NOPSA

Nopeat Digitaaliset Kokeilut

centria

University of Applied Sciences

Tom Tuunainen

Tietoturva 2023: Kyberturvallisuus tänään ja huomenna

25.4.2023

MUUVI

Euroopan unioni
Euroopan sosiaalirahasto

Elinkeino-, liikenne- ja ympäristökeskus

KAMK • University of Applied Sciences

Yritysten muutoskumppanina

Vipuvoimaa EU:lta 2014–2020

LAPIN AMK
Lapland University of Applied Sciences

OAMK
OULUN AMMATTIKORKEAKOULU

Vipuvoimaa EU:lta 2014–2020

Euroopan unioni
Euroopan aluekehitysrahasto

POHJOIS-POHJANMAA
COUNCIL OF OULU REGION

centria ammattikorkeakoulu

OAMK
OULUN AMMATTIKORKEAKOULU

https://nopsa.eu

Tehtävä #1

(5 – 10 min.)

Jakaannutaan ryhmiin ja esittäydytään ryhmäläisille

Pohdi samalla seuraavia asioita:

- ***osaatko arvioida kuinka monta valokuvaa sinulla on puhelimessasi ja miltä tuntuisi jos ne häviäisivät?***
- ***mitä sosiaalisen median kanavia käytät ja miltä tuntusi jos joku kaappaisi sometilisi?***
- ***millaista kriittistä tietoa yrityksessäsi on ja mikä olisi pahinta mitä tiedolle voisi tapahtua?***

Miten varmistat tietoturvallisuuden?

Tietoturvan tehtävät:

1) Luottamuksellisuudella tarkoitetaan sitä, että tietoon on pääsy vain niillä henkilöillä, joille se on määritelty.
2) Eheydellä tarkoitetaan sitä, että kukaan ei ole päässyt väärentämään tietoja vaan tieto on oikeasti sitä mitä se väittää olevansa. Tiedot eivät muutu tai tuhoudu hallitsemattomasti. Tieto on juuri sitä tietoa, mitä sen on tarkoitettu olevan.
3) Saatavuudella viitataan siihen, että tieto on saatavissa jatkuvasti niille henkilöille, jotka ovat siihen oikeutettuja.
4) Todennus tarkoittaa sitä, että osapuolet voidaan tunnistaa luotettavasti.

Ennakointi ja suunnitelmallisuus parantavat tietoturvaa

Tietoturvan rakennuspalikat:

1) ennakointi
2) havainnointi
3) reagointi

Kerroksellinen suojaus on tärkeää!

- tietoa tulee suojata useissa eri pisteissä
- tärkein tavoite on supistaa hyökkäyspinta-ala niin pieneksi kuin mahdollista

Tietoturva vaatii jatkuvaa ylläpitoa ja kehittämistä

Vuonna 2022 uusia haavoittuvuuksia tunnistettiin hiukan yli 25000 kappaletta:

- lähde: National Vulnerability Database (NVD)
- https://nvd.nist.gov

Satunnaiset tietoturvaskannaukset eivät yksinään riitä tietoturvan varmistamiseksi

- tilanne voi olla täysin erilainen jo lyhyen ajan kuluessa

Mitä jokaisen yrityksen tietoturvaan tulisi sisältyä?

- Tietoturvaa on laaja ja jatkuvasti muuttuva kokonaisuus
- Siihen sisältyvät monet asiat käyttäjähallinnasta ja –ohjeista tunnistautumisen parhaimpiin käytänteisiin, sekä laitteiden ja verkkojen suojaukseen
- Useimmiten tärkeimmiksi nousevat kuitenkin:
    - turvallinen tunnistautuminen
    - päätelaitteiden suojaus
    - käyttäjähallinta
    - verkon suojaus ja palomuuri

Tehtävä #2

Salaisen aineiston hävittäminen (5 – 10 min.)

Miten hävität salaista tietoa sisältävää aineistoa?

Varmista turvallinen tunnistautuminen

- Kun turvalliset ja luotettavat käyttäjät tiedetään ja tunnistetaan, on hyökkääjien torjuminen helpompaa
  - tyypillinen ratkaisu on Active Directoryn (AD) eli toimialueiden käyttäminen
  - käytännössä Active Directory –tunnusten käyttö tarkoittaa sitä, että työntekijä kirjautuu yrityksen tunnuksilla yrityksen eri palveluihin ja järjestelmiin
- Monivaiheinen tunnistautuminen (MFA) lisää tunnistautumisen turvallisuutta
  - tämä tarkoittaa sitä, että järjestelmiin kirjautumiseen tarvitaan tunnusten lisäksi myös vahvistus esimerkiksi mobiililaitteelta
  - lisätietoa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

Ajantasaisuus auttaa

- Nykyisin suurin osa yritysten infraan kohdistuvista hyökkäyksistä ovat opportunistisia
  - tämä tarkoittaa käytännössä sitä, että hyökkääjiä kiinnostaa yhä harvemmin hyökkäyksen kohde
- Mitä ajantasaisempi yrityksen IT-infrastruktuuri on, sitä kapeammaksi hyökkäyspinta-ala käy
  - yrityksen tietoturvan ei tarvitse olla parhaalla tasolla, kunhan se on keskimääräistä korkeammalla tasolla

Muista myös käyttäjähallinta ja turvalliset verkkoyhteydet

Keskitetty käyttäjähallinta tehostaa toimintoja

- käyttäjähallinnalla mahdollistetaan tietoturvaratkaisujen keskittäminen
- keskittämisen avulla hälytykset tulevat tietoturvasta vastaavalle keskeisesti
- keskitetty hallinta mahdollistaa tarvittavien päivitysten jakelun

Verkkoyhteyksien merkitys on kiistaton

- työnteko on muuttunut paljon ja etätyön suosio vain kasvaa
  - on löydettävä keinot, joilla tarjotaan turvallinen verkkoyhteys työntekijöille paikasta riippumatta
- palomuuri estää luvattomia käyttäjiä ja haittaohjelmia käyttämästä sekä lamauttamasta yrityksen tietokoneita
- antivirustorjunta tutkii ladattuja tiedostoja sekä sivustoja
- VPN-yhteyden (Virtual Private Network) avulla työskentely onnistuu mistä tahansa
  - VPN-yhteyden varassa ollaan kuin omassa toimistoverkossa

Hyvä verkkosuunnittelu estää monet hyökkäykset

Verkkojen eriyttämisellä tarkoitetaan sitä, että kaikki yrityksen laitteet eivät yhdisty samaan verkkoon, vaan eri tarpeisiin eriytetään omat verkot

- tällä helpotetaan erityisesti asetusten ja ehtojen hallintaa, mikä parantaa verkon tietoturvaa

Toimiston verkkoa kutsutaan usein sisäverkoksi

- älykkään identiteetinhallinnan avulla sisäverkkoa voi käyttää ainoastaan yrityksen työntekijät
- VPN-yhteydellä verkkoon pääsee kuitenkin myös kotitoimistolta käsin

Vierasverkko on nimensä mukaan eriytetty vierailijoita varten

- vierailijat voivat kirjautua verkkoon, mutta sen kautta ei ole pääsyä esimerkiksi yrityksen palvelimille

Joissain toimistoympäristöissä on paljon tulostimia, skannereita tai monitoimilaitteita

- on suositeltavaa, että verkkoon yhdistettävät laitteet eivät ole kiinni yrityksen sisäverkossa

Teollisuuden alalla hyödynnetään paljon IoT-ratkaisuja

- tuotantolaitoksen koosta riippuen IoT-laitteille (Internet of Things, esineiden internet) on syytä eriyttää oma verkkonsa, joka voidaan jaotella edelleen esimerkiksi tuotantolinjoittain

Tehtävä #3

Luottamuksellinen tieto (5 – 10 min.)

Miten käsittelet luottamuksellista tietoa työpaikan ulkopuolella?

Vinkit loppukäyttäjille

Ymmärrys auttaa tunnistamaan tietoturva***uhat*** arjessa:

- salasanat ovat yksinkertaisia ja kirjoitettuna muistilapulle näppäimistön alle
- sähköpostit klikataan auki ja liitteet ladataan tietokoneelle ennen kuin sisältöön on tutustuttu
- tietokone tai puhelin yhdistetään avoimeen verkkoon esimerkiksi asiakkaalla, junassa tai hotellissa ilman VPN-suojausta

Vinkit loppukäyttäjille

Hyvä salasana:

- on vaikea ja monimutkainen, mutta helppo muistaa, kuten esimerkiksi jokin lause
- se sisältää seuraavat ominaisuudet; ison kirjaimen, pienen kirjaimen, numeron, tai erikoismerkin
- mitä pidempi salasana on, sen turvallisempi se on
- kirjoitusvirheet, murre, puhekielen ilmaisut, ja muu sanojen rikkominen vahvistavat salasanaa
- varmista, että salasana vaihdetaan riittävän usein, jos monivaiheinen tunnistautuminen ei ole käytössä
- salasanan vaihdosta ei ole mitään haittaakaan, vaikka monivaiheinen tunnistautuminen olisi käytössä
- samaa salasanaa ei tule käyttää eri palveluissa
- äläkä koskaan kerro kenellekään salasanojasi – edes viranomaiset eivät kysy niitä sinulta!

Näin käytät laitteita tietoturvallisesti:

- lukitse tietokoneesi aina kun poistut työpisteeltä
- käytä näytönsuojaa tehdessäsi töitä junassa tai kahvilassa
- älä jätä esimerkiksi puhelinta tai tietokonetta kokoustilaan tai junaan vartioimatta

Vinkit loppukäyttäjille

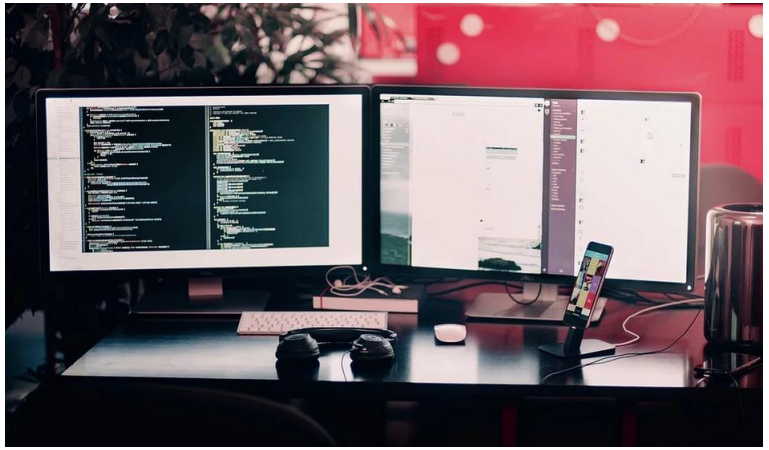
Näillä vinkeillä suojaat tietoa käytännössä:

- yrityksen asiat eivät kuulu sosiaaliseen mediaan tai lähipiirille
- kiinnitä huomiota myös siihen mitä sanot ääneen puhelimessa, tai mitä takana istuva voi lukea näytöltäsi
- harkitse tarkkaan mikä on paras tapa jakaa tietoa

Älä unohda fyysistä tietoturvaa!

- tärkeät paperiasiakirjat tulee olla lukituissa kaapeissa
- vastaanottajan henkilöllisyys kannattaa varmistaa ennen tietojen tai materiaalien luovuttamista
- nimeä kulunvalvonnalle vastuuhenkilö
- hyvä käytäntö on osoittaa vieraille selkeä tila, jossa he voivat odottaa
- fyysisen tietoturvan tärkeys: https://yle.fi/a/3-10320853

“Netiketti”



Huolehdi verkkominästäsi

- Mieti, mitä tietoja kerrot ja kenelle

Suhtaudu vastaanottamiisi viesteihin kriittisesti

- Varmistu viestin aitoudesta ja lähettäjästä
- Älä hätäile – mieti ennen kuin klikkaat

Tee päivityksistä tapa!

Tehtävä #4

Millainen on turvallinen salasana? (5 – 10 min.)

Valitse seuraavista (1-4) oikea(t) vaihtoehdot

Turvallisen salasanan peruspilarit ovat:

1) Salasana ei saa olla helposti arvattavissa
2) Salasanan pituudella on merkitystä
3) Kirjaimet, numerot ja erikoismerkit ovat osa hyvää salasanaa
4) Joka järjestelmässä käytetään eri salasanaa

Yleisimmät kyberuhat

Haittaohjelmat

- Mitä?
  - Ohjelmisto, jonka tarkoituksena on aiheuttaa harmia
- Miksi?
  - Häirintä, vahingonteko, huijaaminen…
- Kuka?
  - Uhriksi voi joutua kuka tahansa, missä tahansa

Suojautuminen

- Pidä käyttöjärjestelmät päivitettynä.
- Pidä ohjelmistot päivitettynä.
- Ota varmuuskopiot.
- Suhtaudu sähköpostiliitteisiin ja linkkeihin terveellä epäluulolla.
- Älä käytä järjestelmiä pääkäyttäjänä. Luo käyttäjille omat tilit, joilla ei ole pääkäyttäjien oikeuksia.

Yleisimmät kyberuhat

Kiristyshaittaohjelmat

- Mitä?
  - Kiristyshaittaohjelma, joka lukitsee tietokoneesi ja tiedostot, ja vaatii lunnaita
- Miksi?
  - Taloudellinen motiivi
- Kuka?
  - Pienet, keskisuuret ja suuret yritykset

Suojautuminen

- Pidä käyttöjärjestelmät päivitettynä.
- Pidä ohjelmistot päivitettynä.
- Ota varmuuskopiot.
- Suhtaudu sähköpostiliitteisiin ja linkkeihin terveellä epäluulolla.
- Älä käytä järjestelmiä pääkäyttäjänä. Luo käyttäjille omat tilit, joilla ei ole pääkäyttäjien oikeuksia.
- Tunne ympäristösi ja tarkista, ettei tarpeettomia palveluita näy julkisena internetiin.

Yleisimmät kyberuhat

Tietojenkalastelu

- Mitä?
  - Aidolta näyttävä viesti, jonka tarkoituksena on huijata viestin vastaanottajalta rahaa tai tietoa tai saada pääsy vastaanottajan järjestelmään
- Kuka?
  - Uhriksi kelpaa kuka tahansa, jolta voi saada esimerkiksi rahaa tai arvokasta tietoa – riittää, että pieni osa kohteista haksahtaa
- Missä?
  - Sähköposti, tekstiviesti, pikaviestit, sosiaalinen media…

Suojautuminen

- Jos saat linkin palveluntarjoajalta ja pyynnön kirjautua sivuille nopeasti, suosittelemme lähetetyn linkin sijaan kirjautumaan palveluntarjoajan oman verkkosivun kautta ja siten varmistamaan, onko viesti aito.
- Jos et ole varma vastaanottamasi viestin lähettäjästä tai sen sisällöstä, varmista asia esimerkiksi soittamalla viestin lähettäjälle. Katso yhteystiedot muualta kuin lähetetystä viestistä (esim. virallisilta verkkosivuilta).
- Jos epäilet linkin aitoutta, älä klikkaa.
- Ole terveen epäluuloinen. Epäilyksen tulisi herätä, jos saat pikaisen pyynnön kirjautua palveluntarjoajan sivuille, maksaa lasku tai muuttaa tilitietoja.

Tehtävä #5

Tietojenkalastelu
(5 – 10 min.)

a) **Saat sähköpostiisi viestin, jossa sinua pyydetään kirjautumaan verkkopankkiisi viestissä olevan linkin kautta. Miten toimit?**

b) **Mitä keinoja sinulla on selvittää, onko verkkosivu aito vai tietojenkalastelusivu?**

Suojautumiskeinoja

Automaattiset päivitykset

- Mitä?
  - Ohjelmiston päivitykset
- Miksi?
  - Turvallisemmin, nopeammin, paremmin…
- Milloin?
  - Päivittäin

Huom!

Kun ohjelmisto tai laite tulee elinkaarensa päähän (End-Of-Life, EOL), valmistaja ei enää tuota siihen päivityksiä. Tässä vaiheessa laite tai ohjelmisto pitää vaihtaa päivitettävään versioon tai täysin uuteen, jonka kehitystä ja turvallisuutta valmistaja tukee. Elinkaari kannattaa huomioida jo hankintahetkellä.

Suojautumiskeinoja

Automaattiset varmuuskopiot

- Mitä?
  - Tietojen varmuuskopiot
- Miksi?
  - Turvallisemmin ja nopeammin
- Milloin?
  - Tänään ja joka ikinen päivä!

Huom!

Joillakin toimialoilla on velvoite säilyttää dokumentaatioita tietty aika (esimerkiksi verotus- ja laskutustiedot). Tarkistathan tietojen tallennusajan oman yrityksesi osalta ja huomioit asian varmuuskopioita tehdessä, jotta tarvittava tieto on tallessa ja palautettavissa.

Suojautumiskeinoja

Monivaiheinen tunnistautuminen

- Mitä?
  - Turvallisuustoimenpide, joka vaatii kahden tai useamman todennustekijän käytön, jotta kirjautuminen järjestelmään on mahdollista
- Miksi?
  - Parantaa turvallisuutta
- Missä?
  - Ota monivaiheinen tunnistautuminen käyttöön kirjautuessasi tärkeisiin yrityksen sisäisiin ja ulkoisiin palveluihin

Yhä parempi suoja

Käyttöoikeuksien hallinta

- Mitä?
  - Käyttö- ja pääsyoikeuksien hallinta: Kenellä on oikeus päästä yrityksen käyttämissä järjestelmissä olevaan tietoon?
- Miksi?
  - Riskien vähentäminen – henkilöstö, jolla ei ole tarvetta tietoon, ei tarvitse pääsyoikeutta siihen
- Kuka?
  - Vähemmän oikeuden periaate

Tarkista

- Rajoita pääkäyttäjäoikeuksia. Pääkäyttäjäoikeuksia ei tarvita päivittäisessä työssä.
- Älä jaa kirjautumistietoja.
- Älä käytä yhteiskäyttötunnuksia.
- Muista poistaa käyttöoikeudet henkilöiltä, joilla ei ole niille enää tarvetta, kuten entiset työntekijät ja palveluntarjoajat.

Yhä parempi suoja

Salalause/salasanalause

- Mitä?
  - Pidempi on parempi tässäkin tapauksessa – käytä salasanan sijaan salalausetta
- Miksi?
  - Turvallisuus parantuu käyttämällä salalausetta
- Missä?
  - Kaikissa palveluissa, joissa salasanaa käytetään

Hyvä salalause on:

- **Yksilöllinen** – Samaa salalausetta ei käytetä useissa eri palveluissa eikä sitä ole otettu tunnetusta kappaleesta tai sanonnasta.
- **Pitkä** – Salalause on vaikeampia arvata, jos siinä käytetään yksittäisten sanojen sijaan kokonaista lausetta.
- **Monimutkainen** – Salalause sisältää erikokoisia kirjaimia, sekä erikoismerkkejä ja numeroita.
- **Helppo muistaa** – Salalause on helpompi muistaa, jos sen taustalle kehittää itselleen helposti muistettavan systeemin tai käytä apuna salasanojen hallintaohjelmaa.

Yhä parempi suoja

Harjoitus- ja koulutustoiminta

- Mitä?
  - Tarjoa henkilöstölle koulutusta, jotta he osaavat toimia työssään tietoturvallisesti
- Miksi?
  - Työntekijällä on tärkeä rooli yrityksen tietoturvan edistämisessä
- Milloin?
  - Tee kyberturvallisuudesta jokapäiväistä ja harjoittele säännöllisesti

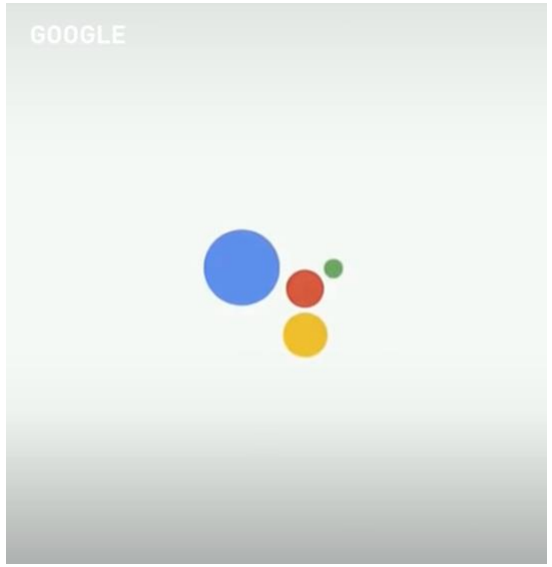
Huom!

Harjoittelua on jo sekin, että yritystä uhkaavia tilanteita mietitään vaikka kahvikupin äärellä.

Tehtävä #6

Vastuu
(5 – 10 min.)

Kuka on vastuussa tietoturvan toteutumisesta työpaikallasi?



Google's AI Assistant Can Now Make Real Phone Calls

https://www.youtube.com/watch?v=JvbHu_bVa_g

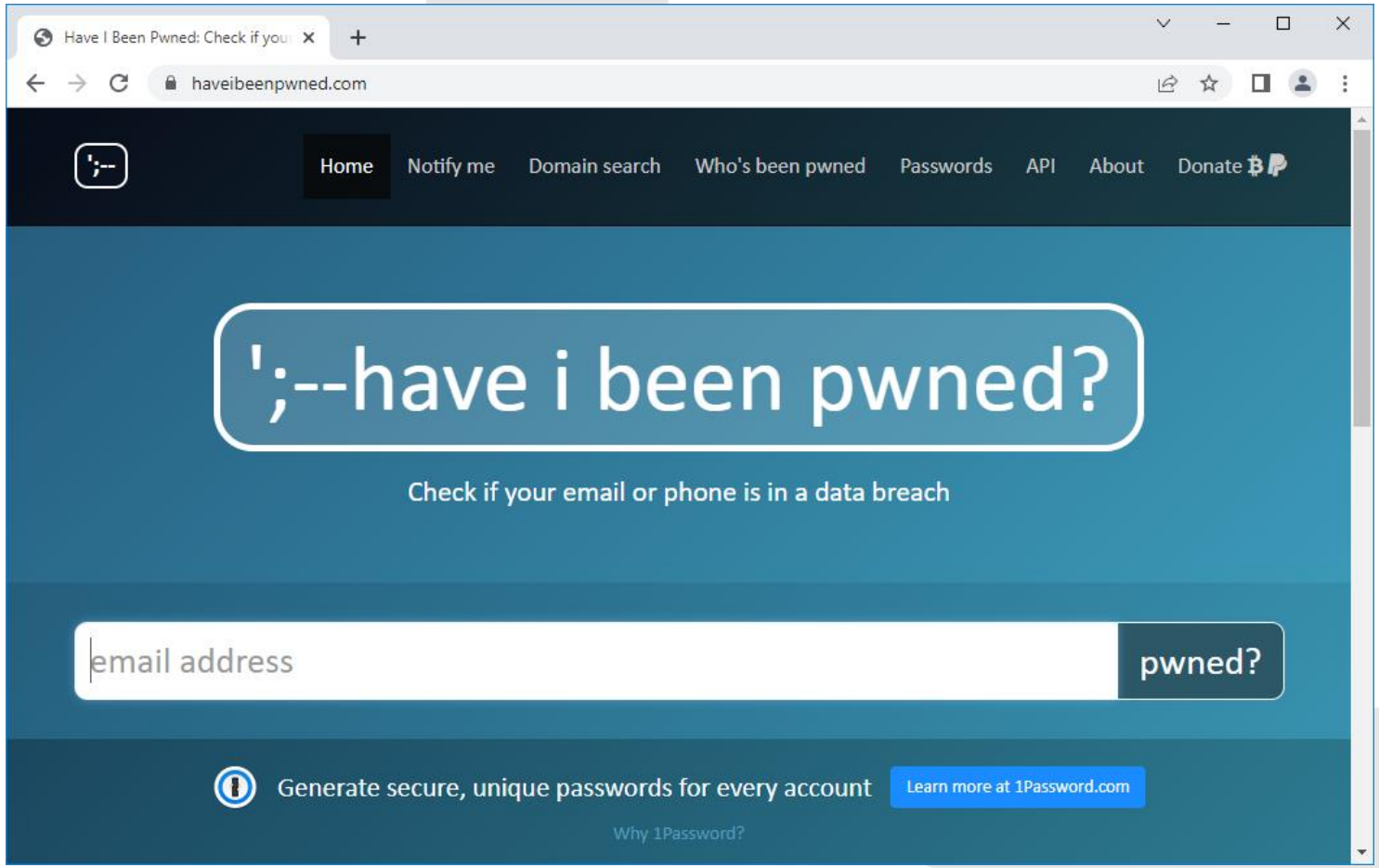
‘Deep Fakes’ Are Becoming More Realistic Thanks To New Technology

https://www.youtube.com/watch?v=CDMVaQOvtxU

CHATGPT

OpenAI

Onko tilisi hakkeroitu?



https://haveibeenpwned.com

Tom Tuunainen
Centria SecuLab
seculab@centria.fi
https://seculab.fi