

Turvallisuudesta huolehtiminen digitaalisessa maailmassa



Mitä yleisiä uhkia on?



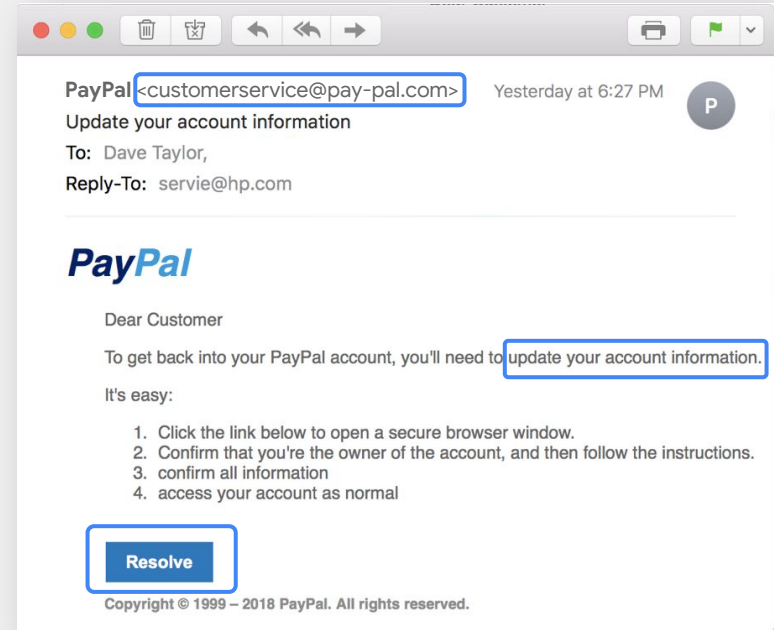
Tiedätkö, mitä **verkkourkinta (phishing)** on?

-  a Rentouttava viikonloppu järven rannalla
-  b Se on jonkinlainen tietokonevirus.
-  c Tilanne, jossa joku esiintyy hyvämaineisena yrityksenä tai henkilönä saadakseen haltuunsa henkilötietojasi
-  d Se tarkoittaa, että joku hakkeroi tietokoneeni ja seuraa toimiani.

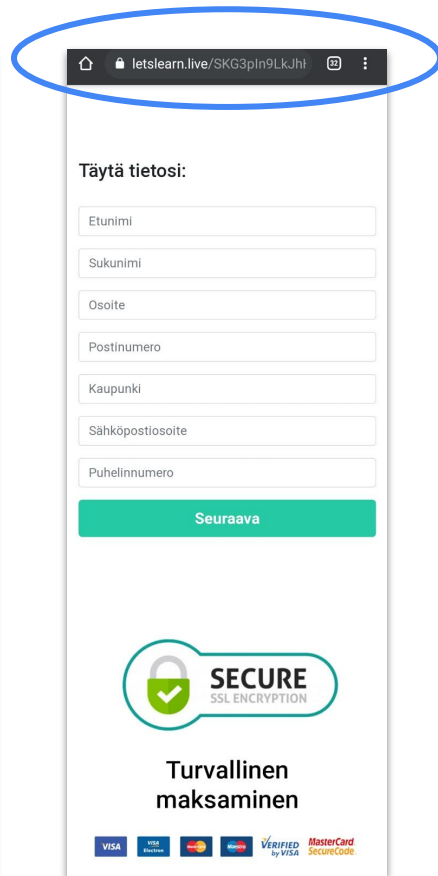
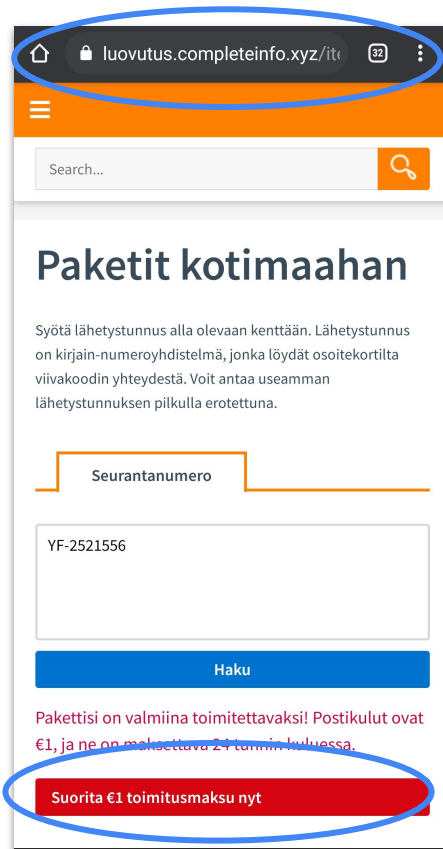
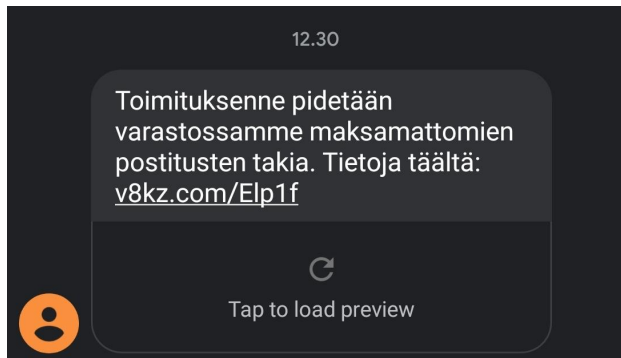
Mitä verkkourkinta on?

Verkkourkinta on [petos](#), jossa hyökkääjä esittää olevansa hyvämaineinen organisaatio tai henkilö.

Hyökkääjä käyttää urkintaan sähköpostiviestejä, tekstiviestejä, sosiaalisen median suoria viestejä tai muita tapoja jakaakseen haitallisia linkkejä tai liitetiedostoja, jotka voivat suorittaa erilaisia toimintoja, kuten [hankkia kirjautumistunnuksia](#) tai [tilitietoja](#).



Ole tarkkana - huijaukset voivat olla erittäin taitavia



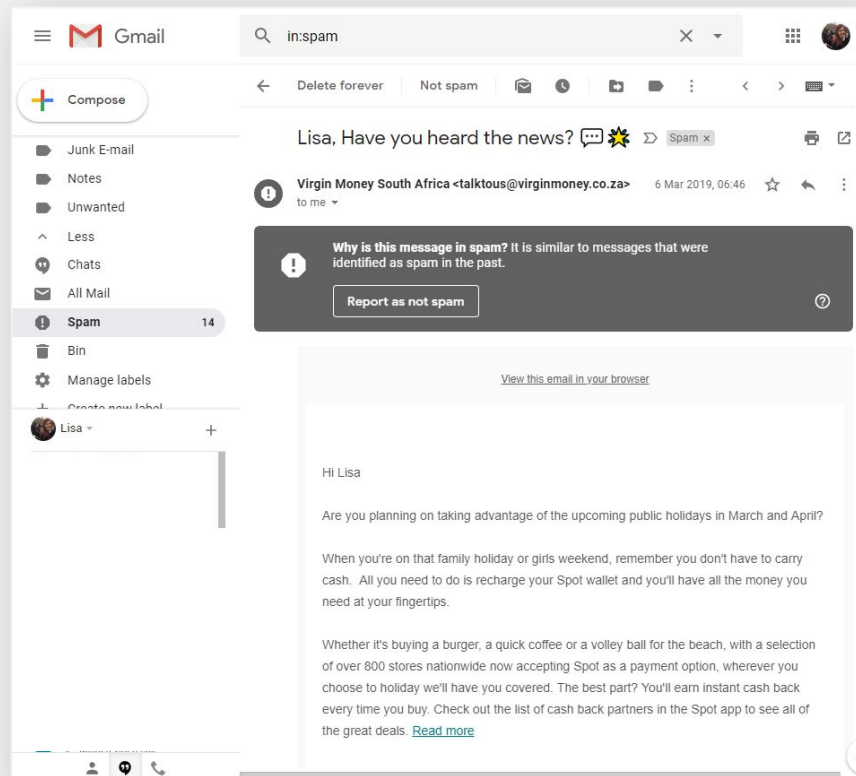
Tiedätkö, mitä **roskaposti** (spam) on?

-  a Säilykemerkki
-  b Hakkerin työväline
-  c Nimetöntä massamainontaa, jota lähetetään tilaamatta sähköpostitse
-  d Tietokonevirus

Mitä roskaposti (spam) on?

Roskaposti on suurina määrinä lähetettävää sähköpostia, jota ei ole tilattu.

Roskaposti voi olla myös epäoleellisia julkaisuja yhteisöryhmässä, sosiaalisessa mediassa tai ilmoitustauluissa.

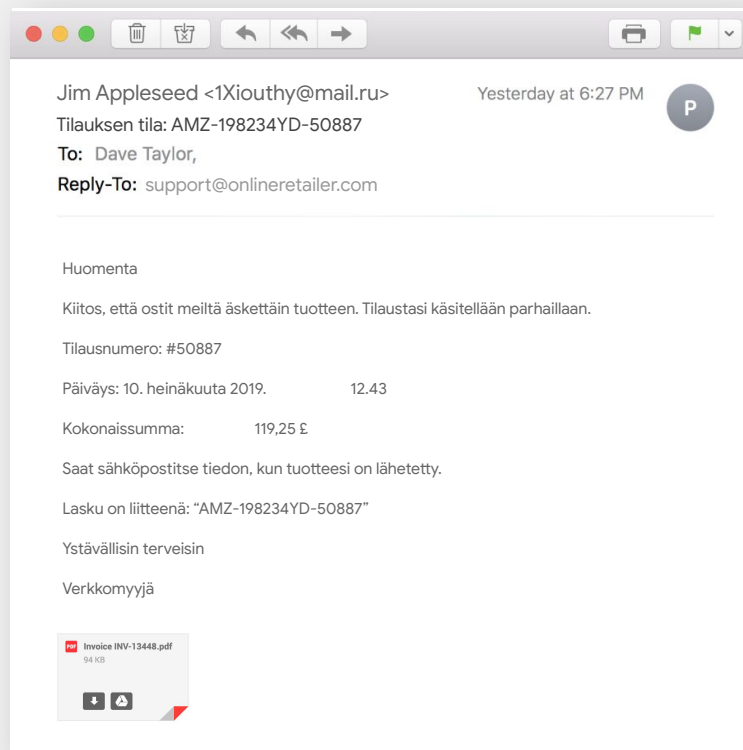


Kuinka tietokoneviruksia voidaan levittää?

-  a Sähköpostien liitetiedostoissa
-  b Verkkolatauksissa
-  c Sosiaalisen median julkaisuissa, joita klikkaat
-  d Haettaessa tietoja verkosta

Mikä on tietokonevirus?

Tietokonevirus on **koodipätkä**, joka voi kopioida itsensä ja joka yleensä vaikuttaa haitallisesti esimerkiksi vioittamalla järjestelmää tai tuhoamalla dataa.



Miksi kutsutaan sellaista henkilöä, joka hyödyntää IT-taitojaan päästäkseen luvatta käsiksi järjestelmiin tai verkostoihin, jotta saisi niistä tietoja?



Turvallisuusinsinööriksi



Hakkeriksi



Kyberturvallisuusanalyytikoksi



Tietoturvakavastavaksi

Mikä on hakkeri?

Hakkeri on henkilö, joka käyttää IT-, verkottumis- tai muita taitoja ratkaistakseen **teknisen ongelman**. Termi hakkeri voi viitata kehen tahansa ihmiseen, jolla on teknisiä taitoja, mutta usein se viittaa henkilöön, joka käyttää kykyjään päästäkseen **rikosmielessä** sisälle järjestelmiin tai verkkoihin, joita hänellä ei ole lupa käyttää.



Tiedä, mitä varoa



Selaa verkkoa turvallisesti

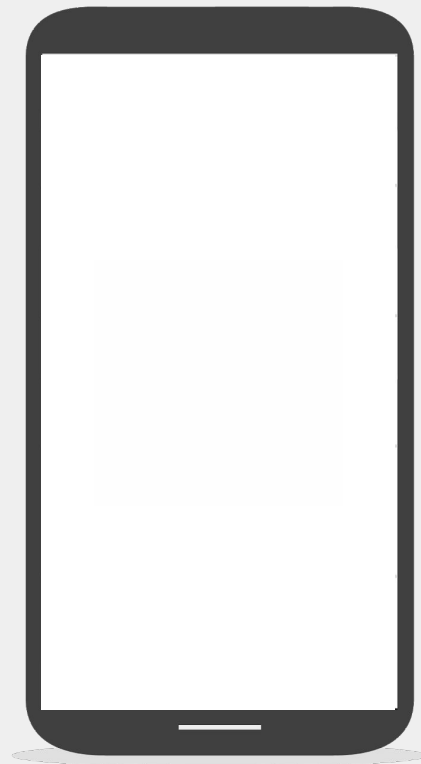
- Tarkista aina, että verkko-osoite on täydellinen eikä siinä ole outoja liitteitä
- Katso, onko käytössä riippulukko ja **https://**
- Varo sähköposti- tai tekstiviestejä, joissa pyydetään arkaluonteisia tilitietoja tai tekemään muutoksia tilillesi



Turvaa laitteesi

Pahansuovat ihmiset pääsevät nopeimmin tietoihisi ottamalla ne **suoraan** kannettavasta tietokoneestasi tai laitteestasi.

Ethän jätä laukkuasikaan vartioimatta. Riski on vähintään samansuuruinen, jos jätät digitaaliset laitteet lukitsematta tai et käytä niissä tunnuskoodia.



Vinkkejä

1

Aseta laitteeseesi salasana tai tunnuskoodi

2

Älä kerro ihmisille salasanaasi ja varmista, että se on vahva

3

Älä käytä helppoa tunnuskoodia, kuten syntymäpäivääsi

4

Muista, että kaikki kannettavat tietokoneet eivät mene lukkoon automaattisesti

5

Älä jätä laitettasi vartioimatta



Julkinen WiFi: mahtava vai riskialtis?

Joitakin yksinkertaisia vinkkejä, jos käytät julkista WiFi-verkkoa:



1 Yritä käyttää suojattua WiFi-yhteyttä, jossa on salasana tai salaus



2 Ota tiedostojen jakaminen ja verkon etsiminen pois käytöstä



3 Vältä lisäämästä henkilö- tai maksukorttitietojasi verkkosivuille

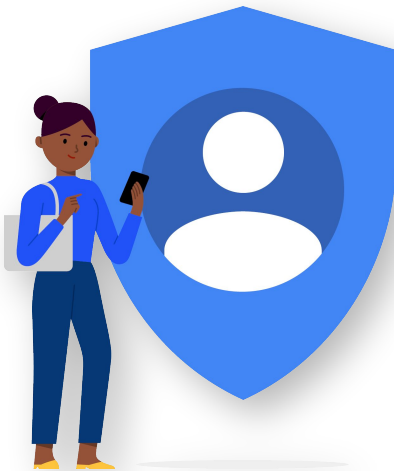


4 Vältä käyttämästä verkkopankkia tai tekemästä verkko-ostoksia



5 Älä lataa tai asenna ohjelmistoja!

Pysy verkossa turvassa



Olet varovainen myös ”oikeassa” maailmassa

1

Noudatat terveitä elämäntapoja, ettet sairastuisi

2

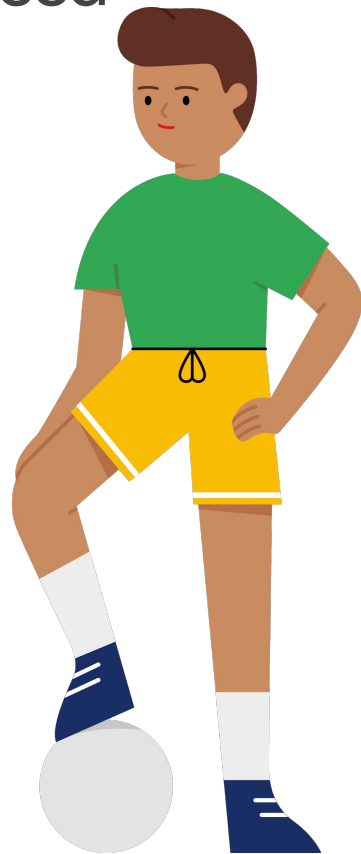
Pidät passisi turvallisessa paikassa, kun olet lomalla

3

Pidät silmällä ja vältät väärennetyjä tavaroita

4

Et kerro umpimähkään soittelijalle syntymäpäivääsi voittaaksesi palkinnon



Tutustu Googlen Turvallisuuskeskukseen



Turvallisuuskeskus

Esittely

Tietoturvasi

Tietosuoja

Perheille

Periaatteet



Koska luomme teknologiaa kaikille,
meidän täytyy myös suojella kaikkia
sen käyttäjiä.

Kun Google perustettiin, yksi sen keskeisistä ajatuksista oli käyttäjän kunnioittaminen yhtiön kaikessa toiminnassa. Internetin kehittyessä meidän on siis jatkuvasti kehitettävä tietoturvateknologiaamme ja tietosuojatyökalujamme, jotta sinä ja perheesi pysytte turvassa verkossa.

Kirjoita selaimeen:
safety.google

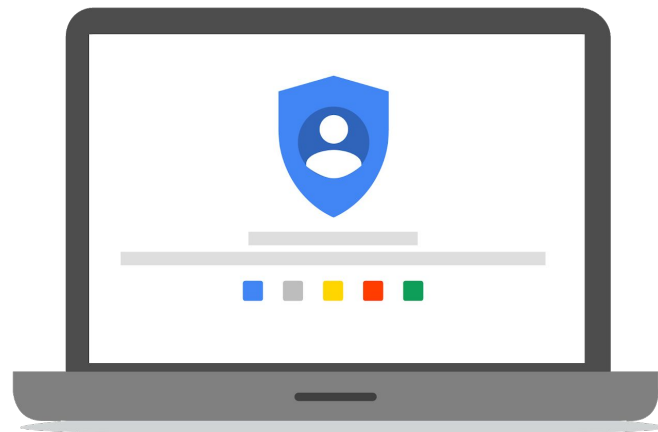


Suojaa laitteesi virustentorjuntaohjelmilla

Voit helposti suojata kannettavan tietokoneesi ja laitteesi virustentorjuntaohjelmilla

On olemassa useita ilmaisia virustentorjuntaohjelmia, jotka voivat

- 1 poistaa virukset laitteista
- 2 estää virukset ja haittaohjelmat
- 3 tarkistaa laitteen säännöllisesti



Jos jotain menee pieleen...



Mistä tiedän, onko laitteeni hakkeroitu?

- 1 Huomaat rahaa hävinneen
- 2 Viestejä pahansuovalta taholta
- 3 Ei-toivottuja lisäosia ja työkalurivejä selaimessa
- 4 Paljon ponnahdusikkunoita tai ohjelmistoja, joita et ole asentanut
- 5 Ihmiset ovat saaneet sinulta outoja julkaisuja tai pyyntöjä, joita et ole lähettänyt

**Tee Googlen
verkkourkintatesti:**

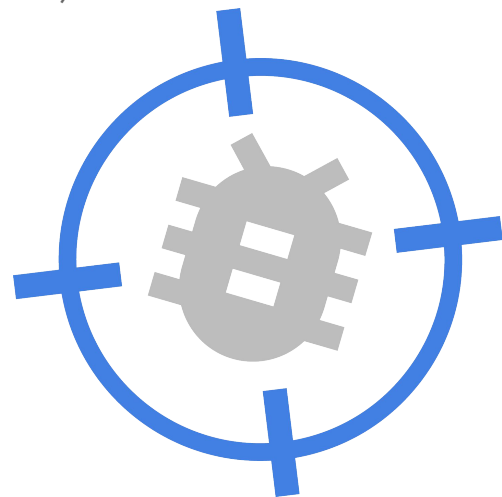
phishingquiz.withgoogle.com



Mitä tehdä, jos laitteesi on hakkeroitu?

Rauhoitu, älä mene paniikkiin ja seuraa näitä ohjeita:

- 1 Irrota laitteesi WiFi-verkosta/Ethernet-kaapelista
- 2 Tarkista laitteesi ja poista virukset
- 3 Jos tietoturva on vaarantunut tai olet epävarma tilanteesta, vaihda salasanasasi
- 4 Ota yhteyttä pankkiisi, **jos** taloudelliset tietosi ovat vaarassa



Tärkeimmät kohdat:



Ole
valpas

Käytä aina turvallisia
salasanoja ja
tunnuksia, hyödynnä
kaksivaiheista
vahvistusta

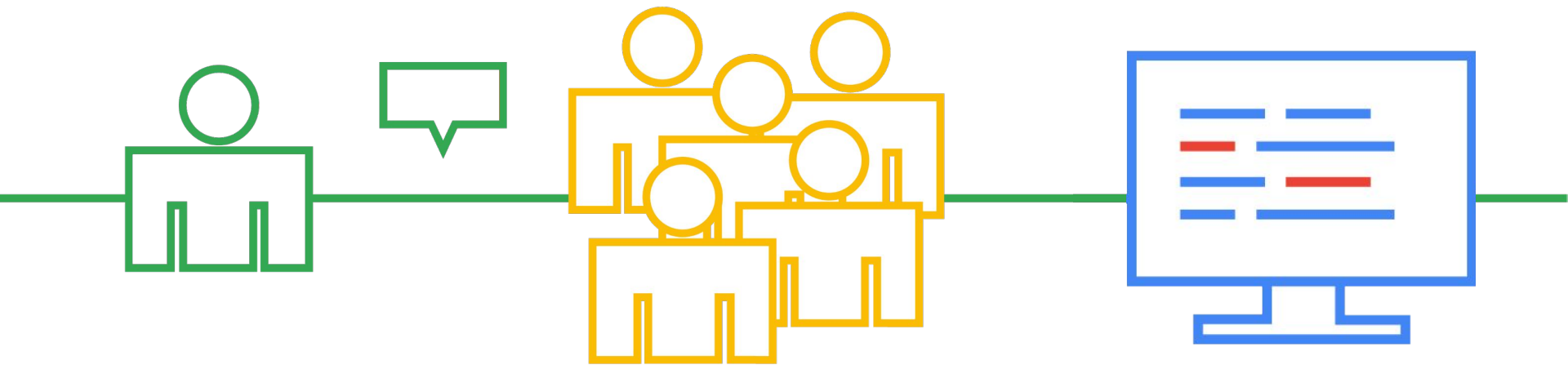
Ole
varuillasi

Varo mahdollisia
huijauksia - ole
epäileväinen

Pysy
turvassa

Ryhdy toimenpiteisiin
hakkeroinnin
estämiseksi ja varaudu

Osallistu **ilmaisiin työpajoihimme**
tai suorita **sertifikaatti verkko-opiskeluna**



Opiskele verkossa
g.co/digitalgaragefi

Kiitos!

