VoiceLink

Tietoturvan checklist

VoiceLinkin kanssa
IT=ihanteellisesti toimiva

www.voicelink.fi

VoiceLink

Tervetuloa VoiceLinkin tietoturvaoppaaseen!

Tästä oppaasta löydät listan, jonka läpikäymällä osaat tunnistaa tietoturvariskit ja suojautua niiltä.

Kyberrikolliset ovat ottaneet kohteekseen muuttuvan työmaailman. Työnantajan on mahdollistettava töiden tekeminen missä ja milloin vain ja tämä luo uusia haasteita henkilöstön ja yrityksen laitteiston suojaamiselle, sillä kotiverkko on varsinainen kyberrikollisen unelma.

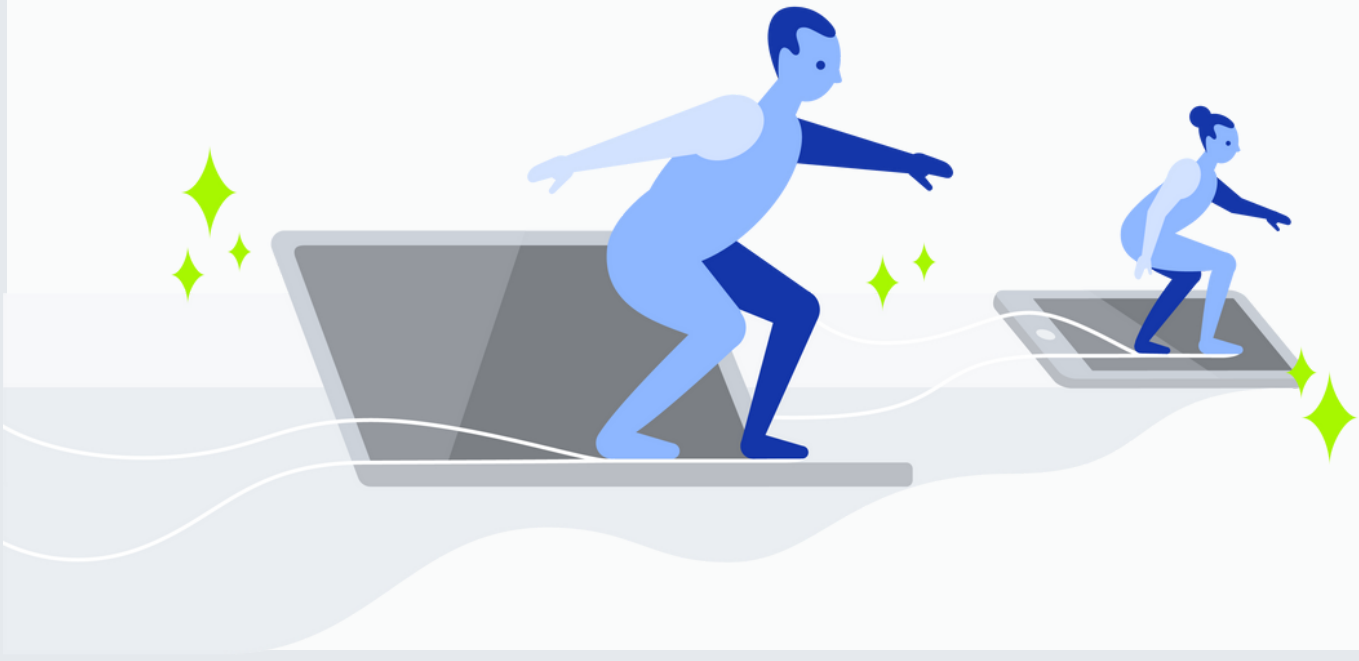
Pian tiedät mitä tietoturvan ylläpito vaatii sinulta ja yritykseltäsi, osaat varmistua yrityksesi tietoturvallisuudesta ja ryhtyä oikeisiin toimiin tietoturvanne kehittämiseksi. Käy lista rauhassa läpi ja merkitse kohdat suoritetuiksi sitä mukaa. Lista on jaettu neljään teemaan, jotta sinun on helppo tarkastella tarvittavia toimenpiteitä aihealueittain.

VoiceLink

Laitteet

Huolehdi, että laitteet ja ohjelmistot ovat ajan tasalla

- [ ] Koneissa ja matkapuhelimissa on hyvät tietoturvaohjelmistot
- [ ] Laiteinventaario on ajantasalla
- [ ] Laitteiden jatkuvat päivitykset ovat ajan tasalla
- [ ] Kriittisistä palveluista ja tiedoista on olemassa varmuuskopiot (mielellään useammassa paikassa)
- [ ] Varmuuskopioinnin palautusta testataan säännöllisesti
- [ ] Käytössä on keskitetty käyttäjäoikeuksien hallinta



VoiceLink

Kouluttaminen

Huolehdi siitä, että yrityksessä noudatetaan parhaita tietoturvakäytäntöjä

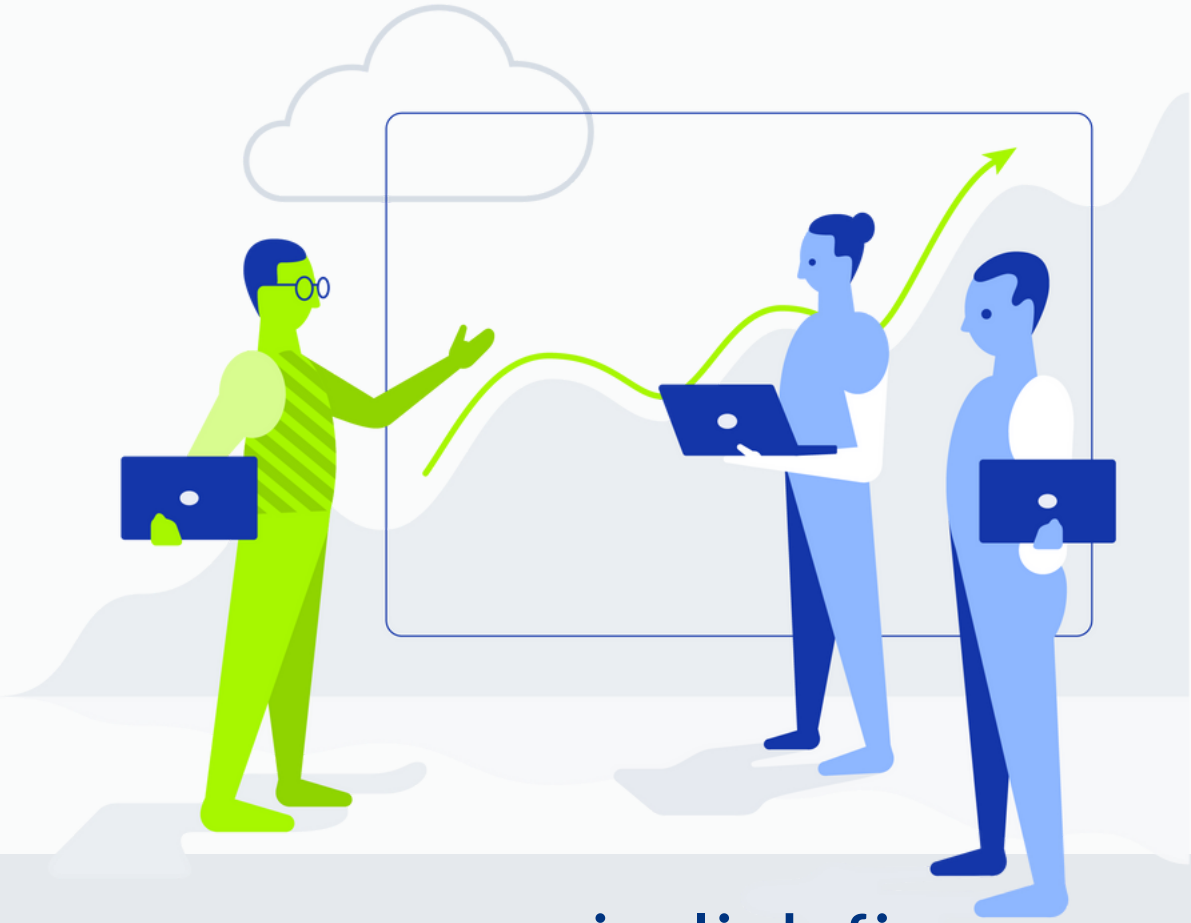
- [ ] Työntekijöillä on hyvät turvallisuusrutiinit
- [ ] Kaikilla on käytössään kaksivaiheinen tunnistautuminen
- [ ] Työntekijät ovat tietoisia tietoturvakäytännöistä
- [ ] Työntekijöiden koulutus tietoturvahyökkäyksiä vastaan
- [ ] Oletussalasanoja ei jätetä käyttöön
- [ ] Salasanat ovat riittävän pitkiä ja sisältävät erikoismerkkejä. Parhaassa tapauksessa henkilökunta hyödyntää salasanan hallintapalveluita

VoiceLink

Riskienhallinta

Tee suunnitelma ja toimintakaava kaikkiin tietoturvan eri vaiheisiin

- [ ] Huolehdi ennaltaehkäisevästä tiedon säilyttämiskäytännöstä ja varaudu myös pahimpaan mahdolliseen tilanteeseen
- [ ] Varmista, että olette laatineet toipumissuunnitelman katastrofin varalle
- [ ] Seuraa riskien tilaa ja uhkien kehittymistä säännöllisesti

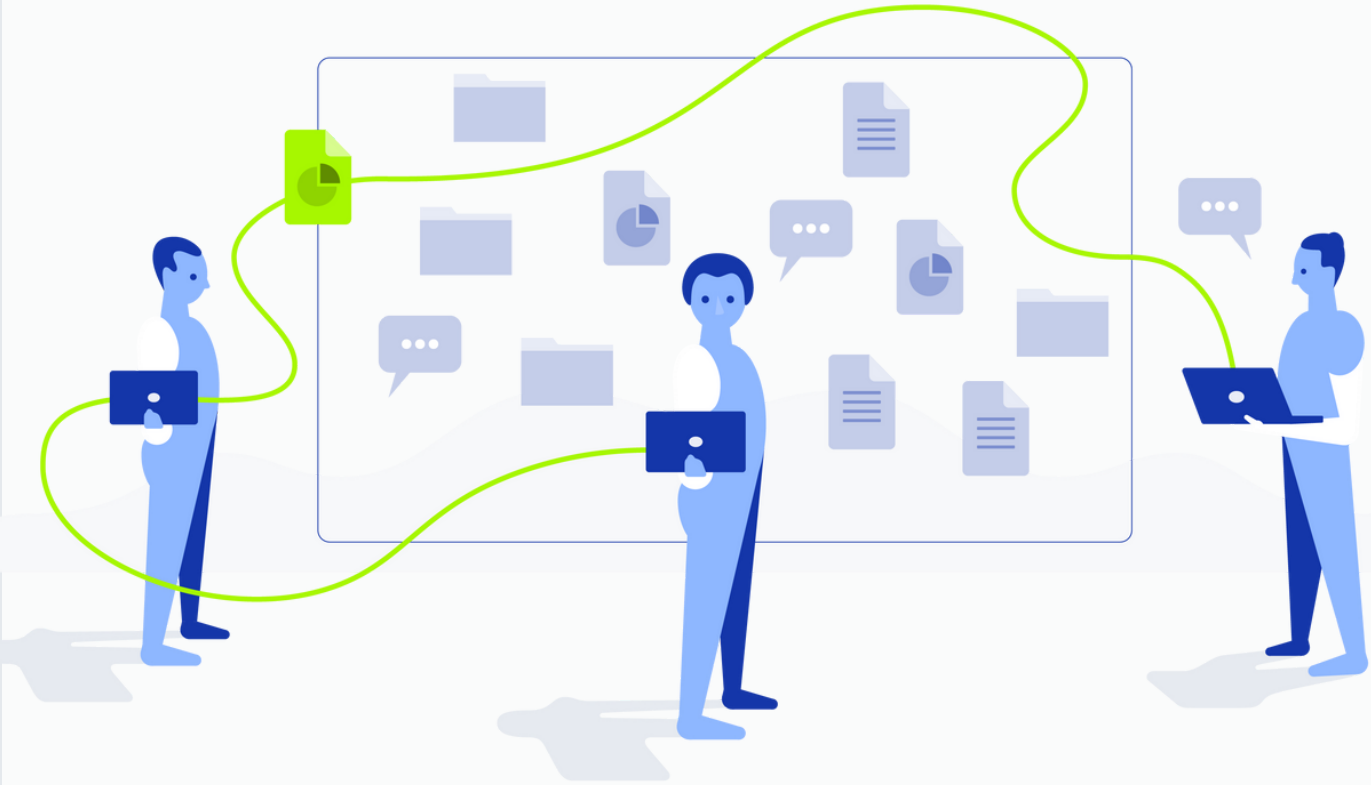


VoiceLink

Asiantuntija-verkosto

Huolehdi, että asiantuntijaverkosto on kunnossa kaikilla eri osa-alueilla. Voit minimoida tietoturvan suuret ja pienet riskit ulkoistamalla palvelun osaavalle ja luotettavalle kumppanille

- [ ] Tunnista milloin omat resurssisi eivät ole riittävät ja ota yhteyttä ulkopuoliseen kumppaniin



www.voicelink.fi

VoiceLink

Verkkoympäristöt & pilvipalvelut

Huomioi tietoturvariskit kolmella tasolla: päätelaitteella, pilvessä ja verkkoympäristössä niin toimistolla kuin työntekijöiden etätyöpisteilläkin

- [ ] Huolehdi, että IT-ympäristöllä on tarpeeksi havainnointikykyä ja hallintaa
- [ ] Varmista, että päätelaitteet ja asiakastietokannat ovat suojattuna
- [ ] Pidä huoli, että logitiedot ovat saatavilla tarpeeksi pitkälle historiaan, jotta tietomurron ilmentyessä voidaan tarkistaa, mistä, mille laitteelle ja mihin aikaan murto on tapahtunut
- [ ] Huolehdi myös datan varmuuskopioinnista sekä niiden toimivuudesta, niin pilvestä, palvelimelta, kuin päätelaitteeltakin.
- [ ] Huomioi pilvipalvelun tietoturvaominaisuudet sekä käyttäjäoikeudet.

VoiceLink

Lopuksi

Suurimpana riskinä yrityksen tietoturvassa voidaan pitää puutteellista ymmärrystä käytössä olevasta toimintaympäristöstä ja siihen kohdistuvista uhkista. Muista siis ennakoida.

Mikäli kaipaat apua, jotta saat kaikki ruudut täytettyä, otathan meihin yhteyttä.

(09) 41 500 510
myynti@voicelink.fi

Kun olet käynyt tämän listan kokonaisuudessaan läpi, olet huolehtinut yrityksesi tietoturvan perusasiat kuntoon. Jos haluat varmistaa parhaan mahdollisen tietoturvan yrityksellesi, on tämän päälle vielä paljon muuta. Ota yhteyttä, niin rakennetaan yrityksellesi kaiken kattava tietoturvasuunnitelma.