HYÖKKÄYKSEN ANATOMIA

Antti Laatikainen, Johtava konsultti
WithSecure Consulting

WITH secure

ÄLÄ HÄTÄILE

Valmistautumalla näistä selviää

Hyökkäyksen anatomia

Erään murron tarina

Puolustuksen työkalut

Arkipäivän vinkit

Miksi tietoturva on tärkeää?

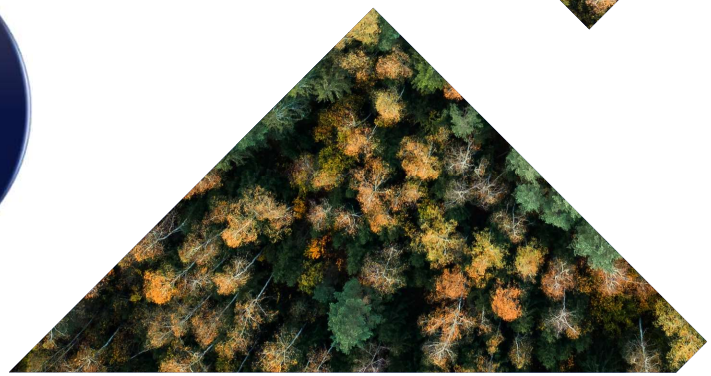
Rahaa, henkilöllisyys, arkaluontoista tietoa	• - Rikollinen tavoittelee kaikkea rahanarvoista.
Nettiyhteys tai tietokoneesi	• - Nettiyhteyttäsi tai laitteitasi käytetään rikolliseen toimintaan.
Maine	• - Nimelläsi tehtaillut rikokset ja vahingonteot ovat kiusallisia ja haitallisia.

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

WITH secure

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.

WITH secure

Hyökkäys on palapeli

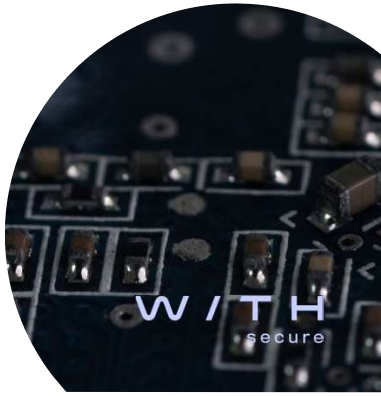
Tiedusteluvaiheessa kaikki tieto on hyvää tietoa.

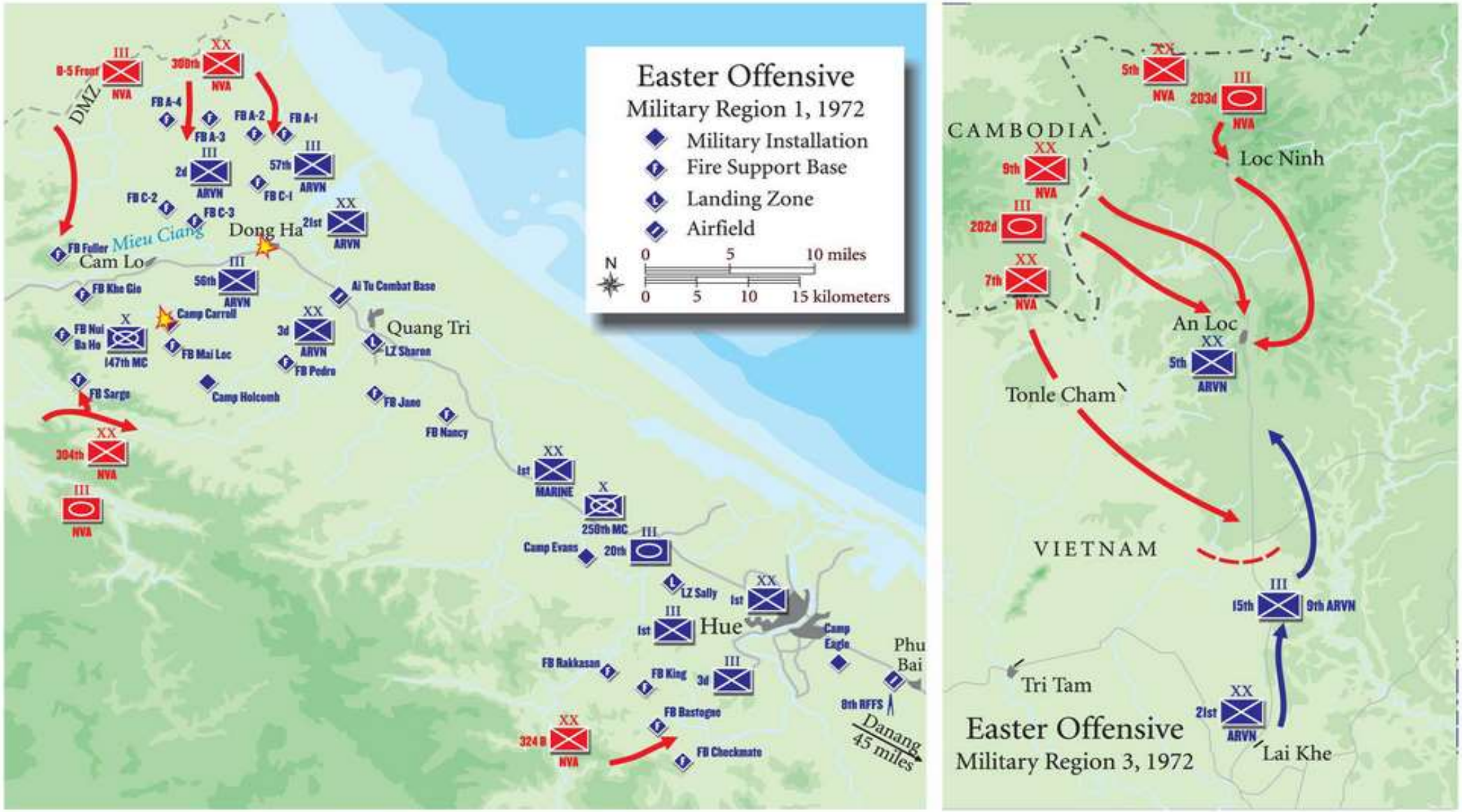
Murto on yleensä nopea, hyvin suunniteltu ja pistemäinen.

Sisäinen levittäytyminen tehdään harkiten ja mahdollisimman hiljaa.

Todellinen vahinko tehdään kun maalit on tunnistettu ja ajoitus oikea.

Mahdollisuuksien mukaan jäljet pyyhitään.




Easter Offensive
Military Region 1, 1972
Military Installation
Fire Support Base
Landing Zone
Airfield
N
0 5 10 miles
0 5 10 15 kilometers
DMZ
B-5 Front
III
NVA
XX
308th
NVA
FB A-4
FB A-3
FB A-2
FB A-1
III
2d
ARVN
III
57th
ARVN
FB C-2
FB C-3
FB C-1
XX
21st
ARVN
Mieu Giang
Dong Ha
FB Fuller
Cam Lo
III
56th
ARVN
FB Khe Gio
Ai Tu Combat Base
Camp Carroll
X
147th MC
FB Nui Ba Ho
FB Mai Loc
XX
3d
ARVN
FB Pedro
Quang Tri
LZ Sharon
Camp Holcomb
FB Sarge
FB Jane
FB Nancy
XX
304th
NVA
III
NVA
XX
1st
MARINE
X
258th MC
III
20th
Camp Evans
LZ Sally
XX
1st
III
1st
Hue
Camp Eagle
Phu Bai
FB Rakkasan
FB King
III
3d
8th RFFS
FB Bastogne
XX
324 B
NVA
FB Checkmate
Danang
45 miles
CAMBODIA
XX
5th
NVA
III
203d
NVA
Loc Ninh
XX
9th
NVA
III
202d
XX
7th
NVA
An Loc
XX
5th
ARVN
Tonle Cham
VIETNAM
III
15th
9th ARVN
Tri Tam
XX
21st
ARVN
Lai Khe
Easter Offensive
Military Region 3, 1972

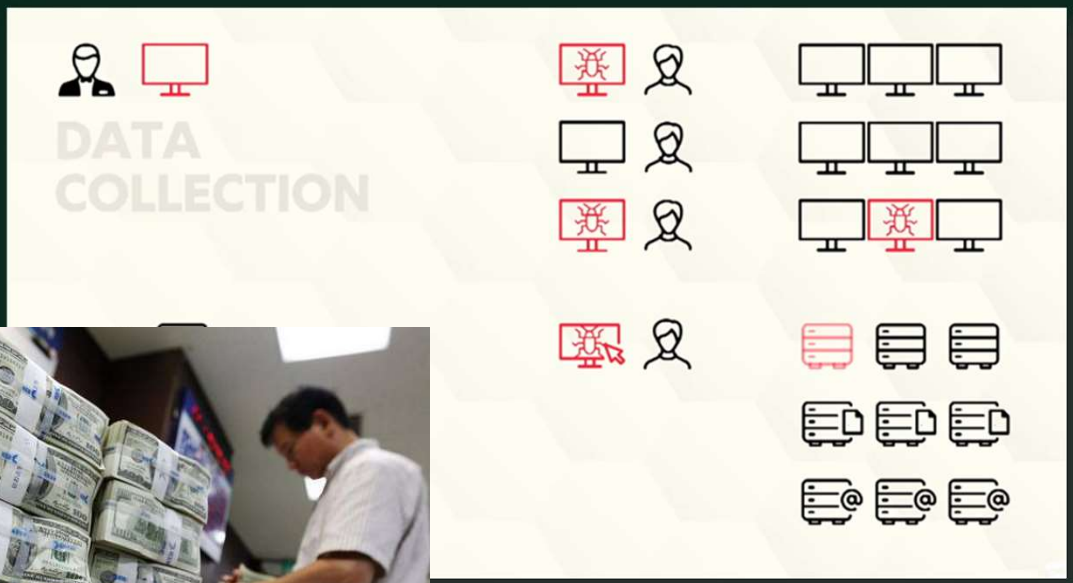
Hämärää bisnestä

Kohdennettu hyökkäys ei tarkoita että olit kohde alusta asti.

Opportunistisen sisäänpääsyn jälkeen kohteet arvotetaan ja etenemisestä päätetään.

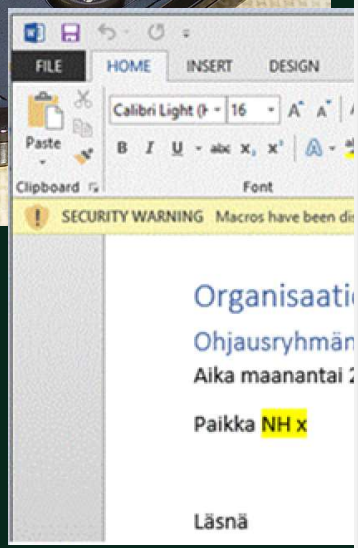
Toiminta kuin yrityksessä.

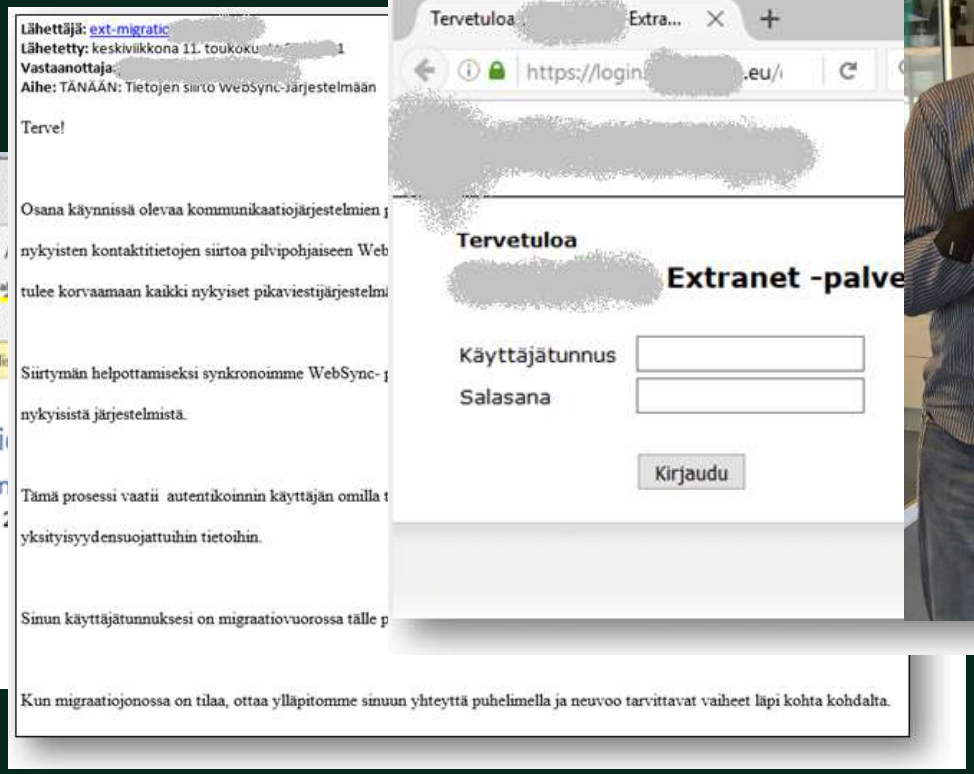
Contileaksissa HR huolia



WITH secure

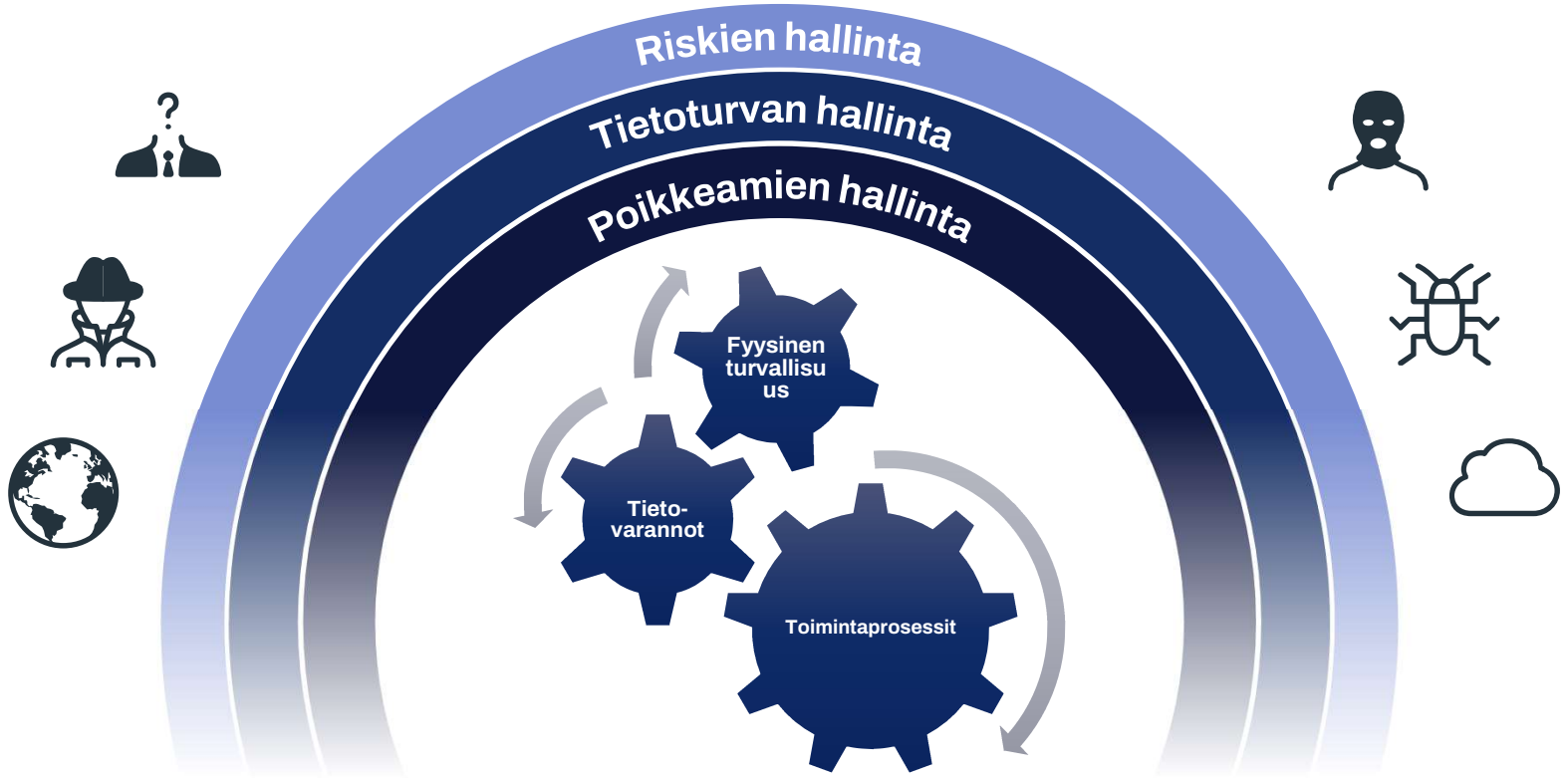
Erään murron tarina





WITH secure

Puolustuksen työkalut



WITH secure

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

WITH secure

KyberVPK

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

KyberVPK

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.

KyberVPK

Oman elämän kyberturva

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työkaluihin

4: Vältä huijaukset

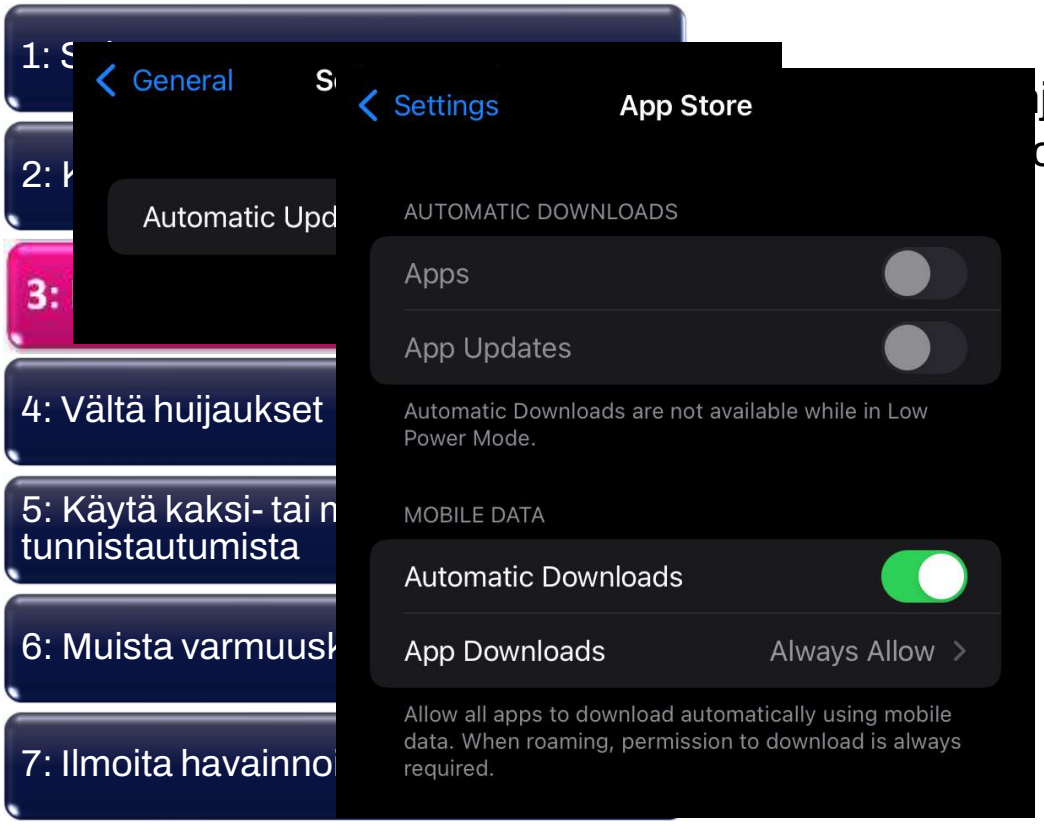
5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi

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

Oman elämän kyberturva



jelmat ja käyttöjärjestelmä!
omaattiseksi aina jos mahdollista.

Oman elämän kybertur

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työkaluihin

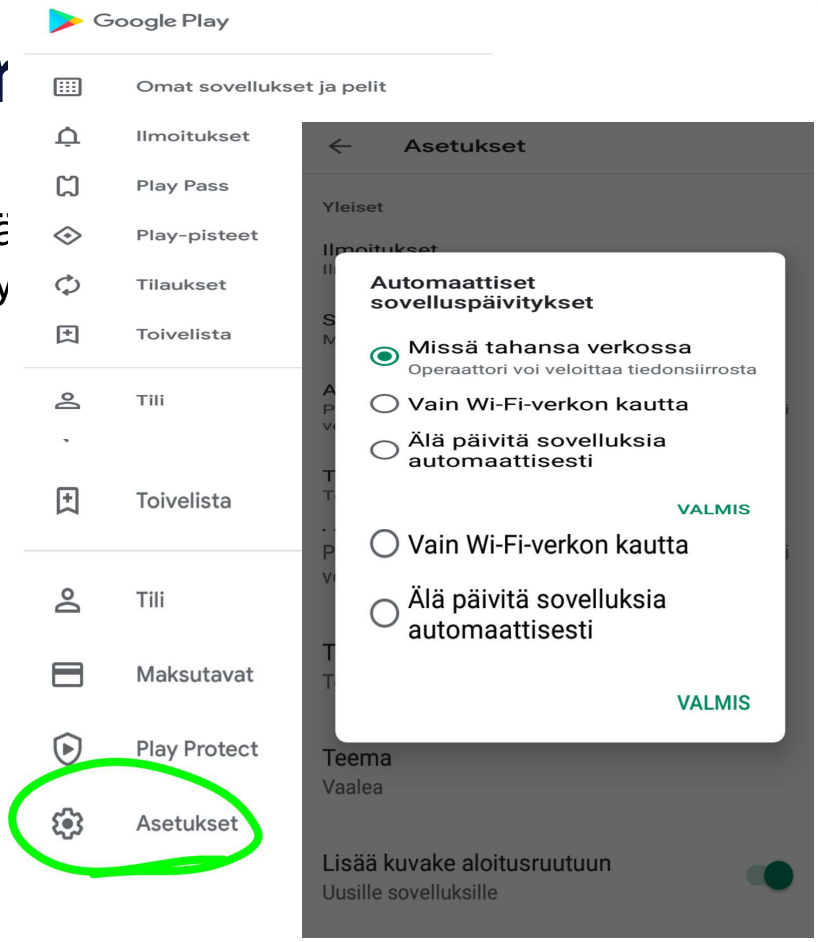
4: Vältä huijaukset

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi

✓ Pä
Ky



KyberVPK

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.
- ✓ Nettiselaimissa 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?

KyberVPK

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

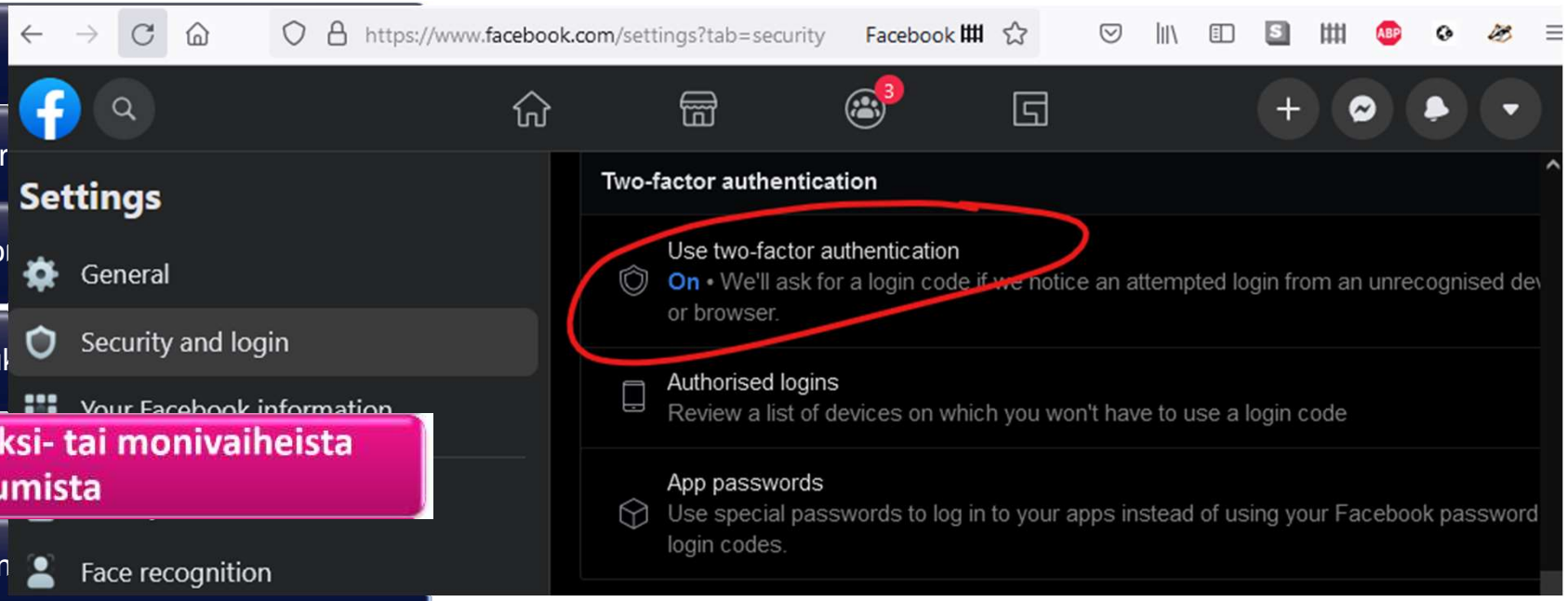
3: Kiinnitä huo

4: Vältä huijauk

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varm

7: Ilmoita havainnoistasi



Oman elämän kyberturva

1: Salasanat

2: Klikkaile harkiten

3: Kiinnitä huomiota työk

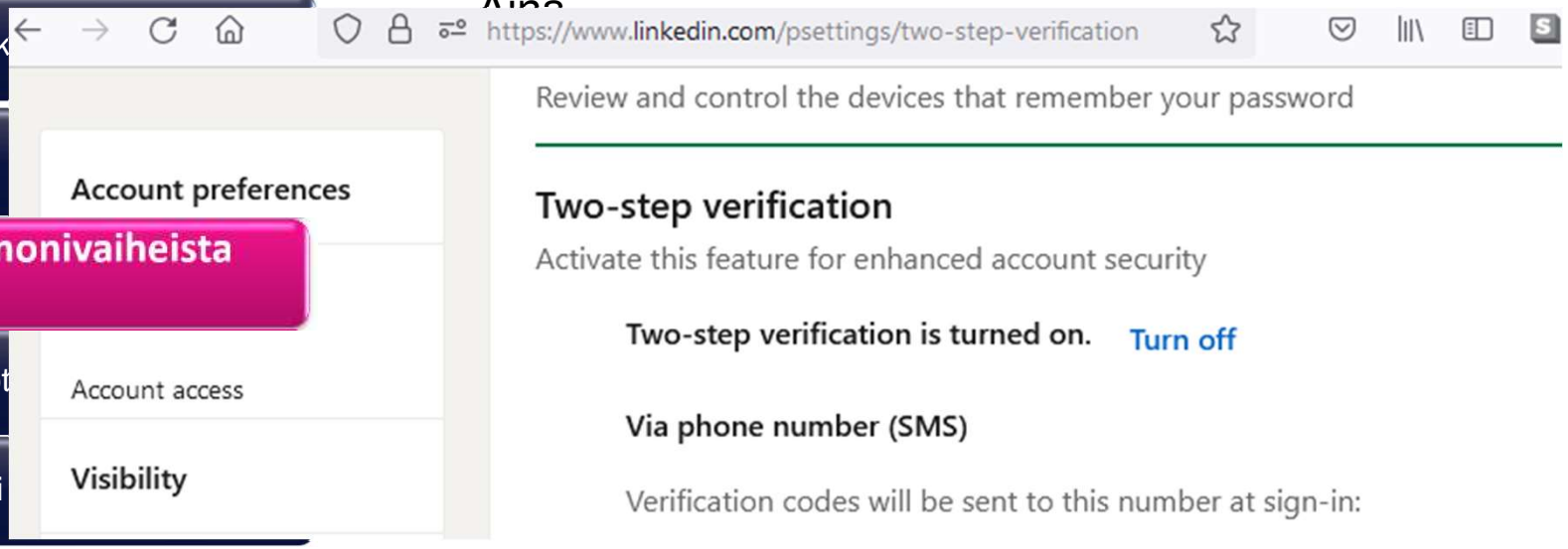
4: Vältä huijaukset

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



KyberVPK

Oman elämän kyb

1: Salasanat

2: Klikkaile harkiten

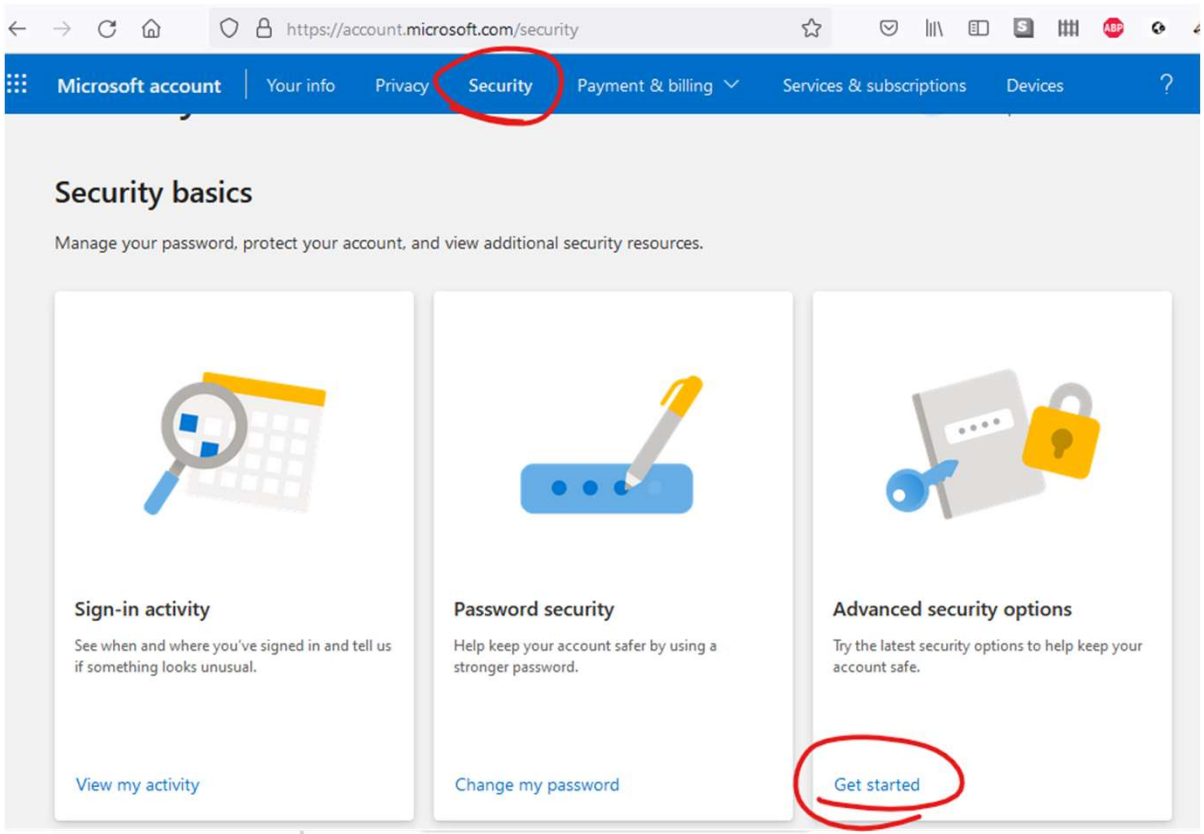
3: Kiinnitä huomiota työkaluihin

4: Vältä huijaukset

5: Käytä kaksi- tai monivaiheista tunnistautumista

6: Muista varmuuskopiot

7: Ilmoita havainnoistasi



KyberVPK

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 kympin USB levyllä välttää ison harmin.

KyberVPK

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

kan**nattaako puolassa maksaa euroilla**

pit

pit

kan**nattaako puolassa maksaa euroilla**

pit

pit

pit**ääkö puolassa antaa tippiä**

[redacted] ja **11 muuta** tykkäävät

[redacted] Googlen tekoäly on pelottavan hyvä... 3/3.

Maailma menossa parempaan

.. mutta ei yksinkertaisempaan.

WITH secure


WITH®
secure