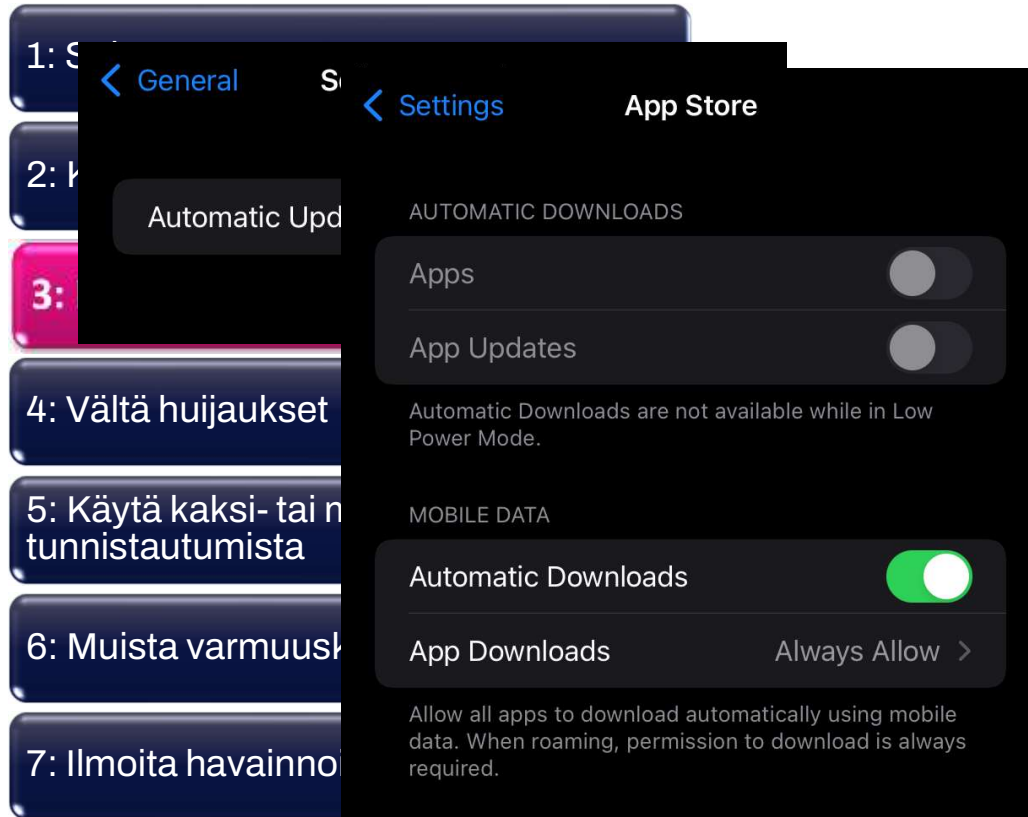
5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi

- ✓ Päivitä ohjelmat ja käyttöjärjestelmä!
Kytke automaattiseksi aina jos mahdollista.

Oman elämän kyberturva



ohjelmat ja käyttöjärjestelmä!
omaattiseksi aina jos mahdollista.

Oman elämän kybertur

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työkaluihin

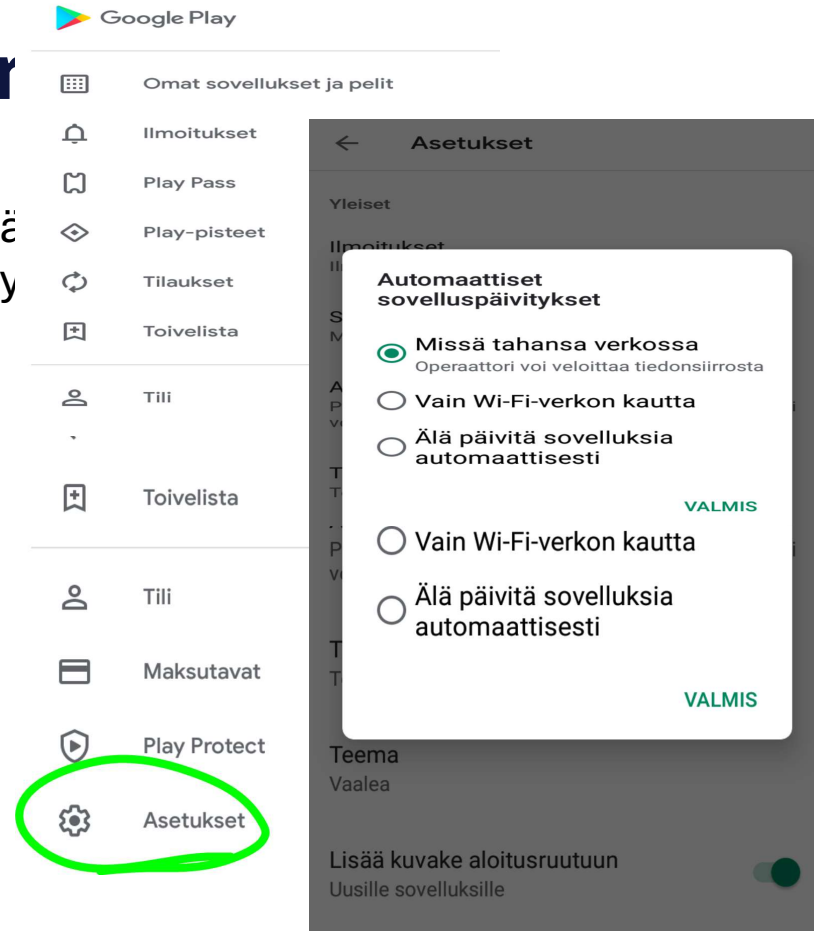
4: Vältä huijaukset

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi

✓ P
Ky



Oman elämän kyberturva

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työkaluihin

4: Vältä huijaukset

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi

- ✓ Päivitä ohjelmat ja käyttöjärjestelmä!
Kytke automaattiseksi aina jos mahdollista.
- ✓ Netiselaimissa on eroja.
 - Firefox – Yksityisyydensuoja
 - Google Chrome – Tietoturva
- ✓ Lisäosilla lisäsuojaa:
 - https everywhere
 - Facebook container
 - Privacy Badger

Oman elämän kyberturva

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työkaluihin

4: Vältä huijaukset

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi

- ✓ Jos jokin kuulostaa liian hyvältä ollakseen totta, se todennäköisesti on.
- ✓ “SoMe kuplat”, pidä mielessä mitä kaikkea sinusta jo tiedetään.
- ✓ Pyydetäänkö sinua yhtäkkiä tekemään jotain?
- ✓ Ilmoittaako tämä palveluntarjoaja minulle asioita näin?

Oman elämän kyberturva

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työkaluihin

4: Vältä huijaukset

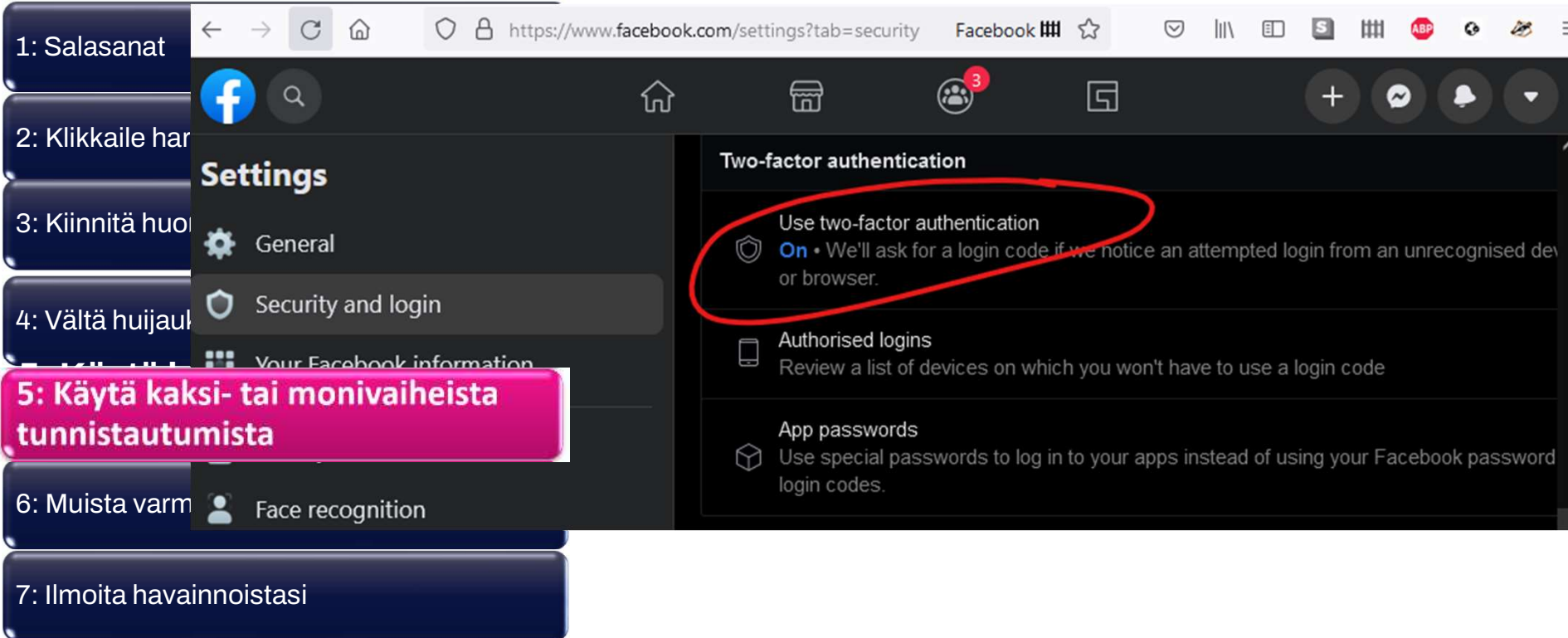
5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi

- ✓ Salasanat ovat matematiikkaa.
- ✓ Salasanat vakoiltavissa tai varastettavissa.
- ✓ Kaikkeen suojaamisen arvoiseen, vahva tunnistus.
Aina.
- ✓ Aina.

Oman elämän kyberturva



1: Salasanat

2: Klikkaile har

3: Kiinnitä hu

4: Vältä huijau

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varm

7: Ilmoita havainnoistasi

Settings

- General
- Security and login
- Your Facebook information
- Face recognition

Two-factor authentication

- Use two-factor authentication
On • We'll ask for a login code if we notice an attempted login from an unrecognised device or browser.
- Authorised logins
Review a list of devices on which you won't have to use a login code
- App passwords
Use special passwords to log in to your apps instead of using your Facebook password login codes.

Oman elämän kyberturva

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työk

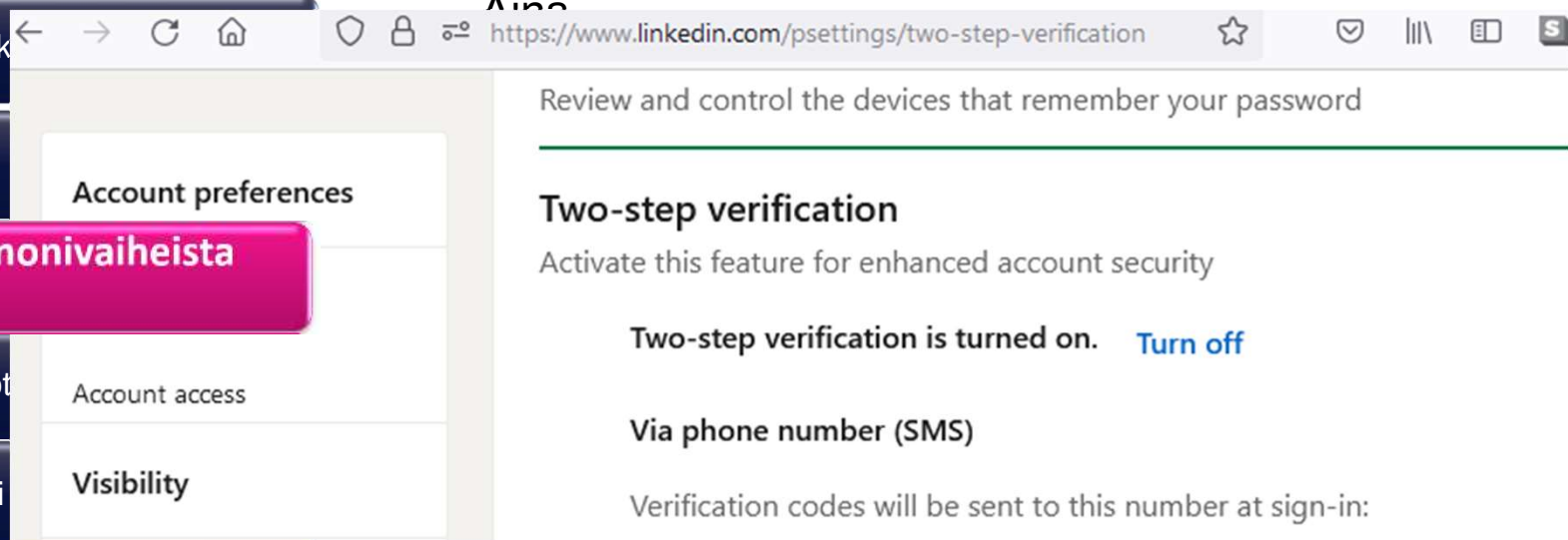
4: Vältä huijaukset

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopioi

7: Ilmoita havainnoistasi

- ✓ Salasanat ovat matematiikkaa.
- ✓ Salasanat vakoiltavissa tai varastettavissa.
- ✓ Kaikkeen suojaamisen arvoiseen, vahva tunnistus.



The screenshot shows a browser window with the URL <https://www.linkedin.com/psettings/two-step-verification>. The page title is "Review and control the devices that remember your password". The main heading is "Two-step verification" with the subtext "Activate this feature for enhanced account security". Below this, it states "Two-step verification is turned on." with a "Turn off" link. Underneath, it says "Via phone number (SMS)" and "Verification codes will be sent to this number at sign-in:". On the left side of the screenshot, a sidebar menu is visible with sections for "Account preferences", "Account access", and "Visibility".

Oman elämän kyb

1: Salasanat

2: Klikkaile harkiten

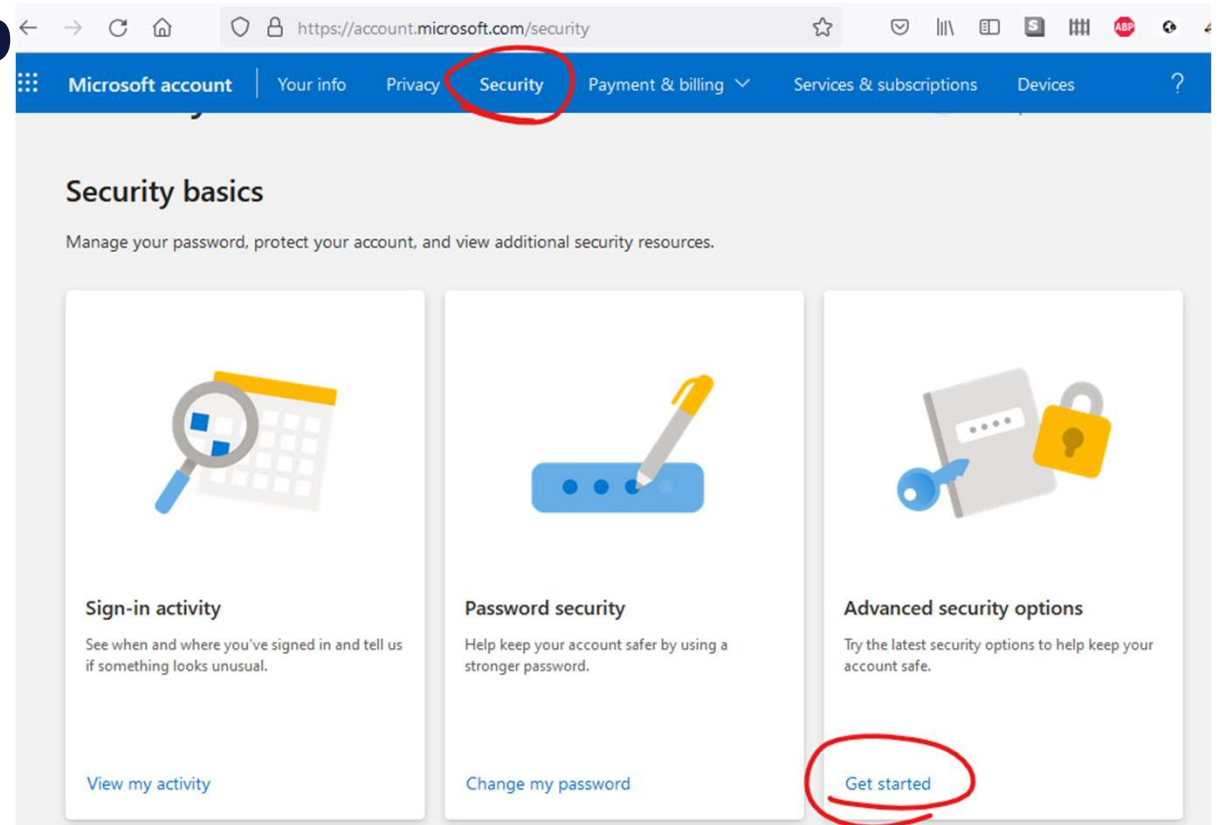
3: Kiinnitä huomiota työkaluihin

4: Vältä huijaukset

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi



The screenshot shows the Microsoft account security page. The browser address bar displays <https://account.microsoft.com/security>. The navigation menu includes "Microsoft account", "Your info", "Privacy", "Security" (circled in red), "Payment & billing", "Services & subscriptions", and "Devices". The main heading is "Security basics" with the subtext "Manage your password, protect your account, and view additional security resources." There are three main sections: "Sign-in activity" with a "View my activity" link, "Password security" with a "Change my password" link, and "Advanced security options" with a "Get started" link (circled in red). Each section includes an icon and a brief description of the feature.

Oman elämän kyberturva

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työkaluihin

4: Vältä huijaukset

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi

- ✓ Krypto-haittaohjelmia vastaan paras suoja.
- ✓ Pilvipalvelut tekevät “parhaansa” asioiden tallessapitämiseen.
- ✓ Muutaman kymppin USB levyllä välttää ison harmin.

Oman elämän kyberturva

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työkaluihin

4: Vältä huijaukset

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi

- ✓ Internetin ekosysteemi on globaali ja pyörii yhteisvastuulla.
- ✓ Olet harvoin ainoa uhri.
- ✓ Ilmoita eteenpäin huijauksista ja vahingoista
 - Sivustojen ylläpito
 - Roskapostisuodattimen ylläpito
 - <https://tietosuoja.fi/ilmoitus-tietosuojavaltuutetulle>
 - <https://poliisi.fi/tee-rikosilmoitus>
 - <https://www.kyberturvallisuuskeskus.fi/fi/ilmoita>

missä

missä

missä **syödä krakovassa**
kan

kan

kannattaako puolassa maksaa euroilla
pit

pit

kannattaako puolassa maksaa euroilla
pit

pit

pitääkö puolassa antaa tippiä

👍 🗨️ 📌

ja 11 muuta tykkäävät

Googlen tekoäly on pelottavan hyvä... 3/3.



Maailma menossa parempaan



.. mutta ei yksinkertaisempaan.

W / T H[®]
secure