METSÄSTÄJÄLIITTO
KOTI KAIKILLE METSÄSTÄJILLE

Tietoturvasuositukset

Tietoturvan tärkein tavoite on suojella laitteita sekä informaatiota luvattomilta käyttäjiltä. Tietoturva on laaja käsite ja koskee meitä jokaista. Kokosimme alle lyhyesti tietoturvan perusasioita.

1. Arvioi, mikä on tärkeintä suojattavaa

Kyberriskien arviointi saattaa kuulostaa suurelta panostukselta, mutta arvokkaimman omaisuuden tunnistaminen auttaa sinua suojelemaan sitä. Listaa digitaalinen omaisuutesi tärkeysjärjestyksessä, esimerkiksi maksutiedot, valokuvat, taloustiedot, sähköiset dokumentit tai sosiaalisen median tilit.

2. Hanki virustorjuntaohjelma - ja lisäkerroksia

Ei ole olemassa yhtä ainoaa työkalua, joka voisi pysäyttää kaikki nykypäivän kyberuhat. Virustentorjuntaohjelmisto on yhä kriittinen haittaohjelmien estämisessä, mutta lisäksi tarvitset muita kerroksia vahvistamaan suojaustasi. Hanki kattava ratkaisu, joka suojaa kaikki laitteesi, yksityisyytesi ja verkkoidentiteettisi.

3. Suojaa mobiililaitteesi

Työasioiden hoitaminen hotellissa, kahvilassa, kirjastossa tai vaikkapa matkalla tuo joustoa elämään, mutta onko se turvallista? Kun käytät yritystietoja mobiililaitteilla, ne on suojattava. Hanki VPN-sovellus salaamaan yhteytesi hakkereilta ja seurannalta julkisissa Wi-Fi-verkoissa.

4. Käytä yksilöllisiä salasanoja ja kaksivaiheista tunnistautumista

Jos rikolliset saavat varastettua jonkin käyttäjätilisi salasanan, he yrittävät käyttää sitä päästäkseen muille tileillesi. Ja se usein myös onnistuu, sillä suurin osa ihmisistä käyttää samaa salasanaa useilla tileillään. Käytä eri salasanaa jokaisella tilillä, jotta rikolliset eivät voi murtautua kaikille käyttäjätileillesi yhdellä salasanalla. Tämän lisäksi salasanojenhallintaohjelma auttaa muistamaan yksilölliset salasanasi.

Toinen tapa suojata tilejäsi on ottaa käyttöön kaksivaiheinen tunnistautuminen. Siinä käytetään salasanan lisäksi toista vahvistustapaa, kuten sormenjälkeä tai tekstiviestinä lähetettävää koodia. Näin rikolliset eivät pääse tilillesi pelkällä salasanalla. Kaksivaiheinen tunnistus on ilmainen tietoturvakeino, ja se on nopea ottaa käyttöön.

(Kinturinkuja 4), PL 91
11101 Riihimäki, Finland

metsastajaliitto.fi
jahtimedia.fi

METSÄSTÄJÄLIITTO
KOTI KAIKILLE METSÄSTÄJILLE

5. Suojaa onlinetilisi ja identiteettisi

Yritysten suosimat verkkopalvelut kuten Facebook, LinkedIn, Google ja Dropbox ovat olleet mukana useissa tietomurroissa vuosien varrella. Näille tileille tallennettujen henkilötietojen menettämisellä tai tilien sulkemisilla voi olla ikäviä seurauksia.

Hyvät salasanakäytännöt, monivaiheinen tunnistautuminen ja jaettujen tunnusten välttäminen auttavat pitämään tilisi turvassa. Tarkista ilmaisella työkalulla, onko sähköpostiosoitteesi ollut osana tietovuotoa.

6. Pysäytä kiristysohjelmat

Kiristysohjelmat eli ransomware voi lukita tiedostosi tai estää pääsyn laitteellesi ja vaatia sitten suurta summaa rahaa tietojesi palauttamisesta. Älä koskaan maksa lunnaita, sillä ei ole takeita siitä, että saat käyttöoikeutesi takaisin. Ransomware voi olla tulla hyvin kalliiksi, joten on järkevää hankkia tehokas suoja sitä vastaan.

7. Varmuuskopioi ja päivitä

Varmuuskopioi tiedot säännöllisesti. Varmuuskopiot takaavat, että pääset käsiksi tietoihisi, jos joudut ransomware-kiristyksen uhriksi. Pidä laitteesi ja ohjelmistosi ajan tasalla. Asenna päivitykset heti, kun niitä on saatavilla. Ohjelmistojen haavoittuvuudet ovat tietoturva-aukkoja, jotka tarjoavat verkkorikollisille helpon tavan saastuttaa järjestelmäsi.

8. Suojaa rahasi

Pankit ovat toistuvasti verkkohuijausten kohteena. Kyberrikolliset yrittävät kalastella pankkitunnuksiasi väärennetyillä verkkosivustoilla, jotka näyttävät verkkopankkisi kirjautumissivulta. Turvaa rahasi pankkitoimintojen suojausohjelmistolla, kun maksat laskuja tai teet verkko-ostoksia yrityksellesi. Pankkitoimintojen suojaus ilmoittaa, kun sivusto on turvallinen, ja varmistaa suojatun yhteyden.

METSÄSTÄJÄLIITTO
KOTI KAIKILLE METSÄSTÄJILLE

9. Tehosta suojaustasi ja ota käyttöön turvallinen selain

Selain on väyläsi nettiin. Suurin osa verkko-ostoksista, latauksista, hauista, jne. tehdään selaimella. Siksi käytössä on hyvä olla turvallinen selain. Käytä sekä yksityisyyteen että tietoturvaan panostavaa selainta, kuten Firefoxia tai Bravea.

On myös tärkeää pitää selain ajan tasalla, jotta se on valmiina uusiin uhkiin. Sama koskee kaikkia käytössäsi olevia selainlaajennuksia ja -lisäosia.

10. Turvalliset toimintatavat

Kyberhyökkäykset alkavat usein epähuomiossa ladatusta haitallisesta liitetiedostosta tai henkilötietojen luovuttamisesta tietojenkalastelusivustolla. Näitä uhkia vastaan ei voi suojautua teknologialla, ja siksi kouluttaminen on tärkeä osa tietoturvaa. Maalaisjärki, varovaisuus, hyvät salasanakäytännöt ja harkinnan käyttäminen tärkeiden tietojen, kuten asiakastietojen, jakamisessa auttavat suojaamaan organisaatiosi tietoja ja mainetta.

Tietoturva on tärkeää, koska toimintasi vaikuttaa myös organisaatiosi ja yhteistyökumppaniesi turvallisuuteen.