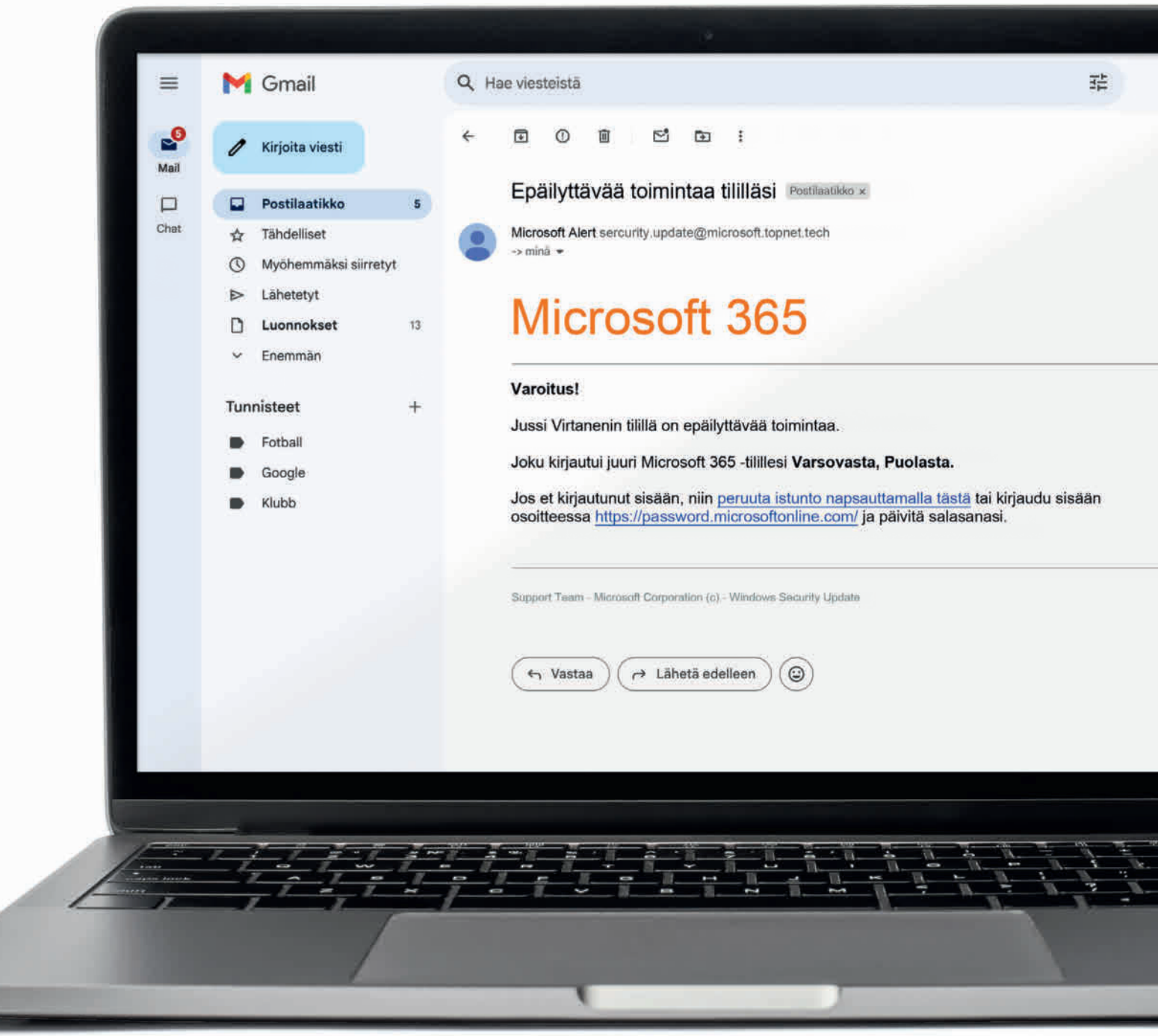
Mistä näkee, että tämä viesti on huijaus?



VASTAUS: Lähettäjä on outo

Näytöllä on esimerkki siitä, miltä Microsoftin yhteydenotolta vaikuttava mutta epäilyttävä ja vaarallinen sähköpostiviesti voi näyttää. Todellisuudessa sähköpostiviesti on huijarilta, ja voit tunnistaa sen katsomalla lähettäjän osoitetta tarkkaan. Merkkijono on pitkä ja monimutkainen, eikä siinä ole sellaista osoitetta, jota Microsoftin kaltaiselta jättiläisyhtiöltä voisi odottaa.

VASTAUS: Logo on vääränlainen

Toinen merkki siitä, että tämä sähköposti on huijareilta eikä Microsoftilta, on Microsoft 365 -tekstin ulkoasu ja grafiikka. Se kun ei näytä ollenkaan siltä miltä pitäisi. Ensinnäkään fontin väri ei ole sama kuin se, mitä Microsoft käyttää markkinoinnissaan, ja toiseksi myös tekstin ”Microsoft 365” lisäksi tekstin vasemmalla puolella pitäisi aina olla tuttu Microsoftin logo.

Kuva: Random435/Shutterstock.com

HAVAITSE HUIJAUKSET AJOISSA

Kymmenen vaaran merkkiä

Hakkerit lähettävät nyt enemmän huijausvestejä kuin koskaan ennen, joten on tärkeää tietää, mitä vaaran merkkejä kannattaa varoa.

Toimittaja
Martin Lorentsen

Saapuvien viestien laatikkoon ilmestyy sähköposti, joka näyttää saapuneen kuljetusyhtiöltä. Sähköpostissa kerrotaan, että paketti on matkalla postitse, mutta toimituksessa on pieni ongelma: pakettia ei voida toimittaa, ellet maksa pientä summaa.

Viesti saattaa vaikuttaa luotettavalta, ja siksi voi tuntua siltä, että siihen pitäisi vastata. Tämäntyyppinen sähköpostiviesti on kuitenkin lähes aina huijaus. Huijarit yrittävät varastaa arkaluonteisia henkilötietojasi, kuten vaikkapa maksutietojasi, sosiaaliturvatunnuksesi tai salasanojasi. Tämäntyyppisiä sähköpostiviestejä ilmestyy yhä useammin postilaatikoihimme. Arvioiden mukaan 1,2 prosenttia kaikista maailmanlaajuisesti lähetetyistä sähköposteista on tietojenkalasteluyrityksiä.

Tietojenkalastelu voi tulla kalliiksi

Jos lankeat johonkin hakkerien asettamista monista ansoista, vaarana on se, että asennat tietokoneellesi haittaohjelman. Se voi johtaa tiedostojesi menettämiseen myöhemmin. Voit myös ajautua paljon suurempiin ongelmiin, kuten identiteettivarkauden kohteeksi tai jopa menettää kaikki säästösi, jos hakkerit onnistuvat huijaamaan sinut luovuttamaan arkaluonteisia henkilötietojasi.

Hakkerit naamioivat huijauksia paremmin

Jotkut huijausviestit ovat ilmeisempiä kuin toiset, mutta tekniikan kehittyminen vaikeuttaa yhä enemmän sen tunnistamista, mikä on huijausta ja mikä täyttä totta.

Vuoden 2025 alussa Google joutui varoittamaan monia Gmail-käyttäjiä siitä, että hakkerit olivat ottaneet kohteekseen 2,5 miljardia tiliä. He käyttivät tuolloin tekoälyä tehdäkseen huijauksistaan uskottavampia.

Kaikki hakkerit eivät ole yhtä ovelia, eikä ole mahdotonta tunnistaa, milloin sähköposti on huijaus. Se edellyttää kuitenkin, että osaa varoa tiettyjä vaaran merkkejä viesteissä.

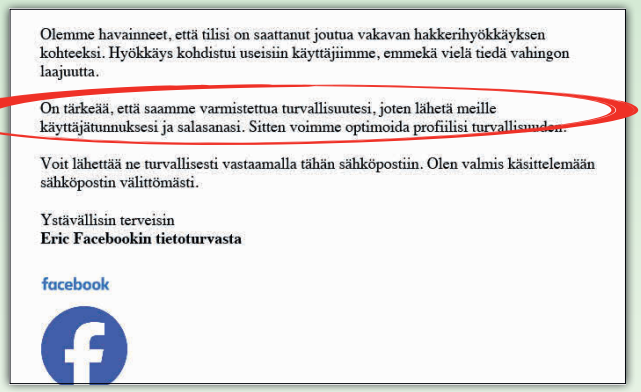
Monet vinkit pätevät myös puhelimeen

Tietojenkalastelua tehdään sähköpostin lisäksi myös tekstiviesteillä. Tämä tunnetaan nimellä ”smishing”. Siinäkin huijarit yrittävät saada vastaanottajan napauttamaan linkkejä, avaamaan liitetiedostoja tai antamaan henkilötietoja. Moniin samoihin vaaran merkkeihin kannattaa kiinnittää huomiota sekä sähköposteissa että tekstiviesteissä.

Viestissä pyydetään antamaan arkaluonteisia tietoja

Vaikka sähköpostin kieli olisi kuinka korrektia ja se näyttäisi luotettavalta, sähköpostiin ei pidä koskaan kirjoittaa arkaluonteisia tietoja, kuten salasanoja. Tämä pätee erityisesti sähköposteihin, joiden lähettäjä pyytää sinua tekemään niin ilman edeltävää vuoropuhelua.

Facebookin tai Netflixin kaltaiset yritykset, pankkisi tai valtion virastot eivät koskaan pyydä sinua antamaan tietojasi tavallisen sähköpostin välityksellä.



Olemme havainneet, että tilisi on saattanut joutua vakavan hakkerihyökkäyksen kohteeksi. Hyökkäys kohdistui useisiin käyttäjiimme, emmekä vielä tiedä vahingon laajuutta.

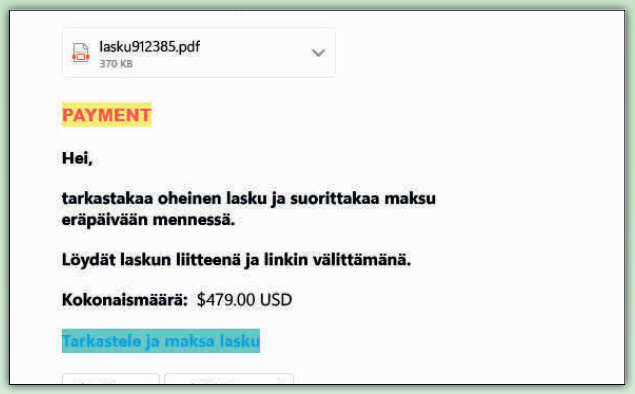
On tärkeää, että saamme varmistettua turvallisuutesi, joten lähetä meille käyttäjätunnuksesi ja salasanasi. Sitten voimme optimoida profiilisi turvallisuuden.

Voit lähettää ne turvallisesti vastaamalla tähän sähköpostiin. Olen valmis käsittelemään sähköpostin välittömästi.

Ystävällisin terveisin
Eric Facebookin tietoturvasta

facebook

Hälytyskellojen pitäisi soida, jos sinua pyydetään lähettämään salasanasi sähköpostitse. Rehdit yhtiöt eivät tee näin.



lasku912385.pdf
370 KB

PAYMENT

Hei,

tarkastakaa oheinen lasku ja suorittakaa maksu eräpäivään mennessä.

Löydät laskun liitteenä ja linkin välittämänä.

Kokonaismäärä: $479.00 USD

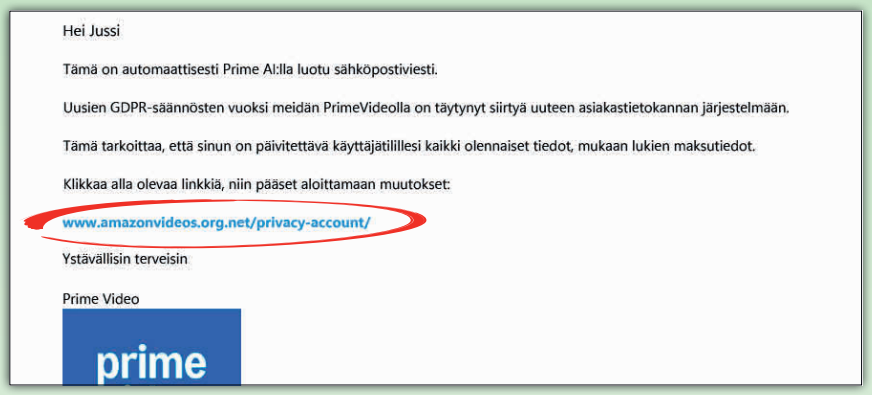
Tarkastele ja maksa lasku

Lasku on yleensä väärennetty, jos se pyydetään avaamaan tietokoneella maksamista varten.

Varo liitetiedostoja

Sähköpostiviesti, jossa pyydetään avaamaan liitetiedosto, saattaa olla huijaus. Hakkerit piilottavat viruksia ja haittaohjelmia usein myös tavallisimpiin tiedostotyyppeihin, kuten pdf-tiedostoihin, joita käytetään yleisesti laskuihin tai sopimuksiin.

Jos avaat liitetiedoston tietokoneellasi, vaarana on, että aktivoit piilotetun lähdekoodin, joka saastuttaa tietokoneesi haittaohjelmalla. Se voi olla kiristysohjelma, joka lukitsee tiedostosi ja vaatii maksua niiden avaamiseksi – tai vakoiluohjelma, joka tarkkailee toimintaasi.



Hei Jussi

Tämä on automaattisesti Prime AI:lla luotu sähköpostiviesti.

Uusien GDPR-säännösten vuoksi meidän PrimeVideolla on täytynyt siirtyä uuteen asiakastietokannan järjestelmään.

Tämä tarkoittaa, että sinun on päivitettävä käyttäjätililläsi kaikki olennaiset tiedot, mukaan lukien maksutiedot.

Klikkaa alla olevaa linkkiä, niin pääset aloittamaan muutokset:

www.amazonvideos.org.net/privacy-account/

Ystävällisin terveisin

Prime Video

prime

Tämä linkki on pitkä, eikä se vastaa lähettäjän verkkotunnusta.

Viestin linkki ei vastaa verkkotunnusta

Huijareiden lähettämien viestien linkeissä ja sähköpostiosoitteissa on usein outoja verkkotunnuksia, jotka eivät vastaa yritystä, jota huijarit esittävät edustavansa.

Yllä olevassa esimerkissä hämäräperäiset huijarit esiintyvät Prime Video -suoratoistopalvelun edustajina, mutta linkki tai URL-osoite, jota pyydetään napsauttamaan on ”amazonvideos.org”, eikä se vastaa todellista verkkotunnusta, joka on ”primevideo.com”.

Jotkut hakkerit piilottavat väärennetyn sivuston linkkiin, joka näyttää oikealta verkkotunnukselta. Voit helposti tarkistaa, onko linkki oikea. Kopioi se leikepöydälle ja liitä sen tietoturvayhtiö TrendMicron verkkosivujen skannaustyökaluun. Työkalu on ladattavissa verkkosivuiltamme **kotimikro.fi/tarkista-linkit**.

Kieli on outoa

Vaikka tekoäly auttaa naamioimaan huijauksia, monille huijausviesteille on ominaista, että niissä käytettävä kieli eroaa tyylistä, jota yleensä käytämme. Huijarit yrittävät yleensä huijata samaan aikaan monia kansallisuuksia, joten käännökset ovat usein heikkoja.
Ole erityisen tarkkana, jos sähköpostiviestissä on kielioppivirheitä tai outoja muotoiluja.

(!) Tilauksesi on peruutettu

Hei Jussi

Maksusi hylättiin, koska kortin myöntäjäsi ei pystynyt vahvistamaan maksutapaasi (Visa****). Klikkaa saadaksesi lisätietoja hylättyjen maksujen osalta

Päivitä maksutapasi niin, että tilauksesi (Google One) säilyy.

PÄIVITÄ KORTILLA MAKSAMINEN

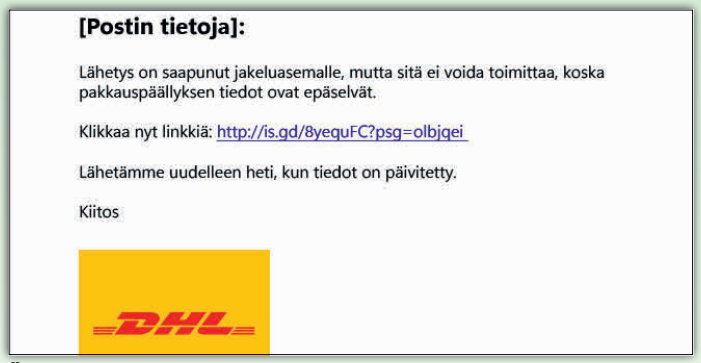
Epätavalliset sanavalinnat ja kirjoitusvirheet ovat merkkejä mahdollisesta huijausyrityksestä.

Et halua menettää pakettia

Yksi yleisimmistä huijaussähköposteista on ilmoitus pakettitoimituksesta, jonka väitetään menneen pieleen. Sähköposti, joka lähetetään usein myös tekstiviestinä, tulee yleensä yllättäen ja sisältää linkin, jota napsauttamalla voi ”korjata virheen”.

Viestissä voidaan esimerkiksi väittää, että vastaanottajan osoitteessa on ongelmia tai että paketista on peritty odottamattomia tullimaksuja, jotka on maksettava linkkiä napsauttamalla. Ellet vastaa, paketti saattaa jäädä toimittamatta.

Mikäli saat tällaisen viestin, kannattaa aina ensin tarkistaa, oletko todella tilannut hiljattain jotain toimitettavaksi kuljetusyritykseltä, jonka edustajana viestin lähettäjä esiintyy.



Älä koskaan napsauta linkkiä. Ota sen sijaan yhteyttä kuljetusyhtiöön sen virallisen verkkosivuston kautta ja selvitä syy viestiin.

Laitteesi saa tartunnan sen sijaan, että se suojattaisiin, jos teet kuten viestissä kehotetaan.

Virustorjuntaohjelmisto lähettää varoituksia viestinä

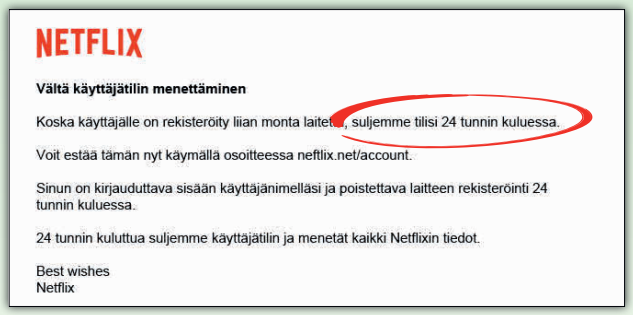
Ellet ole tilannut uutiskirjettä, kuulet harvoin sähköpostitse virustorjuntaohjelmistostasi etkä varsinkaan tietokoneeseesi kohdistuvista uhkista. Tällaiset hälytykset näkyvät suoraan laitteellasi.

Mikäli saat viestin joka näyttää tulevan virustorjuntaohjelmaltasi, voit huoletta poistaa sen. Avaa sen sijaan virustorjuntaohjelma suoraan tietokoneellasi ja suorita skannaus.

Viestissä yritetään saada toimimaan kiireellisesti

Paniikissa saattaa tehdä hätiköityjä päätöksiä. Siksi huijausviesteissä käytetään usein hälyttävää sävyä. Niissä saatetaan esimerkiksi väittää, että olet vaarassa menettää käyttäjätilin käyttöoikeuden, jos et noudata viestin ohjeita. Viesti sisältää yleensä linkin väärennetylle verkkosivustolle, joka näyttää viralliselta. Syöttämällä kirjautumistietosi sinne luovutat ne hakkereille.

Jos olet epävarma, voit aina tarkistaa asian tililtäsi yrityksen viralliselta verkkosivustolta tai avaamalla vastaavan sovelluksen ja kirjautumalla sisään. Sitten näet omin silmin, onko kaikki niin kuin pitääkin.



Saat ehkä ilmoituksen, että tililläsi on tapahtunut jotain mistä johtuen sinun on äkkiä tehtävä vaadittuja muutoksia.

Yllättäen tulevat viestit, joissa sinun väitetään voittaneen jossain kilpailussa, ovat valitettavasti useimmiten huijauksia.

Sinulta pyydetään vain vahvistusta

On aina mukavaa saada hyviä uutisia, kuten periä paljon rahaa tuntemattomalta kaukaiselta sukulaiselta tai voittaa suuri palkinto. Pienenä ehtona on, että sinun on vahvistettava jotain, ennen kuin voit lunastaa palkintosi.

Lähettäjän mukaan se voidaan tehdä nopeasti ja helposti, mutta valitettavasti tällaiset sähköpostiviestit ovat yleensä huijareilta. Kun luulet vahvistavasi palkinnon vastaanottamisen, saatat antaa huijareille pääsyn henkilökohtaisiin tietoihisi ja ajautua suuriin vaikeuksiin.

Jos saat tällaisen viestin, kannattaa ensin tarkistaa, oletko osallistunut kilpailuun. Ota tarvittaessa yhteyttä lähettäjään, mutta älä napsauta mitään viestin linkkiä.