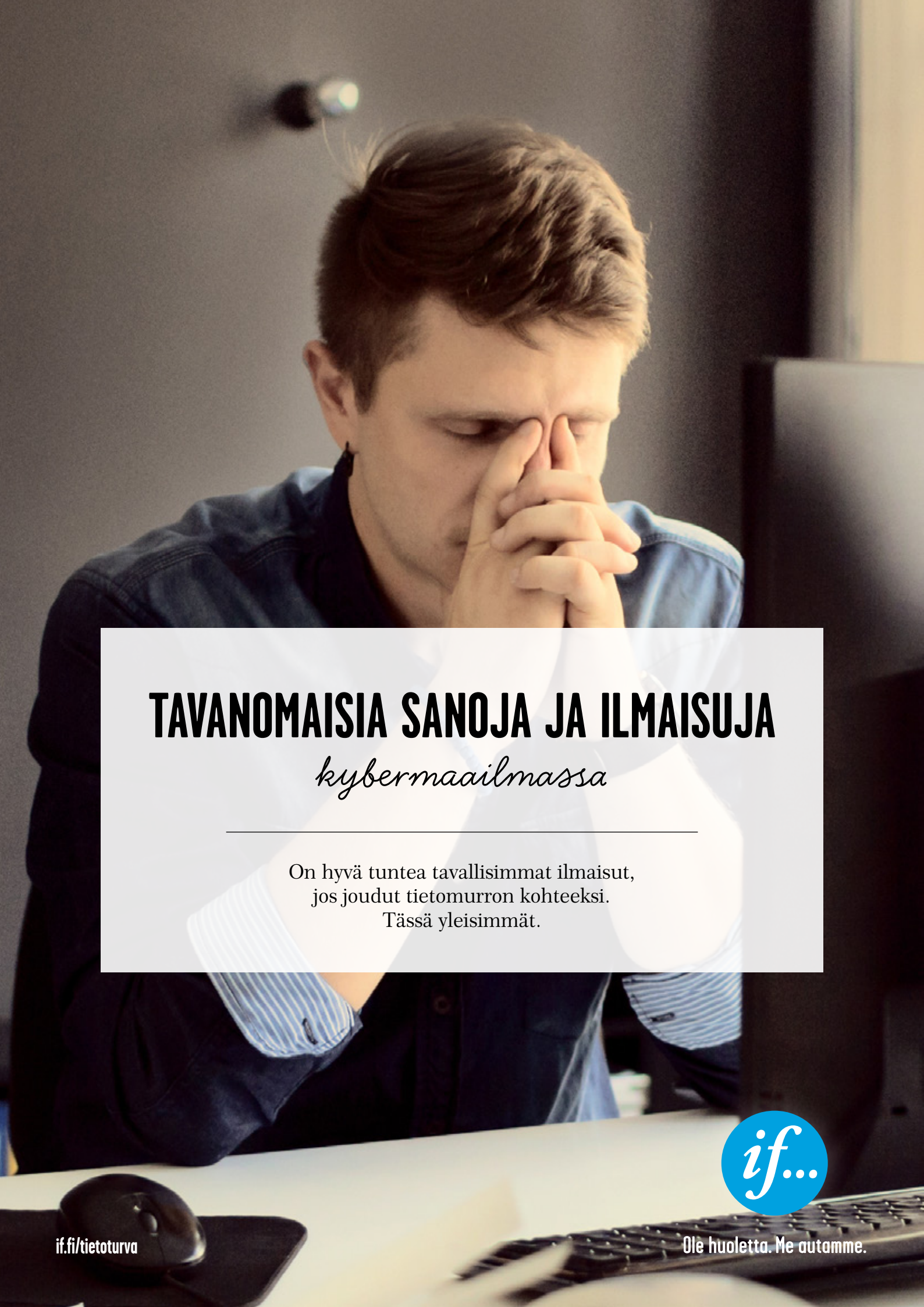

TAVANOMAISIA SANOJA JA ILMAISUJA

kybermaailmassa

On hyvä tuntea tavallisimmat ilmaisut,
jos joudut tietomurron kohteeksi.
Tässä yleisimmät.

if...

KYBERHYÖKKÄYS
Kyberhyökkäys tarkoittaa, että tietokone tai tietokoneen ohjaama järjestelmä altistetaan huomaamattomasti ja internetin avulla ottamaan haltuun tietokoneita tai tietojenkäsittelyjärjestelmiä. Hyökkäyksen tarkoituksena on vahingoittaa, häiritä tai ylikuormittaa järjestelmää.

MALWARE, HAITTAOHJELMAT
Malware, haittaohjelmat, asennetaan tietokoneeseen ja ne suorittavat kätkettyjä toimintoja joko käyttäjän tietämättä tai ilman hänen tietoista hyväksyntäänsä. Monissa tapauksissa vaaditaan erikoistyökaluja poistamaan haittaohjelma kiintolevyltä. Yksinkertaisinta ja yleisintä haittaohjelmatyyppiä kutsutaan nimellä spyware eli vakoiluohjelma. Vakoiluohjelmat valvovat ja kirjaavat Internet-tottumuksia käytettäväksi myöhemmin esim. markkinointitarkoituksiin. Vakoiluohjelma voidaan asentaa tietokoneeseen verkkosivulla käynnin yhteydessä.

SPYWARE, VAKOILUOHJELMA
Monet vakoiluohjelmat käyttävät tietoja näyttääkseen kohdistettuja mainoksia. Vakoiluohjelma, spyware, on ohjelma, joka toimii tietokoneessa ilman käyttäjän suostumusta ja joka kerää ja välittää tietoja toiselle osapuolelle. Kyseessä voi olla esim. sähköpostiviesti, salasana ja muu samankaltainen tieto.
Vakoiluohjelma asentuu yleensä itsestään käyttäjän asentaessa ohjelmia. Kyseessä voi olla troijalaisia tai komponentteja, joista kerrotaan ohjelman käyttöehdoissa, mahdollisesti pienellä kirjoitettuna. Myös tietokonevirukset, madot ja muut haittaohjelmat voivat asentaa vakoiluohjelmia tai asennus voi tapahtua manuaalisesti tietomurron yhteydessä.
Vakavin vakoiluohjelmien tyyppi ovat sellaiset ohjelmat, jotka keräävät esimerkiksi salasanoja, luottokorttinumeroita tai muita arkaluonteisia tietoja.

MAINOSOHJELMA (ADWARE)
Tietokoneen haittaohjelma, joka esittää käyttäjälleen mainoksia ohjelman normaalin käytön yhteydessä. Mainoksilla ei välttämättä ole minkäänlaista yhteyttä itse ohjelman käyttötarkoitukseen. Tavallisesti mainosohjelmat ovat ilmaisohjelmia, jotta ohjelma saavuttaisi mahdollisimman suuren käyttäjä- ja katsojamäärän.

HAKKEROINTI
Hakkerointi tarkoittaa, että joku asiaton henkilö tunkeutuu tiettyyn järjestelmään tai sovellukseen ilman käyttäjän lupaa tai hänen tietämättään.

HAKKERI
Hakkeri on henkilö, joka onnistuu murtautumaan verkkojärjestelmään tai tietokonejärjestelmään, vaikka sitä pidetään turvallisena. On olemassa kahdenlaisia hakkereita, ”valkohattuhakkeri” ja ”mustahattuhakkeri”. ”Valkohattuhakkeri” on henkilö, joka työskentelee yrityksessä ja edistää taidoillaan järjestelmän tietoturvan parantamista. ”Mustahattuhakkeri” on henkilö, joka laittomasti murtautuu järjestelmään joko varastaakseen tietoja tai osoittaakseen osaamistaan.

DENIAL OF SERVICE, DOS
Tietoturvan piirissä Denial of Service eli palvelunesto (usein lyhennetty DoS) on tietojärjestelmään tehty hyökkäys, jonka tarkoituksena on estää järjestelmän normaali käyttö. Yleisin hyökkäystyyppi on ylikuormitushyökkäys.

Tavallisia menettelytapoja:
- haavoittuvuuden tai heikkouden väärinkäyttö, joka saa järjestelmän ohjelmiston kaatumaan tai lukittumaan
- niin suuren liikennemäärän lähettäminen, että järjestelmä tai sovellus kaatuu
- niin suuren roskaliikenteen lähettäminen, että asianmukainen liikenne estyy pääsemästä perille

TIETOKONEVIRUS
Tietokonevirus on tietokoneohjelma, joka levittäytyy lisäämällä kopion itsestään muihin ohjelmiin, toisin sanoen monistamalla itseään ilman käyttäjän lupaa.

TROIJALAINEN
Troijan hevonen eli troijalainen, on tietokoneohjelma, joka näyttää sellaiselta, että sitä voidaan käyttää hyödyksi tai huviksi, mutta joka tekee jotain täysin muuta, kun se on asennettu. Ohjelma voi esimerkiksi vakoilla mitä teet verkossa, suorittaa maksuja nimissäsi, lähettää roskapostia tai hyökätä muihin tietokoneisiin.

WORM, MATO
Mato on ohjelma, joka tekee kopioita itsestään (yleensä yksi järjestelmää kohden) verkon kautta. Se voi tehdä vahinkoa ja vaarantaa tietokoneen tietoturvan. WORM-asemien käytön etu tietoturvan kannalta on, että asemaa lukeva voi olla varma, että tietoja ei ole peukaloitu. Nykyään on olemassa kaksi WORM-median päätyyppiä. Yksi on CD-R ja DVD-R eli optinen media. Toinen WORM-tyyppi ovat elektroniset avaimet ja vastaavat, joiden ominaisuutena on, että yksikköön voidaan kirjoittaa vain kerran.

BACKDOOR ELI TAKAOVI, RAT (REMOTE ACCESS TOOL) ELI ETÄKÄYTTÖTYÖKALU
Tietokoneessa oleva ohjelma, jonka avulla joku muu voi etähallita tietokonettasi. RAT ei ole Troijan hevonen, koska sen tarkoituksena on vasta hyväksymisen jälkeen hallita toisen henkilön tietokonetta.

YHDISTELMÄUHKA
Haittaohjelmia, jotka käyttävät useita menetelmiä ja tekniikoita hyökätäkseen järjestelmiin ja verkkoihin. Tunnetaan myös nimellä Cocktail Malware.

NÄPPÄINNAUHURI, KEYLOGGER
Ohjelmatyyppi, joka havaitsee kaikki tietokoneen näppäimistön painallukset. Keylogger voi siksi kirjautua sisään ja tallentaa sähköpostikeskusteluja, chatteja, salasanoja eli kaikkea kirjoittamasi.

BOTTI
Ohjelmisto, jonka avulla järjestelmää voidaan ohjata etäältä omistajan tietämättä lähettämään roskapostia, tartuttamaan muita järjestelmiä tai hyökkäämään muihin järjestelmiin (joko DoS tai DDoS).

DISTRIBUTED DENIAL OF SERVICE (DDOS)
DDOS tulee sanoista ”Distributed Denial of Service” (hajautettu palvelunestohyökkäys) ja se on laaja hyökkäys verkkoon tai tietokonejärjestelmään. Hakkeri luo ns. bottiverkon käyttämällä esimerkiksi troijalaisia lukuisien verkkoon kytkettyjen tietokoneiden kaappaamiseen, useimmiten niiden omistajien tietämättä. Hakkeri käyttää sitten kaapattuja tietokoneita ohjatakseen useita samanaikaisia kutsuja järjestelmään, esimerkiksi pyytämällä lataamaan tiedoston web-palvelimelta.

Näin kaapatut tietokoneet syövät hyökkäyksen kohteena olevan järjestelmän kaistanleveyden ja kukaan ei pääse käsiksi järjestelmään.

PHISHING, VERKKOKALASTELU
Phishing eli verkkokalastelu on laiton tapa huijata sinua paljastamaan luottokorttien numeroita, salasanoja tai muita arkaluonteisia tietoja. Verkkokalastelu tapahtuu siten, että saat sähköpostin, joka näyttää tulevan pankistasi tai esimerkiksi luottokorttiyhtiöstä. He pyytävät sinua pikaisesti kirjautumaan linkin kautta, joka menee väärennetylle verkkosivulle. Tarkoituksena on huijata sinulta kirjautumistietosi. Sähköpostiviestit voivat olla erittäin hyvin laadittuja ja ei ole helppo huomata, että ne ovat vääriä.

Usein lähettäjän ilmoitetaan olevan käyttäjätukiosasto ja sähköpostissa sanotaan, että tilisi suhteen on ilmennyt jokin ongelma ja että virheen korjaamiseksi tarvitaan kirjautumistietojasi.

Älä koskaan anna kirjautumistietojasi tällä tavalla - laillisessa toiminnassa ei pyydetä salasanoja sähköpostitse.

KOHDISTETTU HYÖKKÄYS, APT (ADVANCED PERSISTENT THREAT)
APT, joka tunnetaan myös kohdennettuna hyökkäyksenä ja jossa hyökkääjä käyttää erilaisten työkalujen ja menetelmien yhdistelmää saadakseen pääsyn tietyn organisaation järjestelmään ilman kohteen hyväksyntää tai tämän tietämättä. Tämä voi tapahtua yksinkertaisen hakkeroinnin avulla, verkkokalastelulla tai käyttämällä haittaohjelmaa.

PALOMUURI (FIREWALL)
Eristävä moniosainen järjestelmä, joka suodattaa suojattavan verkon ja vaarallisemman verkon välisiä yhteyksiä. Useimmiten palomuuria tarvitaan avoimesta internetistä tulevilta hyökkäyksiltä suojautumista varten. Palomuurilaitteilla on sääntöjä, joilla sisään tulevista yhteyksistä suodatetaan pois kaikki muu, paitsi tarvittava minimi.

Oletko miettinyt yrityksesi tietoturvaa?

Tietoturvavakuutuksemme tarjoaa sekä korvauksia että asiantuntija-apua, jos yritys joutuu tietomurron kohteeksi. Sivulta if.fi/tietoturva voit lukea lisää ja pyytää tarjouksen. Voit myös soittaa 010 19 15 00.

Ole huoletta. Me autamme.

Lisätietoja saat Ifin asiantuntijoilta ja osoitteesta if.fi/tietoturva.

*If Vahinkovakuutus Oyj, Suomen sivuliikkeen vakuutuksia säätelee vakuutussopimuslaki ja muu Suomen lainsäädäntö.
Ifin toimintaa valvoo Finanssivalvonta, Snellmaninkatu 6, PL 103, 00101 Helsinki. www.finanssivalvonta.fi, puh. 09 183 5360.*

If Vahinkovakuutus Oyj, Suomen sivuliike, rekisteröity kotipaikka Tukholma, Y-tunnus 1602149-8, PL 4, 00025 IF. 66752 8/2017