

10 helppoa kyberhygieniakäytäntöä

1. Varo, sosiaalista manipulointia, huijauksia ja mitä linkkiä klikkaat!

90% ihmisten aiheuttamista kybervahingoista johtuu siitä, että joku klikkaa vaarallista linkkiä tai antaa tunnuksensa.

2. Käytä kaksivaiheista tunnistautumista.

Sen avulla tiliesi kaappaaminen on huomattavasti vaikeampaa kuin pelkän salasanan avulla.

3. Käytä vahvoja salasanoja ja salasanojen hallintaohjelmaa.

Salasanalause on helpompi muistaa kuin omituinen merkkijono. 16 merkkiä. Salasananhallinta-ohjelma auttaa eniten. Älä kierrätä salasanoja.

4. Asenna virustorjuntaohjelma kaikkiin laitteisiisi.

Säästyt monelta ongelmalta.

5. Älä käytä ilmaisia julkisia verkkoja! Varsinkaan maailmalla!

Käytä omaa tietokonettasi vain **oman kännykkäsi verkon** kautta, ei liittymällä muihin verkkoihin. Ulkomailla osta tarvittaessa paikallinen SIM-kortti datan siirtoon.

6. Päivitä, päivitä, päivitä.

Pidä ohjelmistosi ja laitteesi ajan tasalla päivittämällä ne esim. automaattisesti.

7. Työ- ja kotilaitteet erikseen.

Mikäli käytät samaa laitetta molempiin tarkoituksiin, älä päästä muita henkilöitä laitteillesi.

8. Oikeuksien hallinta kuntoon.

Anna kullekin vain tarvittavat oikeudet eri palveluihin. Poista tunnukset ja palvelut, joita ei käytetä. Pidä huolta, että joka palvelussa on ainakin kaksi adminia.

9. Pidä tietosi luottamuksellisina.

Lukitse kone aina kun nouset sen äärestä. Hanki liikkuvaa työskentelyä varten kalvo, jotta muut eivät voi urkkia tietoja olkasi takaa. Käytä VPN-ohjelmistoa. Luottamukselliset puhelinkeskustelut kuuluvat yksityiseen tilaan.

10. Harjoittele.

Harjoittelemalla parannat oleellisesti mahdollisuksiasi selvittää kyberkriisistä nopeasti.



South-Eastern Finland
University of Applied Sciences

REGIONAL
COUNCIL
KYMEN
LAAKSO



Co-funded by
the European Union

Cyber-
resilient
Kymen-
laakso