



Navigating Mis- and
Disinformation at an Older Age

Turvallinen digiarki

NÄIN SUOJAAT ITSESI VERKOSSA



Nordplus



Vanhustyön keskusliitto
CENTRALFÖRBUNDET FÖR DE GAMLAS VÄL RY



Tämän materiaalin avulla voidaan opettaa turvallisia toimintatapoja, joilla suojaat laitteesi, tietosi ja verkkotilisi.

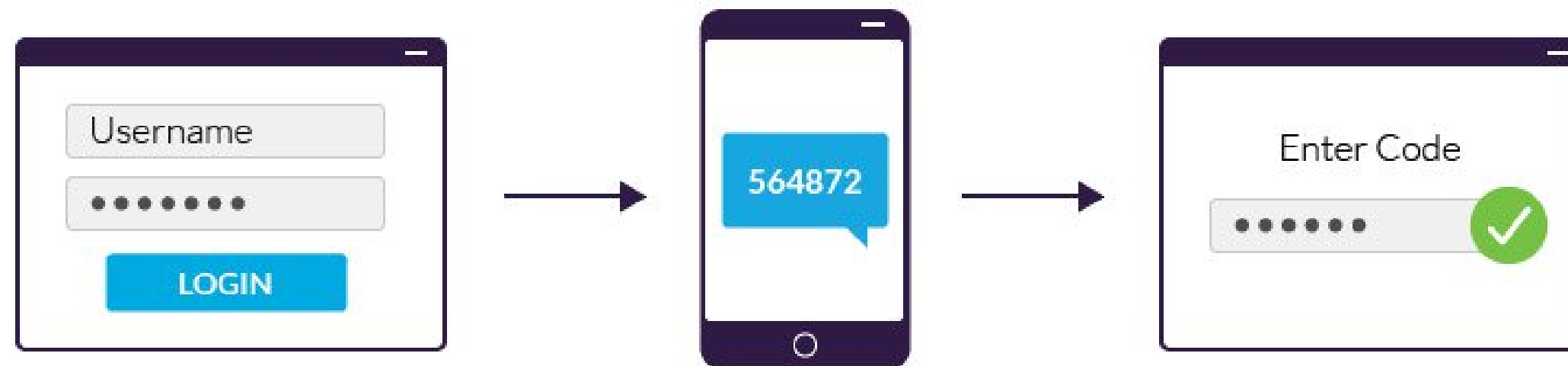
Eesitys käsittelee esimerkiksi monivaiheista tunnistautumista (MFA), salasanojen hallintaa sekä laitteiden turvallista käyttöä.

Eesityksen lopussa oleva **Muista nämä** kokoaa viisi tärkeintä digiturvavinkkiä helposti muistettavaan muotoon.

Vahvat salasana

- Käytä jokaisessa palvelussa eri ja vahvaa salasanaa. Salasanojen hallintaohjelma voi auttaa luomaan ja säilyttämään ne turvallisesti.
- Mitä pidempi salasana on, sitä turvallisempi se yleensä on.
- Hyvä salasana sisältää isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä.
- Ota käyttöön monivaiheinen tunnistautuminen (MFA) aina kun mahdollista. Tällöin kirjautuminen edellyttää salasanan lisäksi esimerkiksi puhelimeen lähetettävää vahvistuskoodia.

Kaksivaiheinen tunnistautuminen 2FA



Esimerkki mobiililaitteella käytettävästä kaksivaiheisesta tunnistautumisesta.

1. Käyttäjä kirjoittaa palveluun käyttäjätunnuksen ja salasanan
2. Käyttäjä vastaanottaa vahvistuskoodin mobiililaitteelle
3. Käyttäjä kirjoittaa vahvistuskoodin jatkaakseen kirjautumista palveluun

Ohjelmistojen päivitykset ja turvalliset lataukset

- Pidä käyttöjärjestelmä, sovellukset ja tietoturvaohjelmat ajan tasalla.
- Päivitykset sisältävät usein tärkeitä tietoturvakorjauksia.
- Lataa ohjelmia vain luotettavista lähteistä.
- Vältä tuntemattomilta verkkosivuilta ladattavia ilmaisohjelmia, sillä ne voivat sisältää haittaohjelmia.

Turvallinen toiminta verkossa



- Suhtaudu epäillen epäilyttäviin sähköposteihin, tekstiviesteihin ja linkkeihin. Älä avaa liitteitä tai klikkaa linkkejä tuntemattomilta lähettäjiltä.
- Käytä turvallisia verkkosivustoja. Kun osoite alkaa <https://>, yhteys on salattu. Tarkista lisäksi sivuston osoite ja ylläpitäjä.
- Vältä julkisten langattomien verkkojen käyttöä esimerkiksi verkkopankissa tai verkko-ostoksilla.
- Käytä eri sähköpostiosoitteita eri tarkoituksiin. Varaa ensisijainen sähköpostiosoite tärkeään asiointiin ja käytä toista osoitetta palveluihin rekisteröitymiseen.

Yksityisyysasetukset ja tietojen jakaminen



- Tarkista säännöllisesti sosiaalisen median yksityisyysasetukset ja säädä, kuka voi nähdä tietosi.
- Jaa henkilötietojasi vain silloin, kun se on tarpeellista ja luotettavan toimijan kanssa.
- Mieti ennen julkaisemista, sillä verkkoon laitettua sisältöä voi olla vaikea poistaa kokonaan.



Laitteiden suojaaminen

- Lukitse laitteesi vahvalla salasanalla, sormenjäljellä tai kasvojentunnistuksella.
- Ota käyttöön laitteen salaus, jotta tietosi pysyvät turvassa, vaikka laite katoaisi tai varastettaisiin.
- Tee tärkeistä tiedoistasi säännöllisesti varmuuskopiot esimerkiksi ulkoiselle levylle tai pilvipalveluun.
- Varmuuskopioiden avulla voit palauttaa tietosi esimerkiksi laitteen rikkoutuessa tai kyberhyökkäyksen jälkeen.



Muut suositukset



- Seuraa tietoturvaan liittyviä uutisia ja ajankohtaisia ilmiöitä.
- Tarkista säännöllisesti käyttäjätiliesi ilmoitukset mahdollisesta epäilyttävästä toiminnasta.
- Tarkista sovellusten pyytämät käyttöoikeudet ja anna vain ne oikeudet, joita sovellus todella tarvitsee.
Esimerkki: Jos taskulaskin pyytää oikeutta yhteystietoihisi tai sijaintiisi, mieti tarvitseeko se niitä oikeasti.
- VPN-yhteys (Virtual private network) antaa lisäturvaa julkisissa langattomissa verkoissa, kuten kahviloissa, hotelleissa tai lentokentillä.

Muista nämä viisi asiaa

1. Käytä vahvoja salasanoja ja eri salasanoja jokaisessa palvelussa.
2. Ota käyttöön kaksivaiheinen tunnistautuminen, kun se on tarjolla.
3. Huolehdi laitteiden ja ohjelmistojen päivityksistä.
4. Ole varovainen epäilyttävien sähköpostien, tekstiviestien ja linkkien kanssa.
5. Tee säännöllisesti varmuuskopioita.

