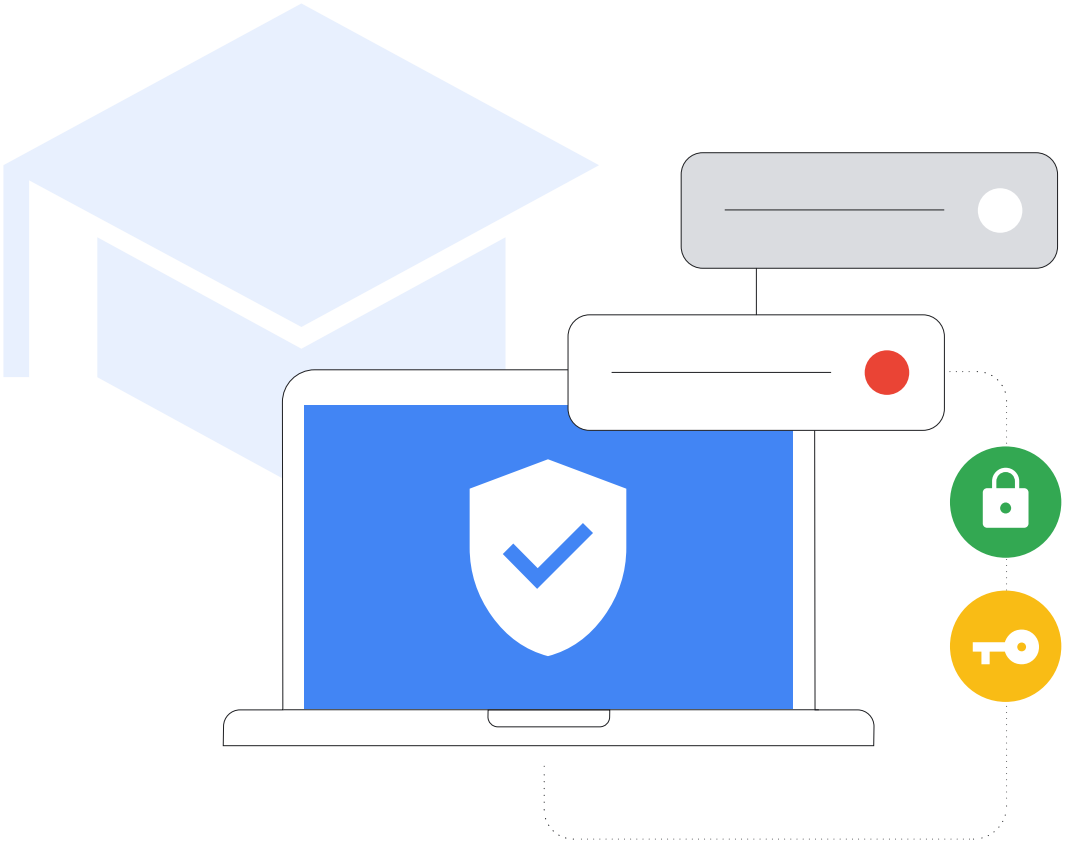
Google for Education

Perusopetuksen kyberturvallisuusopas

Päivitetty elokuussa 2023



Safer with Google

Kyberturvallisuusohjeet perus-ja keskiasteen koulutukseen

Yhteenveto

Kuten CISAn Protecting Our Future -raportissa korostetaan, perus- ja keskiasteen oppilaitosten on tärkeää investoida kyberturvallisuuteen oppilaiden, perheiden, opettajien ja muun henkilökunnan sekä yhteisön jäsenten turvallisuuden varmistamiseksi. Tämä dokumentti sisältää ohjeita ja parhaita käytäntöjä, joiden avulla oppilaitosten IT-järjestelmänvalvojat voivat ottaa käyttöön ja määrittää laitteistoja ja ohjelmistoja perus- ja keskiasteen oppilaitoksissa kyberturvallisuuden vahvistamiseksi. Dokumentissa sekä kuvataan parhaita käytäntöjä että annetaan Googlen tuotteisiin ja palveluihin liittyviä erityisohjeita. Google haluaa järjestää maailman tiedot ja tuoda ne kaikkien saataville. Tämä periaate ohjaa työtämme Google for Education -tiimissä kehittäessämme opetukseen ja oppimiseen sopivia työkaluja. Olemme koonneet tähän oppaaseen kokemuksiamme tästä työstä.

Kerromme tietoturvan parhaista käytännöistä aihepiireittäin ja tarkastelemme yksityiskohtaisesti järjestelmien käyttöönotto-, määritys- ja riskienhallintastrategioita. Esittelemme myös Googlen lähestymistavan kyberturvallisuuteen palveluidemme ja erityisesti opetustyökalujen kannalta. Vaikka tässä oppaassa kerrotaan yksityiskohtaisia ohjeita tuotteesta tai palvelusta riippumatta, olemme sitä mieltä, että tuotteemme tarjoavat erinomaista suojaa välittömiä hyökkäyksiä vastaan.

Riski

Oppilaitokset ovat kyberhyökkäysten ykköskohteita. Haitalliset toimijat pyrkivät käyttämään oppilaitosten datavoittoisia ympäristöjä oman edun saavuttamiseksi. 46 prosenttia oppilaitoksista, jotka eivät vielä ole joutuneet hyökkäysten kohteeksi, uskoo jossain vaiheessa valikoituvansa kohteeksi, koska kiristysohjelmahyökkäyksistä on tullut entistä kehittyneempiä – ja siten myös hankalampia estää. 42 prosenttia näistä oppilaitoksista on sitä mieltä, että kiristysohjelmat ovat niin yleisiä, että hyökkäys on vain ajan kysymys. Vuonna 2020 oppilaitokset joutuivat siirtymään nopeasti etäopetukseen. Nopean muutoksen vuoksi kyberturvallisuus jäi puutteelliseksi, mikä puolestaan altisti oppilaitoksia hyökkäyksille.

Ratkaisu

Nämä hyökkäykset ovat vältettävissä. Riskiä ei voida täysin eliminoida minkään teknologian avulla, mutta opetusala ja koulutusteknologiatoimittajat voivat tehdä yhteistyötä parhaiden käytäntöjen omaksumiseksi. Turvallisuutta korostavan ja kattavan lähestymistavan avulla riskiä on mahdollista pienentää. Asianmukaisilla varotoimilla ja käytännöillä on mahdollista suojata käyttäjät ja laitteet sekä varmistaa datan yksityisyys. Kaikki tämä auttaa oppilaitoksia hallitsemaan riskiä ja välttämään hyökkäykset.

Tärkeimmät suositukset:

- **KÄYTÄ SUOJATTUA TODENNUSTA.** Näin voit pitää arkaluontoiset tiedot turvassa, suojata sähköpostit, tiedostot ja muun sisällön sekä estää valtuuttamattomia käyttäjiä pääsemästä oppilaitoksen järjestelmiin. Hyödynnä parhaita käytäntöjä käyttäjien todennukseen. Näihin lukeutuvat muun muassa vahvat salasanat ja kaksivaiheinen vahvistus, avainkoodit sekä mahdollisuuksien mukaan myös salasanojen ylläpitotyökalut erityisesti IT-järjestelmänvalvojilla ja henkilökunnalla, jotka käsittelevät arkaluontoisia tietoja.
- **KÄYTÄ ASIANMUKAISIA SUOJAUSASETUKSIA.** Oikeanlaisten asetusten avulla voit pitää käyttäjät, datan ja ympäristön turvassa. Googlen tuotteet suunnitellaan aina turvallisuutta silmällä pitäen. Siksi on tärkeää, että järjestelmänvalvojat myös määrittävät verkot ja järjestelmät sekä käyttävät niitä asianmukaisesti turvallisuuden varmistamiseksi. Oppilaitosten tietoturva voidaan taata noudattamalla Zero Trust -mallia ja pienimmän oikeuden periaatetta. Käyttäjillä tulee olla pääsy vain ohjelmistoihin, dataan, sovelluksiin ja järjestelmiin, joita he tarvitsevat tehdäkseen työnsä tehokkaasti.
- **PÄIVITÄ JÄRJESTELMÄT JA PIDÄ NE AJAN TASALLA.** Näin voit varmistaa, että käyttäjät on suojattu uusimmilta uhkilta. Käytä nykystandardien mukaisia käyttöjärjestelmiä ja selaimia ja varmista, että käyttäjien kaikilla laitteilla on uusimmat ohjelmistoversiot (tai hyväksytyt pitkäaikaiset vakaat versiot) ja että ne päivittyvät automaattisesti. Voit parantaa suojausta siirtymällä turvallisempiin ratkaisuihin, kuten Chromebookeihin. ChromeOS-laitteilla ei ole koskaan havaittu kiristysohjelmia.
- **HYÖDYNNÄ REAALIAIKAISIA ILMOITUS- JA VALVONTAJÄRJESTELMIÄ.** Näin voit parantaa suojausta ja torjua mahdolliset ongelmat nopeasti. Voit käyttää ensisijaisen yhteiskäyttö- ja viestintäohjelmistosi (esim. Google Workspace for Educationin) sisäänrakennettuja ominaisuuksia tai ottaa käyttöön erillisiä tietoturvatapahtumien kirjaus- ja valvontaratkaisuja. Varmista tapahtumien kattava valvonta oppilaitoksen verkossa, laitteilla ja sovelluksissa sekä käyttäjien ja datan osalta. Seuraa kirjautumista tileille, tiedostonjakoa, sähköpostien määrää (erityisesti tietojenkalasteluyrityksiä ja haittaohjelmia), laitetapahtumia sekä asetusten muutoksia. Pidä ilmoitus- ja valvontaratkaisusi ajan tasalla, jotta saat ilmoituksia uhkista, kriittisistä tapahtumista ja järjestelmän muutoksista.
- **KOULUTA OPETTAJIA, HENKILÖKUNTAA JA OPPILAITA.** Näin he oppivat käyttämään laitteita ja ohjelmistoja turvallisesti, tunnistamaan mahdollisia uhkia ja ilmoittamaan niistä sekä jakamaan dataa asianmukaisesti. Kaikki tämä auttaa suojautumaan yleisimpiä hyökkäyksiä vastaan. Oppilaitokset ja koulupiirit voivat luoda brändättyjä oppimateriaaleja valmiiden maksuttomien materiaalien ohella. Näin ne saavat kattavan työkalupakin oppilaitosten tarpeisiin.

[1] https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Suositukset Googlen tuotteiden käyttäjille:

Google Workspace for Educationin ja Chromebookien kaltaisilla Googlen tuotteilla voit parantaa oppilaitoksesi kyberturvallisuutta ja helpottaa suositusten käyttöönottoa. Yhdessä nämä kaikki tarjoavat kattavan ratkaisun käyttäjien yksityisyyden suojaamiseen ja luokkansa parhaan suojauksen oppilaitoksellesi.

Nämä strategiat ja jäljempänä kuvatut ohjeet luovat erinomaisen perustan tietoturvalle perus- ja keskiasteen oppilaitoksissa.

Googlen lähestymistapa opetukseen ja oppimiseen

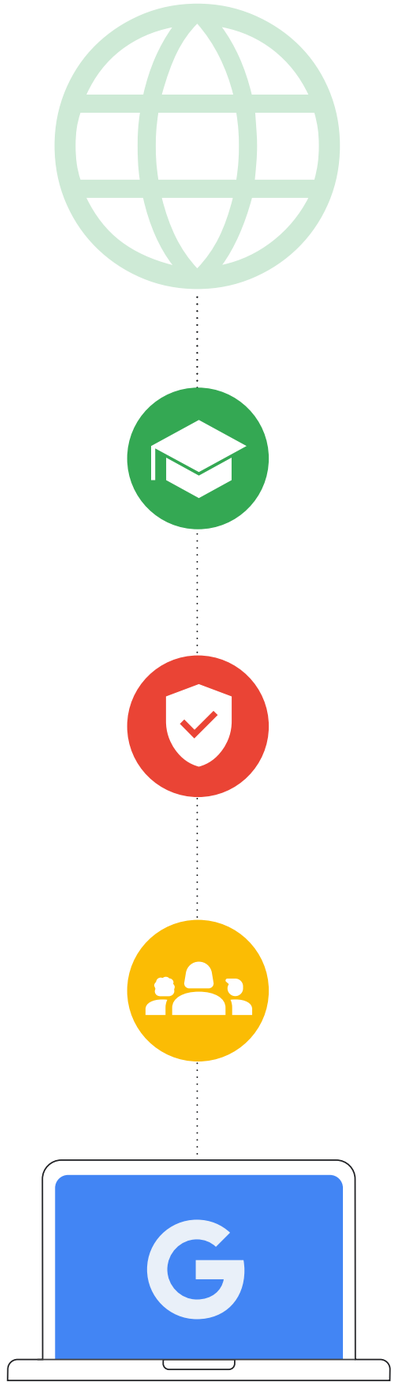
Google haluaa järjestää maailman tiedot ja tuoda ne kaikkien saataville. Tämä periaate on totta myös koulutussektorilla. Google for Education -tiimissä toimimme tämän periaatteen mukaisesti kehittämällä Chromebookien ja Google Classroomin kaltaisia työkaluja, joiden avulla oppilaat ja opettajat voivat helposti ja turvallisesti luoda, jakaa ja järjestää sisältöä sekä käyttää opetusmateriaaleja ja verkkotyökaluja.

Oppilaitokset ansaitsevat teknologioita, jotka ovat oletusarvoisesti turvallisia ja jotka on suunniteltu yksityisyyttä silmällä pitäen. Lisäksi ne antavat päätösvallan sinulle sekä sisältävät luotettavaa sisältöä ja dataa. Chromebookien ja Google Workspace for Educationin kaltaisten tuotteiden avulla oppilaitokset saavat luokkansa parhaan tietoturvan, joka noudattaa eri alueiden tiukkoja koulutusstandardeja. IT-järjestelmänvalvojat voivat tarkastella ja valvoa dataa ja tietoturvakäytäntöjä kattavasti ja sujuvasti. Oppilaat voivat keskittyä oppimiseen entistä turvallisemmassa digitaalisessa ympäristössä, joka sisältää ikäryhmälle sopivaa sisältöä ja auttaa estämään roskasisältöä ja kyberuhkia.

Valmiit turva- ja hallintaominaisuudet, tiukkojen yksityisyysstandardien noudattaminen ja ennakoivat suojaustyökalut ovat meille ensiarvoisen tärkeitä. Kaikkien näiden avulla voimme varmistaa, että oppiminen on turvallista kaikille. ChromeOS-laitteiden avulla voidaan vähentää oppilaitoksiin kohdistuvia uhkia. Ne ovat myös paras keino suojautua kiristysohjelmia vastaan, jotka ovat suurin oppilaitoksiin kohdistuva uhka. Chromebookeihin kohdistetut kiristysohjelmahyökkäykset eivät ole koskaan onnistuneet.

Google Workspace for Education on yksi maailman suosituimmista ja turvallisimmista työkalupaketeista viestintään ja tiimityöskentelyyn. Viimeisestä osiosta saat lisätietoja siitä, miten näiden ratkaisujen avulla voidaan varmistaa tässä kuvattujen suositusten mukainen kyberturvallisuus.

Tämä artikkeli on jaettu kahteen osioon. Ensimmäisessä osiossa kerrotaan yleisiä ohjeita perus- ja keskiasteen oppilaitosten tietoturvaan ja käytäntöihin tuotteesta riippumatta. Toisessa osiossa on ohjeita oppilaitoksille, jotka käyttävät Google for Education -tuotteita, kuten Google Workspace for Educationia ja Chromebookeja. Molemmissa osioissa kuvatut tiedot auttavat oppilaitostasi ja oppilaitasi toimimaan turvallisesti verkossa.



Johdanto

Perus- ja keskiasteen oppilaitokset – niin niiden laitteet kuin verkotkin – ovat äärimmäisen alttiita kyberhyökkäyksille. On hyvin tärkeää, että oppilaitoksilla on käytössään paras mahdollinen ratkaisu, jonka avulla voidaan suojata oppilaita sekä estää datan, palvelujen ja materiaalien häviäminen, sillä hyökkäysten seurauksena menetetään aikaa ja rahaa. (Lähde)

Tämän oppaan tarkoituksena on edistää kyberturvallisuuden parhaita käytäntöjä järjestelmänvalvojien keskuudessa ja oppilaitoksen järjestelmissä, jotta oppimisympäristöistä voidaan tehdä entistä turvallisempia. Näiden parhaiden käytäntöjen avulla perus- ja keskiasteen oppilaitokset voivat lieventää tai estää niiden järjestelmiin kohdistuvia vakavia ja kalliiksi koituvia kyberhyökkäyksiä ja pitää oppilaat, perheet, opettajat ja henkilökunta turvassa.

Oppilaitoksiin kohdistuu entistä useammin yhä vakavampia kyberhyökkäyksiä. K-12 Cybersecurity Resource Centerin mukaan opetusalan organisaatioihin Yhdysvaltojen kaikissa 50 osavaltiossa kohdistui yli 1 300 julkisesti ilmoitettua kyberturvallisuuden ongelmatapausta vuosina 2016–2021. Tämän päivän opetuksen järjestäjien on varmistettava oppilaiden, opettajien ja henkilökunnan datan ja henkilökohtaisten tietojen sekä oppilaitoksen järjestelmien ja tietojen turvallisuus. Tehtävä on haastava, koska koulutusalan on perinteisesti ollut vaikeampi pitää kyberturvallisuus ajan tasalla muihin sektoreihin verrattuna.

Kyberhyökkäykset (kuten kiristysohjelmat, tietojenkalastelu ja haittaohjelmat) voivat johtaa henkilökohtaisten tunnistetietojen vaarantumiseen suuressa mittakaavassa. Hyökkäyksistä voi aiheutua lunnasmaksuja ja keskeytyksiä opetukseen ja oppilaitoksen muihin toimintoihin. Maksettujen kiristysmaksujen keskiarvo on viisinkertaistunut 812 260 dollariin vuodesta 2020. Äskettäisen kiristysohjelmahyökkäyksen seurauksena koko oppilaitos kaikkine järjestelmineen jouduttiin sulkemaan, minkä vaikutukset heijastuivat koko yhteisöön, koska oppilaat eivät voineet mennä kouluun useisiin päiviin. Koska keinot ja rahoitus ovat rajalliset, perus- ja keskiasteen oppilaitokset ovat edelleen näiden hyökkäysten ensisijaisia kohteita, ellei kyberturvallisuuden parantamiseen panosteta tehokkaammin.

Kyberturvallisuuteen voidaan parhaiten vaikuttaa viestinnän, yhteistyön ja kumppanuuden avulla. Tämä dokumentti on laadittu käyttämällä apuna Googlen turvallisuus- ja suojausvinkkejä, National Institute for Standards and Technologyn (NIST) Cybersecurity Framework -viitekehystä sekä CISAn vuoden 2023 työkalupakkia ja suosituksia perus- ja keskiasteen oppilaitosten kyberturvallisuuteen liittyen. Kaikki nämä ovat kyberturvallisuuden käytäntöjen laajasti hyväksyttyjä lähteitä. Dokumentissa annetaan yleisiä ohjeita, joita IT-järjestelmänvalvojien kannattaa seurata tai harkita. Kerromme myös joistakin Googlen omista käytännöistä ja tuotteitamme koskevista ohjeista sekä muiden yritysten tarjoamista tietoturvavinkeistä -ja palveluista. Järjestelmänvalvojien kannattaa tutustua yritysten tarjoamaan tietoturvaohjeistukseen ja noudattaa niiden uusimpia käytäntöjä. Palvelusta vastaava yritys osaa parhaiten kertoa omista tuotteistaan ja niihin mahdollisesti tehdyistä muutoksista.

Ennen kuin sovellat alla kuvattuja suosituksia käytännössä, huomioi myös seuraavat näkökohdat:

Huomioitavaa

1. **Oppilaiden suojaaminen.**
   Oppilaitosten tarpeet vaihtelevat, ja joissakin organisaatioissa saatetaan tarvita lisätoimia tietoturvan ja yksityisyyden suojaamiseen. Monissa koulutusteknologian työkaluissa on ikään perustuvia pääsyoikeusasetuksia, joilla voidaan esimerkiksi rajoittaa sopimatonta sisältöä tai varmistaa sijainnin ja yhteystietojen yksityisyys.
2. **Tallennettavan datan tyyppi.**
   Jos tallennat arkaluontoisia tietoja, data kannattaa salata tai tallentaa eri paikkaan.
3. **Millaisia laitteita käytät ja millainen käyttöönottomalli sinulla on.**
   Laitteiden ja sovellusten päivitys tulee automatisoida, jotta turvallisuus on paras mahdollinen, data voidaan suojata ja tilit voidaan eristää. Näin varmistetaan, että käyttäjillä on pääsy vain omiin tietoihinsa.
4. **Oppilaitoksen, koulupiirin ja alueen käytännöt.**
   Oppilaitoksessasi saattaa olla erityisiä teknologian käyttöön liittyviä käytäntöjä. Sinun on huolehdittava, että kaikki suojaustoimet määritetään näiden käytäntöjen mukaisesti.

Päivittäin
100 miljoonaa
tietojenkalasteluyritystä jää Gmailin haaviin.

Viikoittain
300,000
vaarallista sivustoa pysähtyy Googlen tunnistukseen.

Päivittäin
74 miljoonaa
käyttäjää saa apua Google Salasanoista.

Vuosittain
700 miljoonaa
ihmistä suojaa toimintansa tietoturvatarkistuksen avulla.

Tietoturvaan liittyvät yleiset ohjeet

Suojatun todennuksen käyttäminen

Suojatun todennuksen on oltava prioriteettilistan kärjessä oppilaitoksissa ja muissa organisaatioissa. Vuoden 2022 viimeisellä neljänneksellä heikosti suojatut tai ilman tunnuksia käytettävät tilit aiheuttivat 48 prosenttia kaikista tietomurroista. Toimimalla tärkeimpien suositusten mukaisesti voidaan todentaa käyttäjien henkilöllisyys ja varmistaa, että käyttäjillä on pääsy vain roolin edellyttämiin tietoihin.

IT-järjestelmänvalvojien kannattaa ottaa käyttöön kaksivaiheinen vahvistus ja siirtyä salasanattomaan todennukseen (kuten avainkoodeihin) mahdollisuuksien mukaan erityisesti silloin, kun käyttäjät käyttävät oppilaitoksen järjestelmiä etänä. Kaksivaiheinen vahvistus parantaa verkossa käytettävien tilien suojausta, jolloin niihin on vaikeampi hakkeroitua.

Perus- ja keskiasteen oppilaitoksissa käytetään nykyisin monia eri laitteita ja käyttöönottomalleja, joten teknisten ympäristöjen kirjo on laaja. Tilien ja laitteiden turvallisuus vaihtelee käyttäjäroolien ja -tyyppien sekä alempana listattujen parhaiden käytäntöjen mukaan: IT-järjestelmänvalvojat, opettajat ja muu opetushenkilöstö sekä vanhemmat oppilaat käyttävät määritettyjä laitteita ja nuoremmilla oppilailla on puolestaan käytössä jaetut laitteet. Alla on kuvattu kullekin ryhmälle tarkoitetut erityiset suositukset.

Todennusmenetelmiä on erilaisia, ja ne sopivat hyvin useimpiin tilanteisiin:

- **Vahvat salasanat**
  Kehota käyttäjiä luomaan omat salasanat ensimmäisen sisäänkirjautumisen yhteydessä ja aseta salasanoille pituus- ja monimutkaisuusvaatimuksia. Salasanat ovat turvallisempia, kun ne ovat pitkiä ja niissä käytetään merkkejä monipuolisesti. Käyttäjiltä ei saa edellyttää salasanan vaihtamista säännöllisesti, sillä se saattaa johtaa yksinkertaisempien salasanojen käyttämiseen ja vähäpätöisten muutosten tekemiseen (salasanasta muutetaan esimerkiksi vain yksi merkki).
- **Kaksivaiheinen vahvistus**
  Kaksivaiheinen vahvistus parantaa tilien suojausta. Tähän käytetään yleensä suojausavainta tai puhelimella olevaa sovellusta, joka luo kertakäyttöisen vahvistuskoodin. Vaikka kaksivaiheinen vahvistus parantaa tilien turvallisuutta, järjestelmänvalvojien ei tule lähettää vahvistuskoodeja tekstiviestillä tai kertoa niitä puhelussa, sillä hyökkäyksiä tehdään myös puhelinnumeroiden perusteella.
- **Salasanaton todennus**
  Avainkoodit ovat turvallisempi ja kätevämpi vaihtoehto salasanoille. Käyttäjät voivat kirjautua sovelluksiin ja sivustoille PIN-koodilla, kuviolla, biometrisellä anturilla (esimerkiksi sormenjälki- tai kasvojentunnistuksella) tai suojausavaimen painikkeella, jolloin heidän ei tarvitse muistaa ja hallinnoida salasanoja. Vaikka näitä ei välttämättä voida soveltaa opetussektorin kaikissa tilanteissa, ne korvaavat perinteiset todennusmenetelmät yhä enenevässä määrin, nopeuttavat kirjautumista ja parantavat turvallisuutta. Avainkoodit suojaavat käyttäjiä tietojenkalasteluyrityksiltä, sillä koodit toimivat vain rekisteröidyillä sivustoilla ja rekisteröidyissä sovelluksissa.
- **Kertakirjautuminen (SSO)**
  Kertakirjautumisen avulla käyttäjät voivat käyttää monia eri sovelluksia ja sivustoja samoilla tunnuksilla. Kun käyttäjien tarvitsee muistaa vain yhdet tunnukset, heidän ei yleensä tarvitse kirjoittaa niitä muistiin. Oppilaitosten ei näin ollen tarvitse hallinnoida monia eri käyttäjätunnuksia, mikä tuo säästöjä myös IT-tuen kuluihin. Google Workspace for Education tukee kertakirjautumista natiivisti, joten käyttäjät voivat kirjautua kolmannen osapuolen sovelluksiin Google-tilillään tai kirjautua Google-tililleen muun palveluntarjoajan tunnuksilla.
- **Salasanojen ylläpitotyökalut**
  Salasanojen ylläpitotyökalujen avulla käyttäjät voivat luoda vahvoja yksilöllisiä salasanoja tileille ja palveluihin, joita he käyttävät opinnoissaan ja töissään (kun kertakirjautuminen ei ole käytössä). Nämä työkalut eivät auta kirjautumaan laitteen käyttöjärjestelmään, vaan niiden avulla salasanoja voi hallita kirjautumisen jälkeen. Google-käyttäjät voivat käyttää Salasanat-palvelua Chromella millä tahansa alustalla, myös ChromeOS:ssä ja Androidissa.

Eri ryhmille kannattaa valita todennusmenetelmistä sopiva yhdistelmä sen mukaan, minkä ikäisiä he ovat, minkä tyyppisiin järjestelmiin ja tietoihin heillä on pääsy ja mikä heidän roolinsa oppilaitoksessa on.

Oppilaitoksen järjestelmänvalvojat

Järjestelmänvalvoja hallinnoi perus- ja keskiasteen oppilaitoksen järjestelmiä ja pitkälti myös dataa. Tilien suojaaminen on ensiarvoisen tärkeää koko järjestelmän turvallisuuden kannalta. Tämä pätee infrastruktuurista tilitietoihin ja oppilaitoksen hallinnoimiin laitteisiin. Oppilaitosten tulee ottaa käyttöön luokkansa paras todennus ja käyttää esimerkiksi vahvoja salasanoja, tehokasta salasanojen ylläpitotyökalua ja kaksivaiheista vahvistusta. Kaikki nämä parantavat turvallisuutta, ja yhdessä käytettynä ne suojaavat järjestelmänvalvojatilin ja organisaation palvelut parhaalla mahdollisella tavalla.

- Järjestelmänvalvojien tulee käyttää fyysistä suojausavainta tai salauksella suojattua kaksivaiheista vahvistusta, joka edellyttää luotettua laitetta ja kehotteita. Tähän voi käyttää esimerkiksi Google Authenticator -sovellusta tai muuta ohjelmaa, joka luo kertakäyttöisen vahvistuskoodin. Vuoden 2019 jälkeen julkaistuissa TPM-sirullisissa Chromebookeissa on virtapainike, jota voi käyttää kaksivaiheiseen vahvistukseen.
- Järjestelmänvalvojien tulee käyttää luotettua salasanojen ylläpitotyökalua, joka tallentaa eri palveluissa tarvittavat salasanat kaksivaiheisen vahvistuksen avulla.

Määritettyjä laitteita käyttävät vanhemmat oppilaat (yleensä 4-luokkalaiset ja sitä vanhemmat)

Vanhemmat oppilaat ovat paremmin perillä itsensä ja tietojensa suojaamisesta. He pystyvät myös yleensä käyttämään vahvempia todennusmenetelmiä, jotka soveltuvat heidän käyttämiinsä palveluihin. Heillä tulee olla pääsy vain omalle tililleen ja heille jaettuihin tietoihin.

- Chromebookeja käyttäville oppilaille tulee antaa mahdollisuus luoda laitekohtainen PIN-koodi, joka nopeuttaa kyseiselle laitteelle kirjautumista. Biometriset vaihtoehdot eivät välttämättä sovellu oppilaitosympäristöihin tai ne eivät ole niissä sallittuja.
- Jokaisen oppilaan tulee luoda yksilöllinen salasana, joka ei sisällä henkilökohtaisia tietoja (esimerkiksi nimeä, vuosiluokkaa tai syntymäpäivää). Oppilaita tulee ohjeistaa monimutkaisten salasanojen käytössä, ja heille tulee antaa vinkkejä salasanan muistamiseen..

Määritettyjä laitteita käyttävät opettajat ja henkilökunta

Järjestelmänvalvojien tapaan myös opettajilla ja muulla henkilöstöllä on pääsy arkaluontoisiin tietoihin. He eivät kuitenkaan vastaa digitaalisesta infrastruktuurista ja heidän tekninen osaamisensa voi olla eritasoista.

- Chromebookeja käyttäville opettajille ja muille työntekijöille on annettava mahdollisuus kirjautua biometrisellä todennuksella, kuten sormenjäljellä, lain niin salliessa.
- Järjestelmänvalvojien tulee pakottaa kaksivaiheisen vahvistuksen käyttö ja siirtyä salasanattomaan todennukseen mahdollisuuksien mukaan ja työntekijöiden käyttäessä oppilaitoksen järjestelmiä etänä..

Jaettuja laitteita käyttävät nuoret oppilaat (yleensä 3-luokkalaiset ja sitä nuoremmat)

Nuoret oppilaat opettelevat vielä käyttämään koulutusteknologiaa. Heille sopivat parhaiten yksinkertaiset todennusmenetelmät, joita voidaan hyödyntää, kun palveluja ja dataa on rajattu.

- Kolmannen osapuolen salasanamenetelmiä (kuten QR-koodeja ja kuvakirjautumista) voidaan ottaa käyttöön nuorimmilla oppilailla ja käyttäjillä, jotka eivät voi kirjautua salasanalla. Koska nämä vaihtoehdot ovat vähemmän turvallisia, oppilaitosten on varmistettava tietoturva erillisillä toimenpiteillä. Järjestelmänvalvojien tulee vaihtaa oppilaan salasana ja päivittää koodi, jos koodi häviää tai joutuu asiattomien käsiin.
- Oppilaitosten tulee opastaa sekä oppilaita että heidän vanhempiaan siitä, miten tärkeää on pitää salasanat turvassa ja tallentaa vaihtoehtoiset kirjautumistiedot (kuten QR-koodit) turvallisesti.
- Tablettien kaltaisilla määritetyillä laitteilla voidaan käyttää PIN-koodia vaihtoehtoisena turvallisena todennusmenetelmänä..

Asianmukaisten suojausasetusten käyttäminen

Koska oppilaitosten laitteiden ja verkkojen näkyvyys on suuri, ne ovat arvokkaita kohteita hyökkääjille kaikkialla maailmassa. Siksi on erittäin tärkeää varmistaa paras mahdollinen suojaus, jotta voidaan estää palveluiden ja materiaalien häviäminen sekä rahan- ja ajanmenetys. Järjestelmänvalvojien tulee ottaa käyttöön tehokkaita ja tarkoituksenmukaisia turvaominaisuuksia, jotka ovat saatavilla oppilaitoksen käyttämissä tuotteissa. Heidän on kuitenkin varmistettava, että opettajien ja muun henkilöstön sekä oppilaiden on helppo käyttää näitä järjestelmiä. Tärkeät suojaus- ja yksityisyysasetukset on valittava siten, etteivät käyttäjät voi poistaa niitä käytöstä tai tehdä niihin muutoksia. Muihin asetuksiin järjestelmänvalvojan tulee valita turvalliset oletusasetukset. On erittäin tärkeää varmistaa paras mahdollinen suojaus, jotta voidaan estää palveluiden ja materiaalien häviäminen sekä rahan- ja ajanmenetys. Jos käytät Chromebookia, lue suosituksia laitekäytäntöjen valintaan viimeisestä osiosta.

Integroi datan minimointiperiaate oppilaitoksesi käytäntöihin. Kerää, käytä ja jaa käyttäjien henkilökohtaisia tietoja vain sellaisilla tavoilla ja sellaisiin tarkoituksiin, kuin on tarpeen palvelun tarjoamista tai sitä varten, mikä on muuten asianmukaista roolien välisen suhteen perusteella.

Sovellukset ja päivitykset

Rajoita ja minimoi käyttäjien mahdollisuutta asentaa sovelluksia, sillä jokainen laitteelle asennettu sovellus on potentiaalinen hyökkäyskohde. Jos mahdollista, käytä vain luotetuista lähteistä peräisin olevia sovelluksia. Suosittele käyttäjiä esimerkiksi tarkistamaan, että Google Play Kaupan sovelluksessa näkyy vahvistusmerkki. Näin voidaan varmistaa, että käyttäjät lataavat virallisia, tietoturvatarkastuksen läpäisseitä sovelluksia. Käyttöjärjestelmään tai laitteistoon tehdyt muutokset (esim. käyttöoikeuksien laajentaminen tai pääkäyttäjän oikeuksien ottaminen) vaarantavat tietoturvan, joten niitä kannattaa välttää.

Pääsyoikeudet ja näkyvyys

Järjestelmänvalvojien tulee varmistaa, että käyttäjillä on pääsy vain niihin tietoihin, ohjelmistoihin, palveluihin ja järjestelmiin, joita he tarvitsevat hoitaakseen työnsä tai opintonsa tehokkaasti. Tämä auttaa rajoittamaan tahatonta pääsyä ja valvomaan, ketkä käyttävät mitäkin tietoja. Huolehdi erityisesti arkaluontoisista tiedoista, kuten käyttäjien henkilökohtaisista tunnistetiedoista ja järjestelmistä (mm. henkilöstöhallinto, palkanlaskenta, arviointi, tietoturva ja asetukset), tarkistamalla, kenellä on pääsy tietoihin ja missä tilanteissa. Rajoita myös pääsyä oppilaitoksen omistamille laitteille ja anna pääsy vain tietyille henkilökunnan jäsenille.

Tarkista datan jakamiskäytännöt yhteiskäyttötyökaluissa, jotta voit estää tahattoman tai liiallisen jakamisen ja luvattoman pääsyn. Rajoita jakamista organisaatiosi ulkopuolelle tai estä se (erityisesti oppilailta) ja ota käyttöön käytäntöjä, joilla voit valvoa arkaluontoisen sisällön jakamista.

Laitemenetykset tai -varkaudet

Jos laite katoaa, data voidaan kuitenkin säilyttää. Järjestelmänvalvojien tulee laatia suunnitelma, jonka avulla varmistetaan, että tiedot ja dokumentit ovat käytettävissä myös, jos laite katoaa tai varastetaan. Dokumentit voidaan tallentaa esimerkiksi pilvipalveluun. Lataa ja tulosta kaksivaiheisen vahvistuksen varakoodit, jotta tilien käyttö ei keskeydy.

Kun laite ilmoitetaan kadonneeksi tai varastetuksi, varmista, että laite ja siihen liittyvät tilit lukitaan etänä mahdollisuuksien mukaan tai ilmiannetaan, jotta niitä ei voida käyttää luvatta. Kadonneet Chromebookit voidaan etätyhjentää, ja Google Workspace for Education -tilejä voidaan valvoa epäilyttävän toiminnan varalta tai ne voidaan jäädyttää (lukita) tarvittaessa.

Lisäsuojaus korkean riskin käyttäjille

Google tarjoaa Lisäsuojaus-ohjelman käyttäjille (mm. Google Workspace for Education -järjestelmänvalvojille), joiden näkyvyys on suuri ja jotka käsittelevät arkaluontoisia tietoja. Ohjelma tarjoaa käyttäjille lisäsuojaa kohdistettuja hyökkäyksiä, kuten tietojenkalasteluyrityksiä, haitallisia latauksia ja salasanavuotoja, vastaan. Lisäsuojaus-ohjelma on erityisesti suunniteltu torjumaan Google-tileille kohdistettuja verkkohyökkäyksiä. Ohjelma hyödyntää automaattisesti vahvoja salasanoja sekä suojausavaimia ja rajoittaa kolmannen osapuolen pääsyä tilin dataan.

Myös muut verkkotilipalvelut tarjoavat vahvoja suojaustyökaluja korkean riskin käyttäjille. Järjestelmänvalvojien ja henkilökunnan tulee aina käyttää näitä työkaluja, jos heillä on pääsy henkilökohtaisiin tietoihin tai teknisiin järjestelmiin.

Järjestelmien päivittäminen ja pitäminen ajan tasalla

Käyttäjät voivat varmistaa oman turvallisuutensa pitämällä laitteen käyttöjärjestelmän ja sovellukset ajan tasalla. Tämä on entistä tärkeämpää perus- ja keskiasteen oppilaitoksissa, koska ne ovat olennainen osa lasten koulunkäyntiä ja arkea. Suurin osa haittaohjelmahyökkäyksistä niin opetusalalla kuin muissakin korkean riskin ympäristöissä on kohdistunut Windowsiin. Esimerkkinä mainittakoon SolarWinds, Los Angeles Unified School Districtiin kohdistettu kiristysohjelmahyökkäys, Little Rock School Districtin hakkerointi, Microsoft Exchange Serverin tietomurto, Albuquerque School Districtin kiristysohjelmahyökkäys ja äskettäin tapahtunut Microsoftin liittovaltion viraston tietomurto. Myös näissä tilanteissa pilviratkaisujen -ja palvelujen käytön pitäisi helpottaa järjestelmänvalvojan työtä vähentämällä hyökkäyksille alttiiden alueiden määrää ja varmistamalla, että järjestelmät ja sovellukset pysyvät ajan tasalla automaattisesti.

Nykystandardien mukaiseen käyttöjärjestelmään päivittäminen ja sen pitäminen ajan tasalla

Käyttöjärjestelmän viimeisin versio sisältää yleensä uusimmat turvaominaisuudet, jotka auttavat estämään tunnettujen toimijoiden tekemät hyökkäykset. Laitteen käyttöjärjestelmän automaattiset päivitykset tulee laittaa päälle. Jos tämä ei ole mahdollista, lataa ja asenna virheenkorjaukset ja päivitykset luotettavasta lähteestä vähintään kuukausittain.

Chromebookien käyttöjärjestelmä on ChromeOS, joten ne päivittyvät usein ja automaattisesti uusimmilla tietoturvapäivityksillä, minkä ansiosta viimeisimmät suojausinnovaatiot voidaan ottaa käyttöön nopeasti. Myös vain luettavissa olevan käyttöjärjestelmän eheys tarkistetaan ennen käynnistystä. Chromebookit salaavat kaiken laitteelle tallennetun datan suojaten sitä luvattomalta käytöltä. Myös jokainen verkkosivu ja sovellus avataan erillisessä hiekkalaatikossa, joten jos jollakin sivustolla tai jossakin sovelluksessa havaitaan haittaohjelma, se ei pääse leviämään laitteen muihin osiin.

Jos oppilaitoksesi ei ole valmis siirtymään Chromebookeihin, oppilaitoksen laitteita voidaan nykyaikaistaa ChromeOS:n ChromeOS Flex -versiolla. ChromeOS Flex tarjoaa kaikille käyttäjille yhdenmukaisen, nykystandardien mukaisen opetus- ja oppimiskokemuksen, jossa on sisäänrakennettu, ennakoiva suojaus ja pilvipohjaiset hallintatyökalut. Flexillä voidaan varmistaa automatisoitu suojaus ja estää haitallisten tiedostojen ja sovellusten suorittaminen. Nykyistä laitekantaa ei tarvitse korvata.

Nykystandardien mukaiseen selaimeen päivittäminen ja sen pitäminen ajan tasalla

On tärkeää varmistaa, että selain on turvallinen ja ajan tasalla. Nykystandardien mukaisissa selaimissa on hyödyllisiä turvaominaisuuksia. Selain voi kehottaa käyttäjiä ottamaan nämä toiminnot helposti käyttöön tai järjestelmänvalvoja voi laittaa ne päälle oletuksena oppilaitoksen tietokoneilla. Tämä auttaa suojaamaan arkaluontoisten tietojen luottamuksellisuutta, kun dataa siirretään internetin välityksellä. Selain on pidettävä ajan tasalla. Olipa kyse työnteosta, oppimisesta tai muusta verkkotoiminnasta, päivitetyn ja nykystandardien mukaisen selaimen on täytettävä seuraavat vaatimukset:

- **Sen on käytettävä vahvaa suojausta,** kuten sivuston pitoa erillään ja selaussuojaa, jotta käyttäjät eivät voi vahingossa siirtyä vaarallisille sivustoille.
- **Sen on käytettävä automaattisia päivityksiä,** joiden avulla selain saa tietoturvapäivitykset nopeasti.
- **Sen on käytettävä suojattua yhteyttä.** Nykystandardien mukaisen selaimen tulee käyttää TLS-salausta. Käyttäjät voivat klikata URL-osoitteen vierestä ja tarkistaa, että yhteyden tila on suojattu.

Chrome on rakennettu turvallisuutta ajatellen, ja selaussuojan kaltaiset turvaominaisuudet ovat käytössä oletusarvoisesti. Integroitu salasanojen ylläpitotyökalu voi täyttää salasanat automaattisesti verkkoa selatessasi, joten voit helposti käyttää vahvoja salasanoja.

Reaaliaikaisten ilmoitus- ja valvontajärjestelmien hyödyntäminen

Reaaliaikaisten ilmoitus- ja valvontajärjestelmien avulla oppilaitokset voivat tunnistaa uhkia ja reagoida niihin nopeasti ennen kuin ne ehtivät aiheuttaa ongelmia. On tärkeää varmistaa, että tietoturvatyökalut toimivat taustalla keräten ja rekisteröiden tietoturvatapahtumia kaikkien järjestelmien laajuudelta. Tekoälyä hyödyntävät työkalut ovat erityisen näppäriä suurien tietomäärien analysoimiseen sekä poikkeamien ja mallien havaitsemiseen. Näin voidaan nopeammin ja helpommin havaita ja prosessoida uhkia sekä korjata haavoittuvuuksia. Samalla voidaan myös valita, mihin tapahtumiin IT-järjestelmänvalvojan tai henkilökunnan tulee tarttua ripeimmin.

Oppilaitokset voivat hyödyntää ensisijaiseen yhteiskäyttö- ja viestintäohjelmistoon, kuten Google Workspace for Educationiin, integroituja ilmoitus- ja valvontatoimintoja, tai ottaa käyttöön erillisiä suojaustietojen ja tapahtumien hallinnan työkaluja (SIEM).

Reaaliaikaiset ilmoitus- ja valvontajärjestelmät pystyvät seuraamaan oppilaitoksen verkkoon, laitteisiin, sovelluksiin, käyttäjiin ja dataan liittyviä tapahtumia, kuten sisäänkirjautumisia, tiedostojen käyttöä, mahdollisia tunkeutumisia, onnistuneita tai yritettyjä datavarkauksia sekä järjestelmänvalvojan tapahtumia.

Jos järjestelmä havaitsee epäilyttävää toimintaa, se voi lähettää ilmoituksen oppilaitoksen IT-tiimille. Järjestelmänvalvojat voivat tutkia asiaa ja ryhtyä toimenpiteisiin ongelman ratkaisemiseksi.

Ilmoitus- ja valvontatyökalujen avulla saadaan myös parempi käsitys oppilaitokseen kohdistuvista uhkista. Reaaliaikaisista järjestelmistä saatua dataa analysoimalla oppilaitokset voivat tunnistaa trendejä ja malleja, joiden perusteella ne voivat parantaa suojaustaan.

Alla on lueteltu parhaita käytäntöjä ilmoitus- ja valvontajärjestelmien (myös SIEM-ratkaisujen) käyttöön:

1. **Tietoturvatavoitteiden määrittely**
   Mieti, mitkä tiedot ja järjestelmät ovat kriittisimpiä oppilaitoksen kannalta ja minkä tyyppisistä uhkista niille aiheutuu suurin riski. Pohdi sitten, minkä tyyppistä dataa sinun tulee kerätä näiden uhkien valvomiseksi.
2. **Tarkoituksenmukaisen datan kerääminen ja oikeanlaisten asetusten valitseminen**
   On tärkeää kerätä tarkoituksenmukaista dataa ja määrittää sovellukset oikein, jotta voit saavuttaa tärkeimmät tietoturvatavoitteesi. Tämä saattaa pitää sisällään palomuureista, sisältösuodattimista, tunkeutumisen havaitsemisjärjestelmistä, verkkopalvelimilta ja muista tietoturvalaitteista sekä viestintä- ja yhteiskäyttöohjelmistoista, oppilaitoksen tietojärjestelmistä ja opetusalustoilta saatavan datan.
3. **Ilmoitusten tutkiminen ja niihin reagoiminen**
   Kun valvontajärjestelmä lähettää ilmoituksen, on tärkeää tutkia tapahtuma ja ryhtyä tarvittaviin toimenpiteisiin. Eri tiimit voivat selvittää yhdessä, mistä ilmoitus on peräisin tai onko se mahdollisesti virheellinen positiivinen ilmoitus. Mahdollisissa tietoturvatilanteissa toimenpiteisiin voi lukeutua tilien jäädyttäminen, salasanojen nollaaminen, sähköpostien asettaminen karanteeniin tai poistaminen, tiedostojen käyttöoikeuksien muuttaminen tai laitteiden tyhjentäminen.

Opettajien ja muun henkilöstön sekä oppilaiden ohjeistaminen

Perus- ja keskiasteen oppilaitosten tulee olla entistä valveutuneempia tietoturvan ja kouluyhteisön toimintatapojen suhteen. Käyttäjiä voidaan kannustaa turvallisempiin tapoihin kampanjoiden ja yhteistyökumppanuuksien avulla. On tärkeää painottaa suojauksen merkitystä opettajille, henkilöstölle ja oppilaille, jotta he oppivat huolehtimaan turvallisuudesta verkossa ja estämään vakavat kyberturvallisuusuhkat. Ohjeista heitä käyttämään oppilaitoksen saatavilla olevia tuotteita ja palveluita sekä tunnistamaan esimerkiksi tietojenkalasteluviestien kaltaisia uhkia ja ilmoittamaan niistä. Tärkeintä on kuitenkin opastaa heitä siinä, miten he voivat omalla toiminnallaan auttaa estämään hyökkäykset. Oppilaitosten ja koulupiirien tulee olla entistä valveutuneempia tietoturvan ja kouluyhteisön toimintatapojen suhteen. Käyttäjiä voidaan kannustaa turvallisempiin tapoihin kampanjoiden ja yhteistyökumppanuuksien avulla.

Laitteiden ja ohjelmistojen turvallinen käyttö

Järjestelmänvalvojat voivat kehittää ikäryhmille sopivia kyberturvallisuuden toimintatapoja yhdessä opettajien ja asiantuntijoiden kanssa. Näin he voivat auttaa oppilaita käyttämään laitteita, ohjelmistoja ja järjestelmiä turvallisesti. Oppilaitoksen omien tai koulupiirikohtaisten koulutusmateriaalien avulla opettajia ja oppilaita voidaan ohjeistaa suosituksissa. Saatavilla on kuitenkin myös valmiita materiaaleja, esimerkiksi Safety.Googlen Be Internet Awesome ja Khan Academyn koulutukset, joita voidaan räätälöidä tarpeen mukaan. Nämä ohjelmat auttavat käyttäjiä toimimaan turvallisesti missä vain – niin koulussa kuin yhteisössäkin.

Uhkien tunnistaminen

Opettajat, henkilöstö ja oppilaat voidaan suojata kouluttamalla heitä tunnistamaan uhkia. Lasten on tärkeää oppia tunnistamaan, onko jokin uhka vai ei, koska he eivät välttämättä osaa sanoa, onko jokin laillista. Heidän tulee oppia tunnistamaan tietyntyyppisiä uhkia ja ilmoittamaan niistä. Järjestelmänvalvojien tulee keskittyä sellaisiin aiheisiin, joista on eniten hyötyä sijoitetun pääoman tuoton kannalta. Ohjeistuksessa ei kuitenkaan tule keskittyä ainoastaan uhkien tunnistamiseen vaan myös toimenpiteisiin tarttumiseen. Käyttäjien tulee osata tunnistaa yleisimpiä uhkia, joita ovat kiristysohjelmat, tietojenkalastelu, käyttäjän manipulointi, haittaohjelmat ja huijaukset. Jos tietyntyyppiset uhkat ovat yleisempiä kyseisessä oppilaitoksessa, kouluyhteisöä on hyvä ohjeistaa niiden osalta.

Datan ja tiedostojen jakaminen turvallisesti

Opettajille ja muulle henkilökunnalle tulee kertoa asianmukaisista tavoista jakaa tiedostoja ja dataa sekä siitä, miten sähköpostiin saapuneita sopimattomia pyyntöjä voi tunnistaa. Heille tulee painottaa, että arkaluontoisia henkilökohtaisia tietoja tulee jakaa ja käsitellä vain tarvittaessa. Tällainen data on suojattava tehokkaasti: sitä ei esimerkiksi saa koskaan jakaa sähköpostitse tai ulkopuolisille. Henkilöstön tulee käyttää tietojen menetyksen estoa (sisältyy ChromeOS:ään ja Workspace for Educationiin), joka varoittaa ja estää loppukäyttäjiä jakamasta arkaluontoisia tietoja (esimerkiksi henkilötunnuksia) sisältäviä tiedostoja tai kopioimasta ja liittämästä arkaluontoista sisältöä verkkotunnuksen ulkopuolelle.

Googlen lähestymistapa käytännössä: Opetussektorille suunnatut laitteet ja palvelut

Koulupiiri voi suojautua parhaiten käyttämällä tehokkaita ohjelmistoja. Ohjelmistojen avulla on pystyttävä minimoimaan haavoittuvuuden riski. Niissä on myös oltava kattavat suojausominaisuudet. Laajempi kyberturvallisuuden vaarantumisen riski voidaan välttää, kun oppilaitoksia edellytetään hankkimaan turvallisia ohjelmistoja tai luotettavien yritysten tarjoamia todistetusti turvallisia ratkaisuja. Google on esimerkiksi vahvistanut ChromeOS:n suojausta ottamalla käyttöön ennakoivia älyratkaisuja, jotka hyödyntävät koneoppimista, pilvipalveluja ja tunnistamiseen liittyvää asiantuntemusta.

Googlen tavoitteena on luoda tuotteita, jotka auttavat vahvistamaan oppilaiden ja opettajien yksityisyyttä ja tarjoavat luokkansa parasta tietoturvaa oppilaitoksellesi. Voit luottaa siihen, että Google for Education -tuotteet ja palvelut suojaavat jatkuvasti käyttäjiä, laitteita ja dataa entistä moninaisimmilta uhilta. Tässä osiossa oppilaitoksen IT-järjestelmänvalvojia opastetaan tietoturvasuosituksissa käytettäessä Google for Education -tuotteita.

Google Workspace for Education

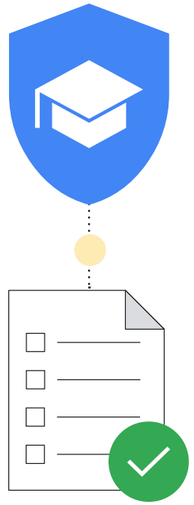
Google Workspace for Education tarjoaa valikoiman Googlen työkaluja ja palveluja, jotka on suunniteltu oppilaitosten tarpeisiin. Niitä voi käyttää yhteistyön tekemiseen, opetuksen sujuvoittamiseen ja turvallisen oppimisympäristön luomiseen. Google for Education -tuotteet ja palvelut suojaavat jatkuvasti käyttäjiä, laitteita ja dataa entistä moninaisimmilta uhilta. Ne tarjoavat myös työkaluja, kuten ilmoitus- ja tietoturvakeskuksia, eDiscoveryn Holvi-ominaisuuden, identiteetin ja pääsyoikeuksien hallintatoiminnon sekä tietojen menetyksen eston.

Olemme laatineet hyödyllisiä materiaaleja, jos olet vasta aloittamassa Google Workspace for Educationin käyttöä. Näiden materiaalien avulla voit tehdä asetukset tässä oppaassa kuvattujen suositusten mukaisesti. Saat lisätietoja Google Workspace for Educationin käyttöönottoon IT-määrityksen pikaoppaasta.

Suojauksen tarkistuslistat

Tutustu suojauksen tarkistuslistoihin, joista saat lisätietoja tietoturvan ja oppilaitoksesi yksityisyyden parantamiseen. Google Workspace for Education Standard- ja Plus-versioita käyttävät oppilaitokset voivat muokata hallintakonsolin asetuksia myös Tietoturvan tila -sivun avulla. Voit tarkistaa esimerkiksi sähköpostin uudelleenohjauksen, laitteen salauksen ja laitteen jakamisasetusten tilan ja tehdä paljon muuta. Voit tarvittaessa muuttaa verkkotunnuksesi asetuksia yleisten tietoturvaohjeiden ja parhaiden käytäntöjen mukaiseksi. Samalla voit huomioida organisaatiosi tarpeet ja riskinhallintakäytännöt.

Miksi koulutusalan uskotaan joutuvan hyökkäyksen kohteeksi



Lähde: https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf

Seuraavassa on muutamia hyödyllisiä vinkkejä, joiden avulla varmistat, että saat parhaan mahdollisen hyödyn Google Workspace for Educationiin sisältyvistä suojausominaisuuksista:

Organisaatioyksiköiden käyttöönotto

Google Workspace for Education -tilin käyttäjille voidaan valita eri asetukset tarpeen mukaan. Organisaatioyksiköt ovat käyttäjäryhmiä, joiden avulla voit lisätä eri käyttäjille eri palveluja, asetuksia ja lupia. Voit esimerkiksi ottaa kaksivaiheisen vahvistuksen käyttöön opettajille ja muulle henkilökunnalle ja ikäryhmälle sopivan todennusmenetelmän nuorille oppilaille. Käytä erillisiä organisaatioyksiköitä henkilökunnalle, opettajille ja oppilaille, niin voit lisätä käytäntöjä erikseen kullekin käyttäjäryhmälle. Rakenne on syytä miettiä huolella, sillä toimivan rakenteen ansiosta Google Workspace for Education -tilin hallinnointi on joustavaa ja sujuvaa.

Salasanakäytäntöjen ja järjestelmänvalvojan tilin suojauksen käyttöönotto

Kuten edellä kuvattiin, käyttäjien todennus on tehokas tapa suojata oppilaitos. Kehittämiemme joustavien menetelmien avulla järjestelmänvalvojat voivat tehokkaasti hallita todennusta ja varmistaa, että käyttäjien tilit on suojattu asianmukaisesti. Salasanakäytäntöjen avulla voidaan varmistaa, että käyttäjät luovat vahvoja salasanoja. Myös kaksivaiheisen vahvistuksen käyttöä kannattaa harkita mahdollisuuksien mukaan turvallisen kirjautumisen suositusten perusteella. Voit pakottaa kaksivaiheisen vahvistuksen käytön tietylle käyttäjäryhmälle (anna heille aikaa toiminnon käyttöönottoon). Kaksivaiheinen vahvistus voidaan ottaa käyttöön monella eri tavalla. Turvallisin tapa on käyttää suojausavaimia. Muita vaihtoehtoja ovat Google-kehote (Googlen sovellusten avulla Androidissa ja iOS:ssä), todennussovellukset (kuten Google Authenticator) sekä vahvistus tekstiviestillä tai puhelulla (turvallisuuden kannalta puhelut ja tekstiviestit ovat heikoimpia).

Jos organisaatiosi käyttää tunnistetietojen tarjoajana muuta kuin Googlea, voit ottaa kertakirjautumisen käyttöön kolmannen osapuolen tunnistetietojen tarjoajan kautta. Voit edelleen halutessasi käyttää kertakirjautumiseen perustuvaa kaksivaiheista vahvistusta muilla kuin pääkäyttäjän tileillä.

Palveluiden laittaminen päälle tai pois päältä

Järjestelmänvalvojat voivat valita Google-hallintakonsolista, mihin Googlen palveluihin käyttäjillä on pääsy Google Workspace for Education -tilillä. Voit hallita pääsyä esimerkiksi Kalenteriin, Driveen, Meetiin ja muihin Googlen palveluihin laittamalla palvelut päälle tai pois päältä organisaatioyksiköittäin. Palveluita on mahdollista laittaa päälle myös ryhmiä käytettäessä. Ennen lisäpalvelun (esim. YouTube, Google Maps ja Blogger) ottamista käyttöön kannattaa vertailla Workspacen ydin- ja lisäpalveluiden välisiä eroja. Järjestelmänvalvojia suositellaan valitsemaan Googlen palveluiden pääsyoikeudet ikäryhmän perusteella. Kannattaa kuitenkin muistaa, että alle 18-vuotiaille asetetaan automaattisesti rajoituksia joissakin Googlen palveluissa Google Workspace for Education -tiliä käytettäessä.

Voit hyödyntää myös kontekstin mukaista pääsyä (saatavilla Workspace for Education Standard- ja Plus-versioissa) ja sallia tai estää pääsyn tiettyihin Google-sovelluksiin (kuten Gmail, Drive ja Kalenteri) laitteen IP-osoitteen, maantieteellisen alkuperän, tietoturvakäytäntöjen ja käyttöjärjestelmän perusteella. Voit esimerkiksi sallia Drive-työpöytäsovelluksen käytön vain yrityksen omistamilla laitteilla tietyissä maissa tai tietyillä alueilla.

Tapoja antaa käyttäjille pääsy palveluihin

Google-hallintakonsolista voit estää koko organisaatioyksikön pääsyn esimerkiksi Google Driveen tai muuhun Googlen palveluun. Jos tietyt organisaatioyksikön käyttäjät tarvitsevat pääsyn Driveen, sinulla on kaksi vaihtoehtoa:

1. Siirrä kyseiset käyttäjät sellaiseen organisaatioyksikköön, jolla on pääsy Driveen.
2. Lisää käyttäjät pääsyoikeusryhmään ja salli pääsy Driveen kyseiselle ryhmälle. Ryhmän jäsenillä on pääsy palveluun, vaikka heidän organisaatioyksiköllään ei olisi pääsyä.

Organisaatioyksiköt

Google Drive on pois päältä organisaatioyksiköillä 1 ja 2.

Pääsyoikeusryhmä

Osalla **organisaatioyksiköiden** 1 ja 2 käyttäjistä on pääsy Google Driveen.

Lähde: https://support.google.com/a/answer/9050643?sjid=4805599982673626852-NA

Datan jakamiskäytäntöjen ja säilytyssääntöjen valitseminen

Järjestelmänvalvojana voit valita, onko käyttäjillä lupa jakaa Google Drive -tiedostoja organisaation ulkopuolisille henkilöille. Tällä tavoin voit estää tahattoman tai liiallisen datan ja tiedostojen jakamisen ja välttää datavuodot. Tiedostojen ja tallennuspaikkojen eriyttäminen, organisaatioyksiköiden luominen ja pienimmän käyttöoikeuden periaatteen noudattaminen ovat tehokkaita keinoja estää hakkeroijien toiminta verkossa, jos yksi tili on joutunut hyökkäyksen kohteeksi. Mitä vähemmän dataa ja verkon osia hyökkääjällä on mahdollisuus käyttää, sitä paremmin vahingot voidaan minimoida.

Laita ulkoinen tiedostonjako pois päältä oppilailla (tai rajoita ulkoinen jakaminen vain sallittuihin verkkotunnuksiin) ja valitse käyttöoikeuksien tarkistuksen asetukseksi “Vain vastaanottajat”. Jos sallit joidenkin tai kaikkien käyttäjien jakaa tiedostoja verkkotunnuksen ulkopuolelle, käyttäjille kannattaa laittaa päälle näkyvä varoitus. Poista käytöstä tiedostojen julkaiseminen verkossa ja edellytä ulkopuolisia yhteiskäyttäjiä .

Workspace for Education Standard- ja Plus-asiakkaat voivat käyttää myös kohdeyleisöjä ja luottamussääntöjä, joiden avulla jakamissuosituksia ja -rajoituksia voidaan lisätä yksityiskohtaisemmin. Esimerkiksi kohdeyleisöjen avulla voit valita, että opettajien linkit jaetaan oletusarvoisesti opettajille ja muulle henkilökunnalle oppilaitoksen kaikkien käyttäjien sijaan. Luottamussääntöjen avulla voidaan estää alakoulujen oppilaita jakamasta tiedostoja vanhemmille oppilaille.

Varmista jaettujen Drivejen käytännöillä, että vain asianmukaiset käyttäjät voivat luoda jaettuja Driveja ja että ulkoisilla käyttäjillä ei ole pääsyä sellaisiin. Suosittelemme sallimaan jaettujen Drivejen luomisen vain järjestelmänvalvojille (tai henkilökunnalle ja opettajille) ja seuraamaan niiden käyttöä tarkasti.

Hakemiston näkyvyyttä ja yhteystietojen jakamista kannattaa mahdollisuuksien mukaan rajoittaa joko estämällä yhteystietojen jakaminen tietyiltä tai kaikilta käyttäjiltä tai luomalla omia hakemistoja, joiden avulla voit rajoittaa käyttäjien näkymistä toisilleen.

Lisää tietojen menetyksen eston käytäntöjä Drivessa ja Gmailissa, jotta voit tunnistaa ja estää arkaluontoiset tiedot. Valmiiden käytäntöjen avulla voit suojata yleiset arkaluontoiset tiedot (esimerkiksi maksukorttien numerot). Voit myös luoda omia käytäntöjä avainsanojen, sanalistojen ja säännöllisten lausekkeiden avulla.

Gmailin asetusten muokkaaminen

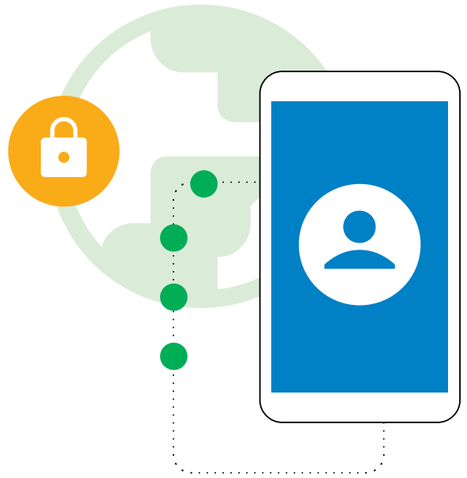
Gmail on yksi Google Workspace for Educationin ydinpalveluista, ja järjestelmänvalvojat voivat suojata oppilaitoksen ja käyttäjät monien sovellukseen sisältyvien asetusten avulla. Estä roskaposti, huijaukset ja tietojenkalastelu Gmailin todennuksella. Muokkaa roskapostisuodattimien asetuksia esimerkiksi edellyttämällä lähettäjän todennusta kaikilta hyväksytyiltä lähettäjiltä ja poistamalla käytöstä roskapostisuodattimien ohittaminen sisäisten lähettäjien osalta.

Poista POP- ja IMAP-käyttö mahdollisuuksien mukaan ja ota käyttöön parannettu viestien skannaus ennen toimittamista ja edistynyt tietojenkalastelu- ja haittaohjelmasuojaus. Jos sallit ulkoiset sähköpostit joillekin tai kaikille käyttäjille, voit ottaa käyttöön ulkoisten vastaanottajien varoitukset.

Google Workspace for Education Standard- ja Plus-asiakkaat voivat suojautua myös haitta- ja kiristysohjelmilta luomalla sääntöjä haitallisten liitteiden havaitsemista varten Security Sandboxin avulla.

Kolmannen osapuolen sovellukset

Hyödynnä sisäänrakennettuja työnkulkuja sellaisten kolmannen osapuolen sovellusten hyväksymiseen, jotka käyttävät tilin dataa APIn kautta. Näin voidaan estää datan jakaminen luvattomasti kolmannen osapuolen sovelluksiin, joita ei ole hyväksytty opetuskäyttöön.



Raportointi ja valvonta

Järjestelmänvalvojana voit valvoa organisaatiosi toimintaa Google-hallintakonsolin raporteista ja lokitapahtumista. Voit seurata esimerkiksi mahdollisia tietoturvariskejä, sisäänkirjautumisia sekä sisällön luomista ja jakamista. Verkkotunnustason datan lisäksi kaavioista ja taulukoista saadaan yksityiskohtaisia tietoja myös käyttäjätasolta. Raporttien ja valvontalokien (esimerkiksi ilmoituskeskuksen) avulla voit esimerkiksi tunnistaa tietoturvariskejä, analysoida palvelujen käyttöä, diagnosoida määritysongelmia ja seurata käyttäjien toimintaa.

Google Workspace for Education Standard- ja Plus-järjestelmänvalvojat voivat Tietoturvan hallintapaneelin avulla saada yleiskatsauksen tietoturvaraporteista, tunnistaa trendejä sekä vertailla nykyistä ja aiempaa dataa. He saavat tietoa Drive-tiedostonjaosta, roskapostista, tietojenkalastelusta ja haittaohjelmista Gmailissa sekä epäilyttävistä kirjautumisista ja laitetapahtumista. Useimmat käyttö-, tapahtuma- ja valvontalokit (mukaan lukien järjestelmänvalvojan, Driven, Meetin ja Chatin lokitapahtumat) ja tietoturvaraportit ovat saatavilla kuusi kuukautta.

Tietoturvakeskuksen hyödyntäminen

Google Workspace for Education Plus- ja Standard-järjestelmänvalvojien käytettävissä on tietoturvakeskus, jossa he voivat tarkastella monipuolisia tietoturvatietoja ja -tilastoja sekä saavat paremman näkyvyyden ja hallinnan verkkotunnusta koskeviin turvallisuusongelmiin.

Tietoturvakeskus sisältää suojaustutkintatyökalun, jonka avulla järjestelmänvalvojat voivat tunnistaa, arvioida ja torjua tietoturva- ja yksityisyysuhkia, kuten tietojenkalasteluyrityksiä, sopimatonta tiedostonjakoa sekä epäilyttäviä kirjautumisia ja laitetapahtumia.

Google Workspace on maailman turvallisin pilvipohjainen työkalupaketti viestintään ja yhteistyöhön

0

aktiivista ohjelmistojen haavoittuvuutta Workspacessa marraskuusta 2021 lähtien*

50%

n mahdolliset säästöt kyberturvallisuuden vakuutusmaksuista Google Workspacea käyttävillä organisaatioilla

2x vähemmän

tietoturvauhkia Workspacea käyttävissä organisaatioissa Microsoft 365:tä käyttäviin verrattuna

2.5x vähemmän

tietoturvauhkia Workspacea käyttävissä organisaatioissa Microsoft Exchangea käyttäviin verrattuna

*CISAn mukaan määrä on huomattavasti pienempi kuin muilla samantyyppisten tuottavuustyökalujen tarjoajilla.

Google Chromebookit opetuskäytössä

Chromebookit ovat perustaltaan suojattuja, joten ne ovat opettajille ja oppilaille sopivia erittäin turvallisia, skaalautuvia ja helppokäyttöisiä tietokoneita. Yhtään kiristysohjelmalla tehtyä hyökkäystä ei ole raportoitu yhdelläkään yritys-, oppilaitos- tai kuluttajakäytössä olleella ChromeOS-laitteella. Chromebookit suojaavat oppilaitoksia kehittyviltä uhkilta esimerkiksi ajantasaisilla ominaisuuksilla ja automaattisilla päivityksillä, jotka suoritetaan taustalla, jotta käyttäjät voivat jatkaa työskentelyä miltei heti.

Automaattiset käyttöjärjestelmä- ja sovelluspäivitykset sekä sisäänrakennettu haittaohjelmasuojaus

Käyttöjärjestelmien, selaimien ja suosittujen sovellusten virheiden ja haavoittuvuuksien avulla hyökkääjät yrittävät jatkuvasti asentaa haittaohjelmia ja varastaa käyttäjädataa. Chromebookit on suunniteltu perustaltaan turvallisiksi. Ne pitävät käyttöjärjestelmän, sovellukset ja tietoturvapäivitykset ajan tasalla käyttäjien suojaamiseksi. Pilvisovellukset eivät edellytä ohjelmistopäivityksiä samaan tapaan kuin paikallisesti asennetut sovellukset. Chromebookeissa on Googlen oma suojaussiru, joka suojaa laitteita, käyttäjäidentiteettejä ja koko järjestelmän eheyttä.

Virustorjuntapäivitykset ovat kaikissa Chromebookeissa automaattisia. Myös salaus, vahvistettu käynnistys, hiekkalaatikko ja automaattiset päivitykset suojaavat oppilaita ja opettajia kyberuhkilta.

Käyttäjädatan suojaaminen

Kirjautuessasi Chromebookille Google-tilillä kaikki datasi tallennetaan salattuihin tiedostoihin, joten kukaan muu laitetta käyttävä ei näe dataasi eikä pysty kirjautumaan tilisi käyttämiin sovelluksiin. Tämä helpottaa laitteiden jakamista turvallisesti oppilaiden kesken luokkahuoneessa, mikä auttaa puolestaan oppilaitoksia säästämään laitekustannuksissa. Chrome Education Upgrade -hallintalisenssillä saat entistä monipuolisempia turvaominaisuuksia ja enemmän näkyvyyttä.

Käyttäjien hallinnoimien laitteiden tietoturvakäytännöt etänä

Oppilaitoksen järjestelmänvalvoja voi määrittää ChromeOS-käytäntöjä sekä asentaa ja päivittää sovelluksia etänä Google-hallintakonsolin avulla. Yksi IT-järjestelmänvalvoja pystyy helposti päivittämään käytäntöjä ja asetuksia satoihin tuhansiin Chromebookeihin kerralla.

Näin toimimalla varmistetaan seuraavat

- Oppilailla on pääsy vain oppilaitoksen hyväksymiin sovelluksiin ja sisältöihin.
- Kaikkiin sovelluksiin ja laajennuksiin on päivitetty uusimmat tietoturvakorjaukset.
- Käyttäjät eivät voi kopioida, siirtää tai jakaa oppilaitoksen dataa laitteen ulkopuolelle.
- Voit tehdä dataan perustuvia päätöksiä tutustumalla Googlen tietoturvasuosituksiin, joissa on hyödyllistä tietoa tietoturvauhkista.
- Voit hallinnoida tietoturva-, identiteetti- ja pääsyoikeuskäytäntöjä keskitetysti kaikkien käyttäjien osalta suoraan hallintakonsolissa.

Käytännöt, jotka järjestelmänvalvojien kannattaa määrittää:

Laitekäytännöt

- **Vierastila**
  Laitteen vierastila on suositeltavaa poistaa käytöstä niin, että oppilaiden ja opettajien on kirjauduttava laitteelle omilla kirjautumistiedoillaan. Näin he eivät voi käyttää laitetta anonyymisti.
- **Kirjautumisrajoitukset**
  Oppilaiden ja opettajien ei tule kirjautua oppilaitoksen Chromebookeille henkilökohtaisilla Gmail-tileillään. Pakota sisäänkirjautuminen vain Workspace-verkkotunnukselle oppilaiden käytössä olevilla laitteilla.
- **Käyttäjä- ja laiteraportoint**
  Järjestelmänvalvojien kannattaa harkita käyttäjä- ja laiteraportoinnin laittamista päälle voidakseen kerätä tietoja Chromebookien käyttötiheydestä, käyttäjistä ja laitteiston tilasta. .
- **Pakotettu uudelleenrekisteröityminen**
  Oppilaitoksen omistamien Chromebookien tulee pysyä oppilaitoksen tiloissa, ellei järjestelmänvalvoja poista tietyn laitteen oikeuksia. Järjestelmänvalvojien kannattaa harkita pakotettua uudelleenrekisteröitymistä Chromebookeilla. Näin voidaan varmistaa, että Chromebook rekisteröi itsensä aina uudelleen, jos se jouduttaisiin tyhjentämään tai yritettäisiin varastaa.

Käyttäjäkäytännöt

- **Incognito-tila**
  Kun oppilailla on käytössään oppilaitoksen Chromebook, heillä on hyvä perusta oppimiseen. Tämä pitää sisällään hyväksytyn selaimen rajoittamisen verkkosisällön suodattimien avulla niin, etteivät käyttäjät pääse sopimattomille sivustoille. Järjestelmänvalvojien tulee poistaa incognito-tila käytöstä niin, etteivät oppilaat pysty kiertämään verkkosuodattimia.
- **Välityspalvelintila**
  Vaikka joissakin oppilaitoksissa hyödynnetään välityspalvelimia verkkosuodatukseen, käyttäjillä ei kuitenkaan saa olla lupaa muuttaa välityspalvelimen asetuksia.
- **Kirjautuminen useaan tiliin**
  Jos käyttäjillä on lupa kirjautua toissijaiselle tilille oppilaitoksen Chromebookia ja Workspace-tiliä käyttäessään, he saattavat luvattomasti kopioida oppilaiden arkaluontoisia tietoja tai oppilaitoksen dataa toissijaiselle tilille. Järjestelmänvalvojien tulee harkita usealle tilille kirjautumisen estämistä.
- **Selainhistoria**
  Oppilaiden kohdalla voi olla hyvä varmistaa, etteivät he pysty tyhjentämään selainhistoriaa. Mahdollisen tietoturvaongelman yhteydessä näistä historiatiedoista voi olla apua tutkinnassa.

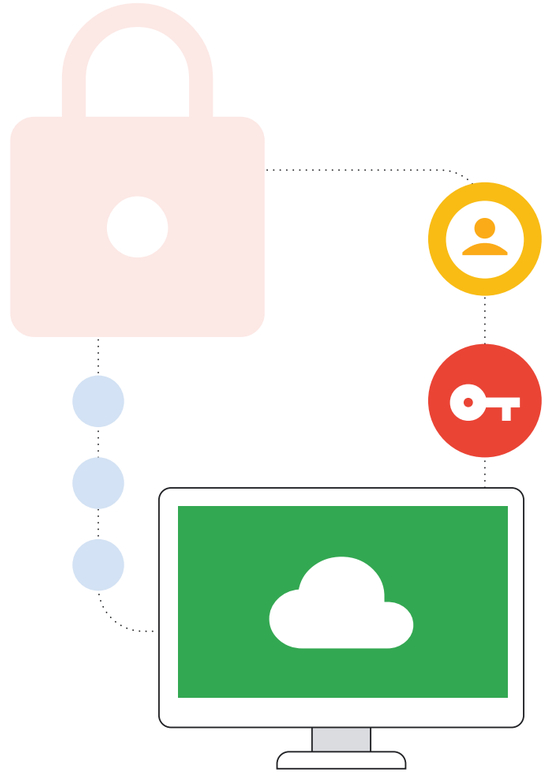
Tämän listan avulla voit varmistaa, että verkkosi on suojattu merkittäviltä kyberturvallisuuden ongelmilta, joita aiheutuu yleisimpien virheiden seurauksena. Muita tietoturvakäytäntöjen suosituksia löydät suojauksen tarkistuslistasta.

Turvallinen käyttö missä ja milloin vain päätelaitteiden hallinnan avulla

ChromeOS:n käytäntöjen etähallinnan avulla järjestelmänvalvojat voivat ottaa käyttöön suojausasetuksia ja asentaa tietoturvatyökaluja (esim. sisältösuodattimia) suoraan laitteille oppilaitoksen verkkopalvelimien sijaan. Näin varmistetaan, että oppilaiden käytössä on samat tietoturvaominaisuudet oppilaitoksen Chromebookeilla niin kotona kuin oppitunneillakin. Tämä on entistä tärkeämpää oppilaitosten siirtyessä entistä enemmän digitaalisiin oppikirjoihin ja verkossa oleviin oppimistyökaluihin, jolloin oppilaiden on otettava tietokoneet mukaan kotiin läksyjen tekemistä varten.

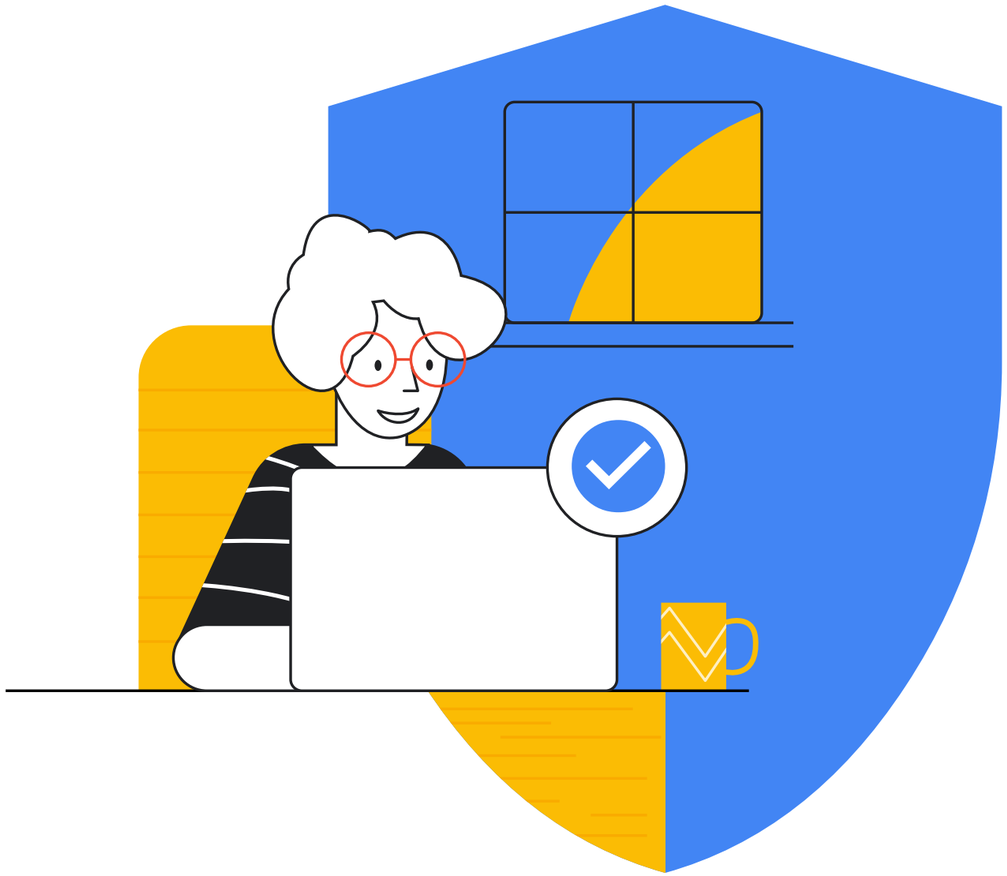
Lopuksi

Perus- ja keskiasteen oppilaitosten suojaaminen kyberturvallisuuden uhkilta on haastava tehtävä. Tähän kannattaa kuitenkin panostaa, jotta voidaan varmistaa oppilaiden, opettajien, henkilöstön ja koko verkkoekosysteemin turvallisuus. Tässä dokumentissa kuvatut asiat ovat hyvä lähtökohta, mutta jokaisen oppilaitoksen tulee soveltaa suosituksia yksilöllisten tarpeiden mukaan ja pysyä ajan tasalla kehittyvistä uhkista ja uusista teknologioista. Dokumentti luo perustan perus- ja keskiasteen oppilaitosten tietoturvaohjelmalle antamalla vinkkejä seuraavista vaiheista ja mahdollisista toimenpiteistä. Googlen monipuoliset materiaalit, koulutustarjonta sekä kyberturvallisuuden asiantuntijat auttavat oppilaitoksia ja organisaatioita tämän oppaan ohjeiden ja tekoälyn kaltaisten uusien teknologioiden soveltamisessa. Opetussektorille tarkoitetut Googlen tuotteet ovat valmiita ratkaisuja, joiden avulla voidaan vastata moniin tässä dokumentissa kuvattuihin kyberturvallisuuden haasteisiin. Meiltä saat apua oman tietoturvaohjelmasi suunnitteluun ja käyttöönottoon.



Lähdeluettelo

- [1]Google. “Tips to Stay Safe & Secure Online”, Googlen turvallisuuskeskus, https://safety.google/security/security-tips/. Viitattu 6.10.2022.
- [2]NIST. “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1”, NIST Technical Series Publications, 16.4.2018, https://doi.org/10.6028/NIST.CSWP.04162018. Viitattu 6.10.2022.
- [3]Microsoft. “Microsoft AccountGuard -ohjelma”, Microsoft AccountGuard -ohjelma, https://www.microsoftaccountguard.com/en-us/. Viitattu 6.10.2022.
- [4]Google. “Lisäsuojaus-ohjelma”, Googlen Lisäsuojaus-ohjelma, https://landing.google.com/advancedprotection. Viitattu 6.10.2022.
- [5]Google. “Googlen turvallisuuskeskus”, Googlen turvallisuuskeskus – Turvallisempaa netin käyttöä, https://safety.google. Viitattu 6.10.2022.
- [6]Meta. “Basics: Help Secure Your Account.”, Help Secure Your Account, https://www.facebook.com/gpa/resources/basics/security. Viitattu 6.10.2022.
- [7]Meta. “Facebook Protect.”, Facebook, https://www.facebook.com/gpa/facebook-protect. Viitattu 6.10.2022.
- [8]NIST. “SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise”, NIST Technical Series Publications, https://doi.org/10.6028/NIST.SP.800-124r1. Viitattu 6.10.2022.
- Avainkoodit: https://developers.google.com/identity/passkeys
- CISAn Protecting Our Future -raportti kyberturvallisuudesta perus- ja keskiasteen oppilaitoksissa https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAOn raportti https://www.gao.gov/products/gao-20-644
- Jos haluat lisätietoja siitä, miten Google for Education voi auttaa suojaamaan oppilaitoksesi, tutustu Google for Educationin tietosuoja- ja tietoturvakeskukseen.
- Zcalerin raportti tietojenkalastelusta



Google for Education

Safer with Google