Asiantuntija: Tekoälypetoksia on torjuttava hyväntahtoisella tekoälyllä

Turvallisuusyritys Syndisin strategiajohtaja David Jacoby kertoo KotiMikrolle, että tekoäly on jo muuttanut verkkoturvallisuutta sekä hyökkääjien että puolustajien kannalta. Tekoälyllä huijauksista voidaan tehdä paljon vakuuttavampia, mutta Jacobyn mukaan tekoäly voi myös vahvistaa puolustusta. Tekoälyä käytetään yhä enemmän verkkoliikenteen epäsäännöllisyyksien havaitsemiseen, petollisten tapahtumien huomioimiseen reaaliajassa, deepfake-sisällön havaitsemiseen ja tapahtumien käsittelyn automatisointiin. Kilpailu kiihdyttää rikollisten innovaatioita, mutta turvajärjestelmät sopeutuvat siihen, usein käyttämällä samaa teknologiaa. Tulevaisuudessa uhkien torjuminen riippuu siitä, kuinka hyvin puolustava tekoäly pysyy hyökkäävän tekoälyn edellä. Koulutus, monivaiheinen tunnistautuminen ja tekoälypohjainen reaaliaikainen uhkien havaitseminen ovat ratkaisevia tekijöitä.

David Jacoby, Syndisin strategiajohtaja

Kuva: Skorzewiak/Shutterstock.com

SUURIMMAT UHKAKUVAT

Rikolliset iskevät ensi vuonna näin

Tuleva vuosi tuo mukanaan useita haasteita turvallisuudellesi. Uusia uhkia on nousemassa esiin, ja näitä hyökkäyksiä on entistä vaikeampi havaita.

Toimittaja
Henning Rasmussen

Varhain sunnuntaiaamuna puhelimesi soi. Tunnistat heti lapsenlapsesi äänen. Hän kertoo hätääntyneenä joutuneensa liikenneonnettomuuteen, jonka seurauksena hänen nenänsä on murtunut ja kivut ovat sietämättömiä. Onnettomuuden yhteydessä poliisi on pidättänyt hänet, ja hän tarvitsee nyt nopeasti muutaman sadan euron siirron perustarpeita varten poliisin huostassa ollessaan.

Tekoälypetokset yleistyvät

Tämä kuulostaa ehkä isovanhempien pahimmalta painajaiselta, mutta itse asiassa kyseessä on huijaus. Lapsenlapsen ääni on tuotettu tekoälyn keinoin, ja puhelimen toisessa päässä on taitavia huijareita, joiden tarkoituksena on saada rahaa. Esimerkki lapsenlapsesta saattaa kuulostaa fiktiolta, mutta itse asiassa juuri näin tapahtui 73-vuotiaalle kanadalaiselle Ruth Cardille.

Hänen tarinansa on julkaistu Yhdysvalloissa ilmestyvässä tunnetussa Washington Post -sanomalehdessä. Ruth Card oli jo ehtinyt nostamaan yli kahta tuhatta euroa vastaavan summan antaakseen rahat huijareille, kun pankkivirkailija pyysi jo hieman iäkkäämmän Ruthin sivummalle ja varoitti häntä. Toinen pankissa asioiva asiakas kun oli vähän aikaa sitten joutunut aivan vastaavan huijauksen uhriksi.

Tekoäly on levinnyt nopeasti moniin palveluihin ja toimintoihin, ja tekoälyä käyttävät nyt laajasti myös huijarit, jotka voivat toteuttaa suurempia, halvempia ja vakuuttavampia huijauksia. Esimerkiksi sukulaisen äänen käyttämiseen tarvitaan vain muutaman lauseen ääninäyte, jotta tekoäly voi luoda kopion äänestä. Ääninäyte voidaan poimia vaikkapa YouTube-videosta tai muusta sosiaalisessa mediassa vapaasti saatavilla olevasta videosta. Petoksen toteuttaminen ei myöskään vaadi suurta teknistä osaamista, sillä ääniä jäljittelevä tekoäly on helposti saatavilla verkosta samoin kuin monia muita työkaluja, joita rikolliset voivat käyttää väärin. Petoksissa käytetään muun muassa ElevenLabs-palvelua. ElevenLabs käyttää tekoälyä, jolla voidaan tuottaa väärennettyjä ääniä. Sitä on kritisoitu esimerkiksi siitä, että sillä saatiin Harry Potter -näyttelijä Emma Watson siteeraamaan Adolf Hitlerin Taisteluni-kirjaa.

Huijaukset kehittyvät koko ajan

Ensi vuonna suuri haaste on, että tekoälyn avulla tehtyjen petosten tunnistaminen on entistä vaikeampaa ja erittäin uskottavat rikokset leviävät kaikille alustoille. On siis varauduttava siihen, että sinua voidaan huijata sekä puhelimitse, tekstiviesteillä että sähköpostitse. Kaikkia sähköisiä viestintävälineitä käytettäessä on noudatettava varovaisuutta, sillä huijauksia voi piillä sekä sovelluksissa, verkkosivuilla että sosiaalisen median mainoksissa. Tästä artikkelista voit lukea lisää suurimmista ja vaarallisimmista vuonna 2026 odotettavissa olevista uhkista.

Huijarit voivat käyttää ilmaisia verkkotyökaluja tai DeepFaceLab-tyyppisiä tietokoneohjelmia luodakseen väärennettyjä videoita, jotka ovat niin realistisia, että ne saavat monet uskomaan videoissa esiintyvien henkilöiden kertomuksia.

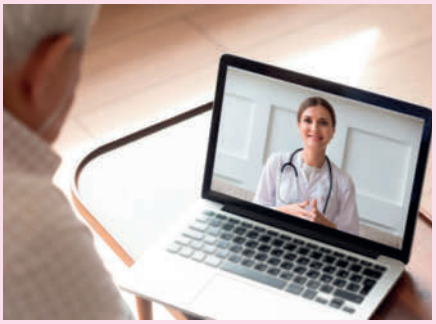
Tekoälyn muodostama uhka

Hakkerit ovat jo kauan käyttäneet tietokoneavusteista älyä luodakseen entistä uskottavampia hyökkäyksiä. Tämä vaatii mahdollisilta kohteilta uudenlaista valmistautumista.

Tekoälystä on tullut yksi hakkereiden käyttämistä menetelmistä. Sen avulla kyberrikolliset voivat räätälöidä huijausviestejä, jotka ovat sekä kieliopillisesti oikein että henkilökohtaisesti kohdistettuja. IBM:n X-Force-raportin mukaan vuonna 2024 jopa 60 prosenttia näistä tekoälyn luomista tietojenkalasteluviesteistä avataan, koska niitä on vaikea erottaa aidoista viesteistä. Toinen kasvava uhka on niin sanotun deepfake-tekniikan laaja käyttö,

PYSYTTELE TURVASSA

Saadessaan puhelun tai viestin läheiseltä perheenjäseneltä, joka kertoo olevansa jonkinlaisissa vaikeuksissa, useimpien voi olla vaikeaa pysyä rauhallisena – ja vielä vaikeampaa on huomata, että kyse on huijauksesta. Siksi monet asiantuntijat suosittelevat, että perheenjäsenet sopivat etukäteen keskenään yhteisestä salasanasta tai lauseesta, jota kukaan muu ei tunne. Näin voit helposti varmistaa, ovatko sinuun yhteyttä ottavat henkilöt oikeasti perheenjäseniä vai huijareita.



Älä usko kaikkea, mitä näet tai luet verkossa. Tunnettuja henkilöitä on käytetty hyväksi huijauksissa, joiden tarkoituksena on esimerkiksi saada sijoittamaan väärennettyyn kryptovaluuttaan. Ole myös varuillasi, jos pankki tai sairaala ottaa sinuun yhteyttä.

Useimmat huolestuvat ja ryhtyvät toimeen, jos pankista tai läheiseltä sukulaiselta tulee huolestuttava puhelu. Varmista kuitenkin ensin, että puhelimen toisessa päässä oleva henkilö on se, kuka hän väittää olevansa ennen kuin ryhdyt toimenpiteisiin.

Kuva: fizkes, Prostock-studio, Tero Vesalainen, Tada Images, Arkhipenko Olga/Shutterstock.com

Ulkoministerin ääntä jäljiteltiin tekoälyn avulla

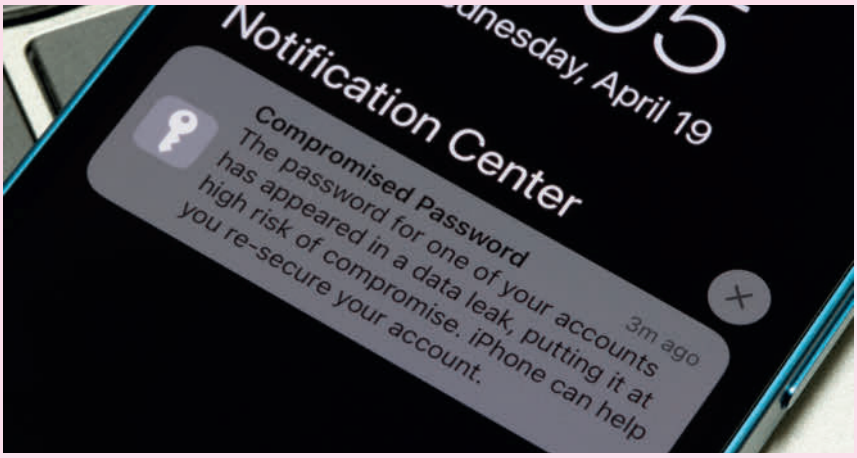
Kesällä 2025 Yhdysvaltain ulkoministeriö lähetti varoituksen maan ulkomaille lähetettyihin diplomaatteihin. Huijarit olivat käyttäneet tekoälyä luodakseen väärennettyjä äänitallenteita ulkoministeri Marco Rubion äänestä. Näitä tallenteita oli käytetty yhteydenotoissa kolmen muun maan ulkoministereihin, yhdysvaltalaiseen senaattoriin ja yhdysvaltalaiseen kuvernööriin. Tekoälyä käyttämällä huijarit olivat onnistuneet ottamaan yhteyttä eri henkilöihin Signal-palvelun kautta tekstiviesteillä ja ääniviesteillä, joissa ääni kuulosti Marco Rubiolta. Tämän jälkeen Yhdysvaltain liittovaltion poliisi FBI on varoittanut, että tämän tyyppiset tekoälyn avulla tehdyt huijaukset ovat voimakkaassa kasvussa.

jossa ääniä ja videoita voidaan jäljitellä pienimpiä yksityiskohtia myöten.

Monissa tapauksissa huijarit ovat soittaneet yrityksiin kloonatuilla äänillä ja esittäneet esimerkiksi yhtiön johtajaa tai talousosaston päällikköä. AP News -uutistoimiston julkaisemassa esimerkissä puolestaan jäljiteltiin yhdysvaltalaista poliitikkoa virkamiesten huijaamiseksi.

Tekoälyä käytetään myös uusien ohjelmistojen ja järjestelmien tietoturva-aukkojen, kuten niin sanottujen nollapäivähyökkäysten, löytämiseen aiempaa huomattavasti nopeammin. Teknisen yliopiston MIT:n tietojenkäsittelytieteen ja tekoälyn laboratorion mukaan hyökkäykset voidaan automatisoida kielimallien avulla, jolloin myös kokemattomat hakkerit voivat aiheuttaa suurta vahinkoa.

Turvallisuustottumustesi on siis muututtava kehityksen mukana.



Saat varoituksen iPhonessa, jos käyttämäsi salasana on vuotanut tietomurron yhteydessä. Voit aktivoida saman suojauksen Google-tililläsi tai suoraan tietokoneellasi HackCheck-ohjelmaa käyttämällä.

Palvelujasi hakkeroidaan

Salasanasi, korttitietosi ja yksityiset tietosi voivat päätyä rikollisten käsiin tietovuotojen yhteydessä.

Tietosi voivat vuotaa, mikäli online-palvelu, johon olet rekisteröitynyt, hakkeroidaan. Sen seurauksena käyttäjätunnuksesi, salasanasi ja joskus myös maksutietosi voidaan myydä edelleen. Analyysiyritys Surfsharkin mukaan vuonna 2023 yli 300 miljoonan tilin tiedot olivat vuotaneet.

Saatat huomata sen vasta, kun tililtäsi yhtäkkiä veloitetaan rahaa tai joku kirjautuu tilillesi sinun nimissäsi ja alkaa jakaa tai lähettää asioita sinun nimissäsi. Stanfordin yliopiston mukaan suurin osa identiteettivarkauksista tapahtuu juuri tietovuotojen seurauksena, ja asia voi koskea sinua, vaikka et olisi tehnyt itse mitään väärää.

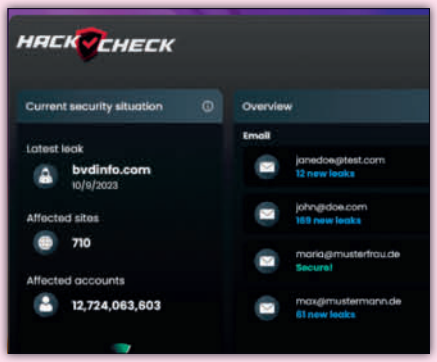
Tietosi voidaan nimittäin varastaa palveluista, joita olet käyttänyt vuosien ajan. Niitä viedään verkkokaupoista ja sähköpostijärjestelmistä, ja tietoja käytetään usein väärin pitkään ennen kuin kaappaus havaitaan.

Siksi on tärkeää, että käytät eri salasanoja kaikissa käyttämissäsi palveluissa. Ota lisäksi kaksivaiheinen tunnistautuminen käyttöön. Sen jälkeen hakkerin on paljon vaikeampi hyödyntää tietojasi.

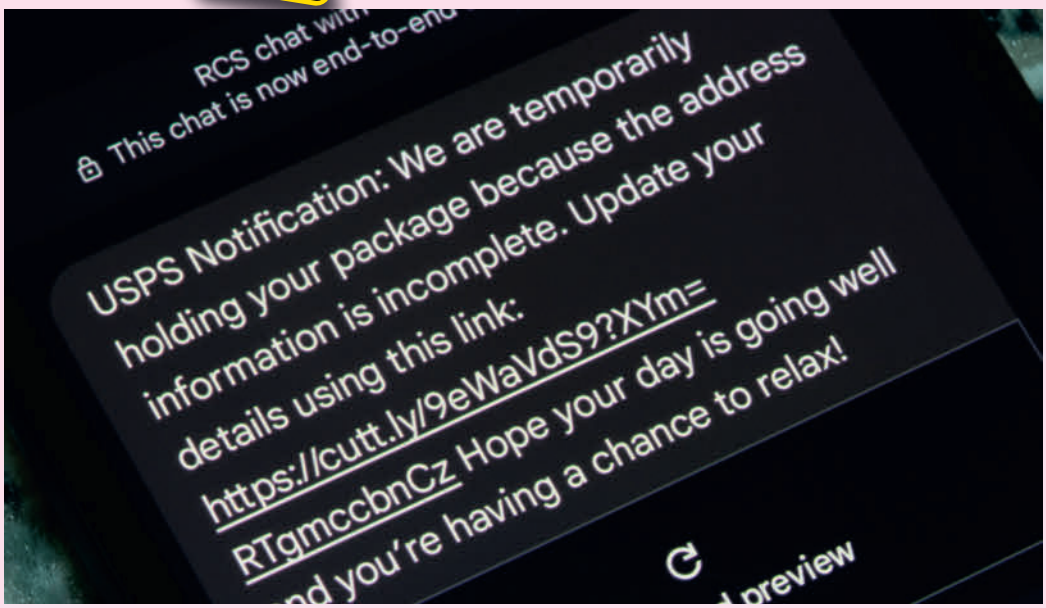
PYSYTTELE TURVASSA

Voit syöttää sähköpostiosoitteesi haveibeenpwned.com -sivustolle ja katsoa sieltä, onko osoitetta käytetty väärin tietovuotojen yhteydessä. Asentamalla Abelssoft HackCheck -ohjelman tietokoneellesi voit myös saada automaattisen ilmoituksen, jos sähköpostiosoitteesi on vuotanut. Tällöin Windowsin työpöydälle tulee varoitus, jos tilisi on vaarassa.

Lataa ohjelma: **kotimikro.fi/2520**



Voit ladata Abelssoft HackCheck -ohjelman verkkosivuiltamme. Se toimii tietokoneesi taustalla ja antaa varoituksen, jos jokin sähköpostiosoitteistasi on joutunut tietomurron kohteeksi.



Saatat saada englanninkielisen tai suomenkielisen ilmoituksen paketista, joka voidaan toimittaa perille vasta, kun olet maksanut pienen toimitusmaksun.

Rikolliset ovat taitavia huijaamaan ja harhauttamaan

Phishing eli tietojenkalastelu ja sen muoto smishing ovat nykyaikaisia huijausmenetelmiä, joilla yritetään saada sinulta tietoja uskottavan tuntuisilla viesteillä.

Rikollisista on tullut entistä ovelampia, joten aitojen ja väärennettyjen viestien erottaminen toisistaan voi olla yhä vaikeampaa. Phishing-tietojenkalastelu tapahtuu tyypillisesti sähköpostitse, kun taas smishing-kalasteluviestit tulevat puhelimeen tekstiviesteinä. Molemmilla on yksi ainoa tarkoitus eli saada sinut napsauttamaan linkkiä tai antamaan henkilökohtaisia tietojasi. Haitalliset sähköpostit ja tekstiviestit saattavat näyttää hämmentävän paljon pankkien, kuljetusyritysten tai viranomaisten lähettämiltä.

Napsauttamalla linkkiä saatat antaa huijareille mahdollisuuden nostaa rahaa maksukorteiltasi tai kirjautua käyttämiisi palveluihin.

Europolin mukaan tämäntyyppiset huijaukset kehittyvät vuosi vuodelta, ja rikolliset käyttävät nykyään usein tekoälyä muotoillakseen huijausviesteihin täydellistä suomen kieltä.

Paras tapa suojautua on noudattaa varovaisuutta. Älä koskaan napsauta tuntemattomia linkkejä. Poista viestit, joiden lähettäjää et tunne.

PYSYTTELE TURVASSA

Väärennetyt viestit eivät sinänsä vahingoita puhelinta tai tietokonetta. Vahinko syntyy vasta, jos noudatat viestien vääriä ohjeita ja esimerkiksi napsautat linkkiä tai syötät tietojasi. Siksi paras keino torjua huijauksia on poistaa väärennetyt viestit ja olla missään tapauksessa napsauttamatta viesteissä olevia linkkejä.

Saatuasi esimerkiksi kuljetusyritykseltä, pankilta tai viranomaiselta viestin, jonka epäilet olevan väärennös, älä reagoi siihen mitenkään. Varmista sen sijaan viestin aitous soittamalla tahoon, jonka väitetään olevan viestin lähettäjä.

Kuva: Gorodenkoff, Tada Images, fizkes,/Shutterstock.com

Älä pelästy vääriä varoituksia

Ponnahdusviestit ja mainokset houkuttelevat sinua tekemään hätiköityjä päätöksiä. Nämä uhkaavat viestit ovat usein huijauksia.

Sekä tietokoneelle että puhelimeen voi tulla vääriä varoituksia, joissa väitetään, että tietokoneeseen tai puhelimeen on tarttunut virus tai kiristyshaittaohjelma. Viestit näyttävät aidoilta, ja niissä käytetään usein tunnettuja logoja, jotka lisäävät niiden uskottavuutta, mutta niiden tarkoituksena on saada sinut napsauttamaan vaarallista linkkiä tai maksamaan väitetystä avusta, jota et tarvitse.

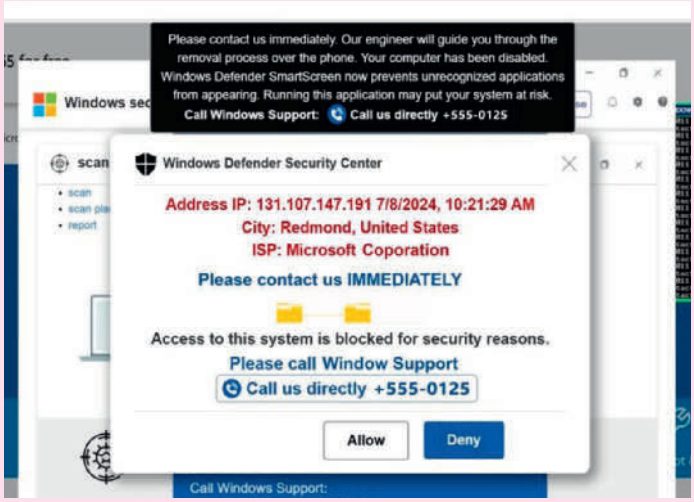
Tietokoneella näitä vääriä viestejä esiintyy usein tietyillä verkkosivustoilla tai haitallisina selainlaajennuksina, mutta joskus kyseessä voivat olla myös bannerimainokset, jotka on suunniteltu näyttämään Windowsin tai tietoturvaohjelman järjestelmäviesteiltä. Puhelimessa kyse on lähes aina viesteistä, jotka ovat peräisin epäilyttävistä sovelluksista, jotka olet itse asentanut, tai selainikkunoista, jotka toimivat puhelimen taustalla.

Europolin mukaan scareware- eli pelotteluohjelmien käyttö on lisääntynyt. Ne hyödyntävät ihmisten pelkoa tietojen tai rahan menettämisestä, ja erityisesti ikääntyneet ihmiset ovat vaarassa. Kun kohtaat hälyttävän viestin, sulje ikkuna välittömästi napsauttamatta mitään ja varmista, että tietokoneellasi on päivitetty virustorjuntaohjelma ja että myös puhelimessasi on tehokas turvallisuussovellus. Näin voit välttää huijauksen.

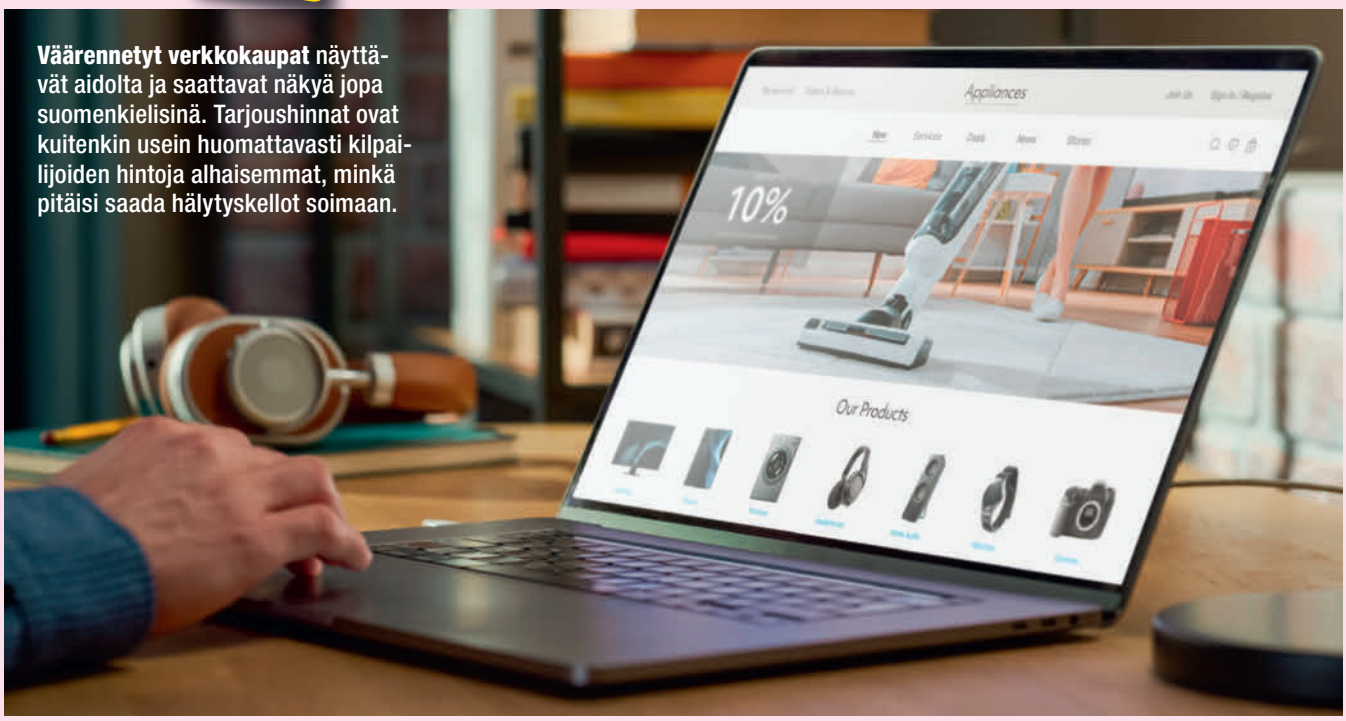
Saatat saada huolestuttavia varoituksia viruksista ja muista uhkista sekä puhelimeesi että tietokoneeseesi. Varsin usein nämä viestit ovat väärennettyjä, joten on tärkeää, että et napsauta tai napauta niitä.

PYSYTTELE TURVASSA

Koska näytöllä näkyvät varoitukset ovat vääriä, ne eivät voi vahingoittaa puhelinta tai tietokonetta. Vahinko tapahtuu vasta, jos noudatat viestien ohjeita ja napsautat linkkejä tai painikkeita. Tämä johtaa usein väärennetyille sivustoille, joilla yritetään kerätä tietojasi tai huijata rahaa. Kannattaa vain sulkea epäilyttävät viestit, jotta et vahingossa napsauta haitallisia kohtia.



Väärä varoitus näyttää tulevan Windowsin Defender-turvaohjelmasta, mutta on todellisuudessa selainikkuna, jossa on väärennetty viesti. Varoitus kannattaa vain sulkea napsauttamalla oikeassa yläkulmassa olevaa rastia tai sitten painamalla näppäimistön Alt + F4-näppäimiä.



Väärennetyt verkkokaupat näyttävät aidolta ja saattavat näkyä jopa suomenkielisinä. Tarjoushinnat ovat kuitenkin usein huomattavasti kilpailijoiden hintoja alhaisemmat, minkä pitäisi saada hälytyskellot soimaan.

Varo huijauksia verkkokaupoissa

Sinun kannattaa olla erityisen varovainen tehdessäsi ostoksia verkkokaupasta, jossa et ole aiemmin asioinut, sillä varomattomuudella saatat menettää sekä rahaa että tietoja.

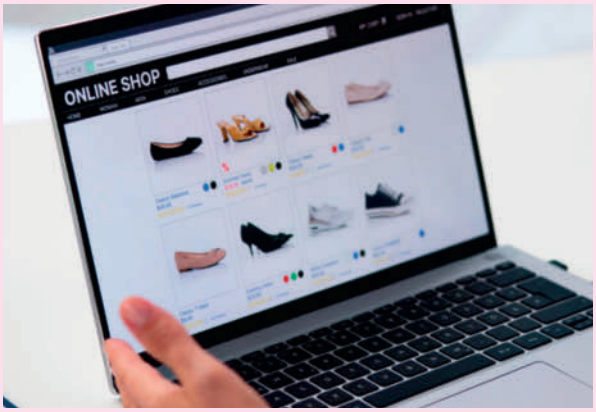
Väärennettyjen verkkokauppojen määrä on kasvanut viime vuosina, joten valitettavasti saatat joutua rikollisten myyjien kynsiin. Tämä ikävä suuntaus on saanut apua tekoälystä, jolla rikollisten on entistä helpompaa luoda aidonnäköisiä ja uskottavia verkkokauppoja. Väärennetyt verkkokaupat näyttävät täysin aidoilta, ja niissä voi olla upeita kuvia ja hienoja kuvauksia, jotka ovat usein myös suomenkielisiä. Myös Google-haussa sponsoroitujen kauppojen joukossa voi olla huijauskauppoja. Julkisivun takana toimivat huijarit, jotka haluavat napata rahasi – joko et saa tuotteita ollenkaan tai saat vain huonolaatuisia tuotteita. Kauppojen takana olevat huijarit voivat myös varastaa maksutietosi ja käyttää niitä sitten petoksiin.

Väärennetyt verkkokaupat saattavat tarjota suosittuja tuotteita tai merkkituotteita poikkeuksellisen edulliseen hintaan. Mikäli hinta vaikuttaa liian hyvältä ollakseen totta, ole erityisen varovainen ja tarkista verkkokauppa taustatietoineen huolellisesti.

Voit tarkastella sivuston yhteystietoja ja lukea arvosteluja osoitteesta **trustpilot.com**. Voit myös tarkistaa,

PYSYTTELE TURVASSA

Paras ja tehokkain suoja on oma tarkkaavaisuus ja varauksellinen suhtautuminen. Rikolliset kehittyvät jatkuvasti yhä taitavammiksi, joten sinun on oltava entistäkin valppaampi, kun näet hyvän tarjouksen tai merkkituotteita huomattavasti normaalia hintaa halvemmalla. Sivustoltamme **kotimikro.fi/2520** voit lukea seitsemän hyvää vinkkiä turvalliseen asiointiin verkkokaupoissa.



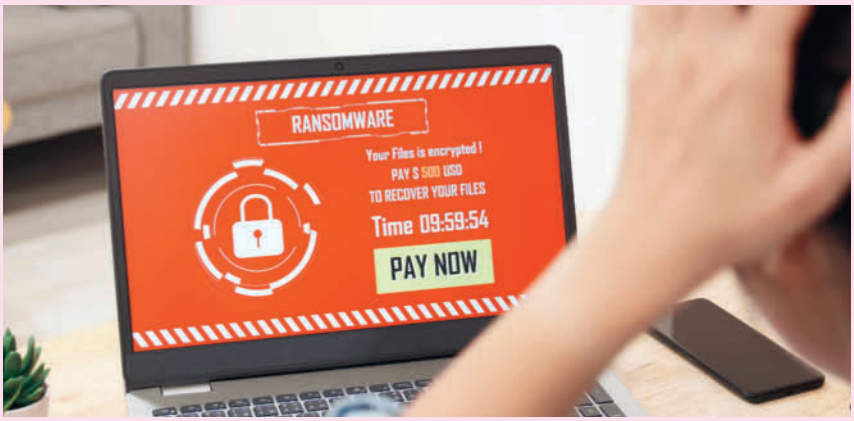
Verkkokaupan erinomaisilta vaikuttaviin tarjouksiin kannattaa suhtautua varauksella. Esimerkiksi yrityksen tunnusnumeron tulisi olla näkyvillä, jotta sen voi tarkistaa yritysrekisteristä. Kannattaa myös katsoa ensin trustpilot.com-verkkosivustolta muiden käyttäjien arvosteluja kyseisestä kaupasta.

käyttääkö sivu suojattua yhteyttä. Suojattu yhteys käyttää s-kirjaimen sisältävää https-protokollaa, eli osoite alkaa kirjainyhdistelmällä https://.

Epätäydelliset tai puutteelliset tiedot verkkokaupan takana olevasta yrityksestä ovat melko varma merkki siitä, että kyseessä on huijauskauppa. Jos sivustolla ei näy yrityksen tunnusnumeroa tai jos sivusto vaikuttaa huonosti laaditulta, kannattaa miettiä tilannetta. Mikäli epäilet yrityksen aitoutta, mutta päätät kuitenkin tehdä ostoksia kyseisestä verkkokaupasta, kannattaa käyttää luottokorttia, jotta voit tehdä ostosta valituksen pankillesi, jos kauppa osoittautuu huijaukseksi.

Aidon näköiset sandaalit olivatkin huonot kopiot

Väärennetyn verkkokaupan uhriksi joutuneet voivat ottaa yhteyttä Euroopan kuluttajakeskukseen Suomessa osoitteessa **www.ecc.fi/**. Esimerkiksi tanskalainen Mathilde kertoo vastaavan tanskalaisen kuluttajakeskuksen sivuilla, kuinka hän löysi näennäisesti tanskalaisesta verkkokaupasta houkuttelevat Birkenstock-sandaalit puoleen hintaan ja tilasi ne välittömästi. Saatuaan myöhemmin vahvistusviestin hän huomasi kuitenkin, että sandaalit oli lähetetty Kiinasta eikä Tanskasta. Kun sandaalit lopulta saapuivat hänen kotiosoitteeseensa, kävi valitettavasti nopeasti selväksi, että sandaalit eivät olleet aidot merkkituotteet, vaan kyse oli huonolaatuisista kopiotuotteista. Mathilde teki lopulta valituksen pankilleen ja sai rahansa takaisin. Tällaisiin verkkokauppoihin, joiden alkuperä on jotain aivan muuta kuin mitä ne väittävät, voi törmätä verkossa liiankin helposti.



Kiristyshaittaohjelma salaa tiedostosi ja vaatii lunnaita. Tämä on vain yksi monista haittaohjelmatyypeistä, jotka voivat tarttua tietokoneeseesi ja puhelimeesi, jos et ole varovainen.

Haittaohjelmat uhkaavat

Jos käy huono tuuri ja saat haittaohjelman tietokoneellesi tai puhelimeesi, vaarana on laitteen hidastuminen ja epävakaus tai rahojen menetys ja henkilökohtaisten tietojen varastaminen.

Haittaohjelmat voivat tarttua tietokoneeseen ja puhelimeen. Ne voivat päästä laitteisiin monin eri tavoin. Haittaohjelmia voi tulla vaarallisten sähköpostien, väärennettyjen latausten tai tartunnan saaneiden verkkosivustojen kautta.

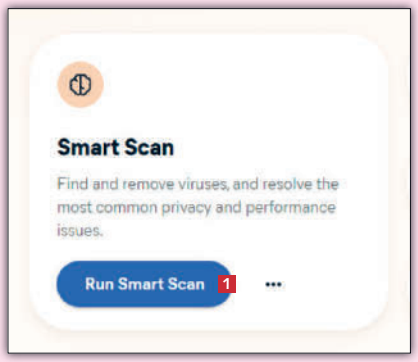
Haittaohjelma voi muun muassa varastaa henkilökohtaisia tietojasi, kuten käyttäjätunnuksia, salasanoja ja pankkitietoja, tai hidastaa tietokoneen tai puhelimen toimintaa ja heikentää niiden vakautta. Siksi kannattaa olla tarkkana, mitä sähköposteissa napsautat tai kun vierailet verkkosivuilla. Lataa ohjelmia vain luotettavista lähteistä, kuten kotimikro.fi. Pidä myös Windows ja ohjelmat ajan tasalla, jotta valmistajat voivat korjata kriittiset tietoturva-aukot, jotka voivat aiheuttaa haavoittuvuuksia. On myös tärkeää, että tietokoneellesi on asennettu toimiva virustorjuntaohjelma.

Voit ladata esimerkiksi maksuttoman Avast One Essential -virustorjuntaohjelman verkkosivuiltamme **kotimikro.fi/2520**.

PYSYTTELE TURVASSA

Tärkein toimi haittaohjelmia vastaan suojautuessa on varmistaa, että tietokoneellasi on perustason virustorjunta asennettuna. Siksi sinun tulisi ensin tarkistaa, että virustorjuntaohjelma on asennettu ja käynnissä, ja vasta sen jälkeen voit harkita lisäohjelmien hankkimista haittaohjelmien torjumiseksi. Voit ladata esimerkiksi Malwarebytes Antimalware -ohjelman verkkosivuiltamme.

Lataa ohjelmat: **kotimikro.fi/2520**



1 Lataa Avast One Essential verkkosivuiltamme ja asenna se. Käynnistä ohjelma ja valitse **Run Smart Scan** 1 tarkistaaksesi tietokoneesi perusteellisesti.