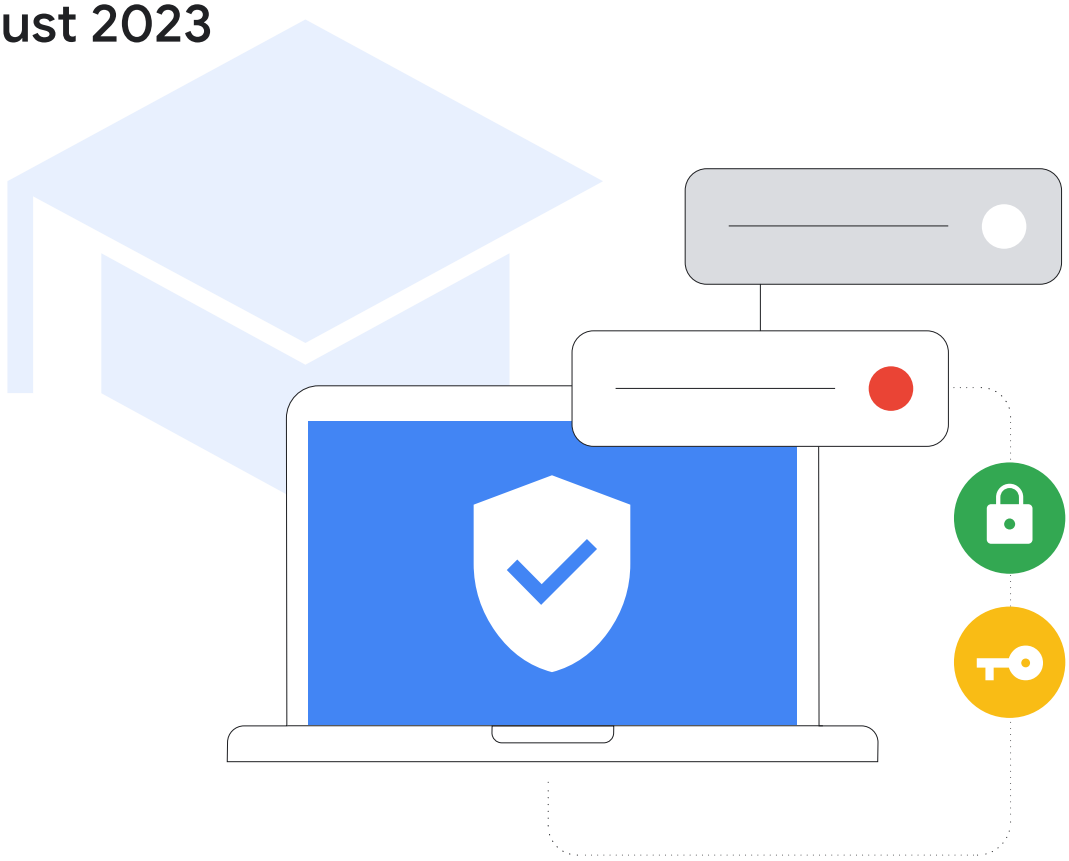
Google for Education

Håndbok i nettsikkerhet for grunnskolen og videregående skole

Oppdatert august 2023



Safer with Google

Sammendrag

CISAs rapport «Protecting Our Future» fremhever at det er helt avgjørende at grunnskoler og videregående skoler investerer i nettsikkerhet for å beskytte elever, familier, lærere, ansatte og lokalsamfunn. I dette dokumentet finner du veiledning og anbefalte fremgangsmåter for konfigurering av maskin- og programvare som IT-administratorer på skoler kan bruke for å styrke nettsikkerheten. Det inkluderer både generelle anbefalte fremgangsmåter og konkrete veiledninger for Google-produkter og -tjenester. Googles mål om å organisere all verdens informasjon og gjøre den tilgjengelig og nyttig for alle, er en viktig motivasjon når vi i Google for Education-teamet utvikler verktøy for undervisning og læring. I denne veiledningen skal vi dele ting vi har lært gjennom dette arbeidet.

Vi gir anbefalte fremgangsmåter for sikkerhet inndelt etter emne, med mer detaljerte innblikk i konfigurering, oppsett og strategier for risikobegrensning. I tillegg forklarer vi Googles tilnærming til nettsikkerhet for tjenestene våre, spesielt utdanningsverktøyene. Selv om den detaljerte veiledningen i dette dokumentet er relevant for alle produkter og tjenester, mener vi at våre egne produkter leveres med enestående beskyttelse mot vanlige angrep.

Risiko

Utdanningsinstitusjoner er blant de største målene for nettangrep, der useriøse aktører prøver å utnytte skolens store databeholdning for egen fortjeneste. 46 % av skoler som ikke har vært utsatt for slike angrep, tror at de kommer til å oppleve det med tiden, fordi angrep med løsepengevirus blir stadig mer sofistikerte og vanskeligere å stoppe. Og 42 % av disse skolene mener at løsepengevirus er så vanlige at et angrep er helt uunngåelig. Da skoler ble tvunget til en svært rask overgang til fjernundervisning i 2020, førte det til betydelige mangler i nettsikkerheten, slik at disse skolene ble sårbare for angrep.

Forsvar

Slike angrep kan motvirkes. Og selv om teknologi ikke kan fjerne risikoen helt, kan utdanningssektoren og selgere av utdanningsteknologi samarbeide om å ta i bruk og implementere anbefalte fremgangsmåter som skaper en trygg, sikker og omfattende tilnærming som reduserer risikoen betydelig. Med de rette forholdsreglene og retningslinjene for å beskytte brukerne, sikre enhetene og ivareta datapersonvernet kan utdanningsinstitusjoner håndtere risiko bedre og motvirke angrep.

De viktigste anbefalingene:

- **BRUK SIKKER AUTENTISERING** for å holde sensitiv informasjon trygg, beskytte e-post, filer og annet innhold og for å forhindre at uautoriserte brukere får tilgang til utdanningssystemer. Følg anbefalte fremgangsmåter for autentisering av brukere, inkludert sterke passord og totrinnsbekreftelse, passnøkler og løsninger for passordlagring der det er mulig, spesielt for IT-administratorer og ansatte som jobber med sensitiv informasjon.
- **BRUK RIKTIGE SIKKERHETSINNSTILLINGER** for å sikre brukerne, dataene og miljøet. Google-produkter har innebygd sikkerhet, men likevel er det helt avgjørende at administratorer bruker og konfigurerer nettverk og systemer på riktig måte for å ivareta sikkerheten. Skoler kan holdes sikre ved å bruke prinsippene om tillitsløshet og minimale rettigheter: Brukerne bør kun ha tilgang til programvaren, dataene, appene og systemene de trenger for å utføre arbeidet sitt effektivt.
- **OPPDATER OG OPPGRADER SYSTEMENE** for å sikre at brukerne er beskyttet mot de nyeste truslene. Bruk moderne operativsystemer (OS) og nettlesere, og sørg for at brukeren kjører de nyeste programvareversjonene på alle enheter (eller godkjente versjoner som har vært stabile lenge), og at de oppdateres automatisk. Oppgradering til en sikrere løsning, for eksempel Chromebook, kan gi bedre sikkerhet. Det har aldri vært oppdaget løsepengevirus på en ChromeOS-enhet.
- **BRUK SYSTEMER SOM VARSLER OG OVERVÅKER I SANNTID** for å bedre sikkerheten og håndtere potensielle problemer raskt. Du kan bruke innebygde funksjoner i hovedprogramvaren for samarbeid og kommunikasjon, for eksempel Google Workspace for Education, eller du kan implementere separate løsninger for sikkerhetslogging og -overvåkning. Sørg for omfattende sporing av aktivitet i hele skolenettverket samt alle enheter, apper, brukere og data. Hold øye med kontopålogging, fildeling, e-postvolum (spesielt forsøk på nettfisking og skadelig programvare), enhetsaktivitet og endringer av konfigurering. Hold løsningen for varsling og overvåkning oppdatert for å få varsler om trusler, kritiske hendelser og systemendringer.
- **GI LÆRERE, ANSATTE OG ELEVER OPPLÆRING** i hvordan de bruker enheter og programvare på en trygg måte, gjenkjenner og melder fra om potensielle trusler samt deler data på riktig måte for å bidra til å beskytte mot noen av de vanligste typene angrep. Skoler eller skoledistrikter kan lage opplæringsmateriell med egne grafiske elementer i tillegg til å bruke fritt tilgjengelig ferdiglaget materiell, og på den måten lage et omfattende verktøysett for skoler.

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

Anbefalinger spesielt for brukere av Google-produkter:

Googles produkter, for eksempel Google Workspace for Education og Chromebook, kan forbedre skolens nettsikkerhet og gjøre det enkelt å implementere hver av disse anbefalingene. Samlet tilbyr de en omfattende løsning som bidrar til å ivareta brukernes personvern og leverer den beste sikkerheten i sin kategori for institusjonen din.

Disse strategiene, kombinert med tilleggsveiledningen som følger senere, danner et utmerket grunnlag for sikkerhet i grunnskoler og videregående skoler.

Googles tilnærming til utdanning

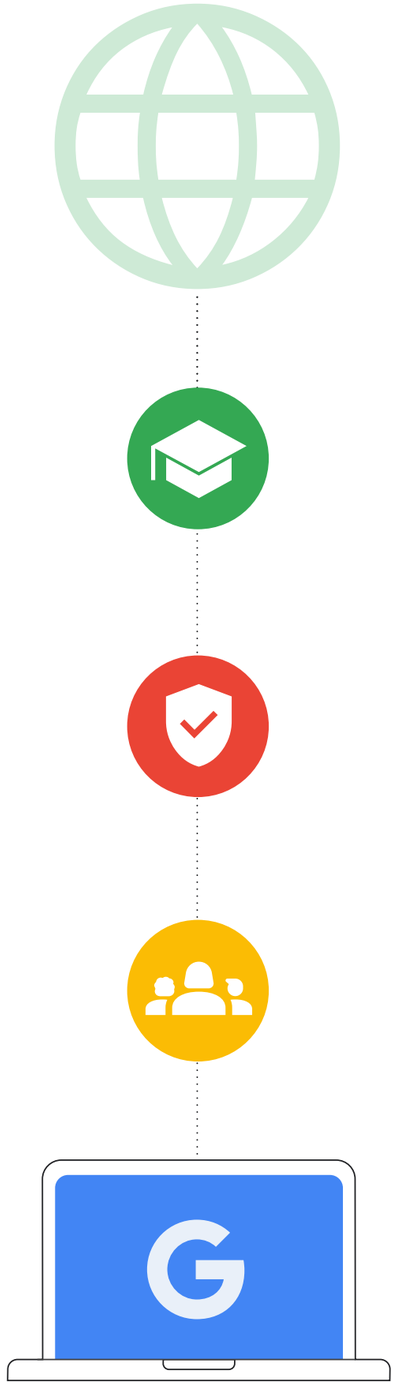
Google har som mål å organisere all verdens informasjon og gjøre den tilgjengelig og nyttig for alle, og dette er også tilfellet i utdanningssektoren. I Google for Education-teamet gjør vi dette ved å utvikle verktøy som Chromebook og Google Classroom, som gjør det enkelt og trygt for elever og lærere å skape, dele og organisere eget innhold samt få tilgang til og bruke utdanningsressurser og nettbaserte verktøy.

Skoler fortjener teknologi som er sikker som standard, har innebygd personvern, gir deg full kontroll og har pålitelig innhold og informasjon. Med produkter som Chromebook og Google Workspace for Education får skoler førsteklasses sikkerhet som overholder de strengeste globale standardene for utdanning. IT-administratorer får fullt innsyn i og enkel kontroll over data og retningslinjer for sikkerhet, og elevene kan leve seg helt inn i læringen i et tryggere digitalt miljø som viser innhold basert på alder, og som motarbeider nettsøppel og nettrusler.

Vi har prioritert innebygde sikkerhetsfunksjoner og -kontroller, personvernstandarder på høyeste nivå og muligheter for å bruke mer proaktive sikkerhetsverktøy for å sørge for at alle kan lære trygt. ChromeOS-enheter bidrar til å motvirke trusler skoler står overfor, og de er det beste forsvaret mot skolenes største trussel: løsepengevirus. Det har aldri forekommet et vellykket angrep med løsepengevirus mot en Chromebook.

Samtidig er Google Workspace for Education en av verdens mest populære og sikre skybaserte kommunikasjons- og samarbeidspakker. I den siste delen finner du mer informasjon om hvordan hver av dem ivaretar nettsikkerheten i forbindelse med disse anbefalingene.

Dette dokumentet består av to deler: Den første inneholder praktisk og generell sikkerhetsveiledning for grunnskoler og videregående skoler uavhengig av produktene de bruker, og den andre inneholder spesifikk veiledning om konfigurering for institusjoner som bruker Google for Education-produkter, for eksempel Google Workspace for Education og Chromebook. I begge delene finner du informasjon som kan bidra til å holde deg og elevene trygge på nettet.



Innledning

Grunnskoler og videregående skoler er utsatt for stor risiko for nettangrep, både mot enheter og i nettverk. Det er helt avgjørende at grunnskoler og videregående skoler bruker best mulige sikkerhetstiltak for å beskytte elevene og forhindre tapene av data, tjenester, ressurser, tid og penger som denne typen angrep kan medføre. (Kilde)

Denne veiledningen er et verktøy for å fremme anbefalte fremgangsmåter for nettsikkerhet som skoleadministratorer og skolesystemer kan implementere for å sikre miljøet bedre. Ved å iverksette disse anbefalte fremgangsmåtene kan grunnskoler og videregående skoler håndtere eller forhindre alvorlige og kostbare nettangrep på utdanningssystemer og beskytte elever, familier, lærere og ansatte.

Nettangrep på skoler blir stadig vanligere og mer alvorlige. Ifølge K-12 Cybersecurity Resource Center var det over 1300 offentliggjorte sikkerhetshendelser på nettet der utdanningsorganisasjoner var involvert, i alle 50 delstater i USA mellom 2016 og 2021. Dagens utdanningsledere må beskytte dataene og personopplysningene til elever, lærere og ansatte, i tillegg til institusjonens systemer og informasjon. Det er en stor oppgave, spesielt med tanke på at utdanningssektoren tradisjonelt har hatt større vansker med å opprettholde nettsikkerheten enn andre sektorer.

Vellykkede nettangrep (for eksempel løsepengevirus, nettfisking eller skadelig programvare) kan føre til omfattende databrudd knyttet til personlig identifiserende informasjon (PII), store økonomiske konsekvenser (en gjennomsnittlig løsepengebetaling er nå fem ganger så stor som i 2020: USD 812 260) og langvarige forstyrrelser eller avbrudd av undervisning og annen skoledrift. Et nylig angrep med løsepengevirus satte hele systemet på en skole ut av spill, noe som skapte ringvirkninger i hele lokalsamfunnet fordi elevene ikke kunne gå på skolen på flere dager. Begrensede ressurser og midler betyr at grunnskoler og videregående skoler fortsatt kommer til å være utsatte mål for opportunistiske aktører, med mindre det investeres i bedre nettsikkerhet.

Best nettsikkerhet oppnås alltid gjennom kommunikasjon, samarbeid og partnerskap. Dette dokumentet er satt sammen av Googles trygghets- og sikkerhetstips, rammeverket for nettsikkerhet (Cybersecurity Framework) fra National Institute for Standards and Technology (NIST) og CISA K-12 Cybersecurity Toolkit and Recommendations for 2023 – generelt anerkjente ressurser om hvordan man bør gå frem for å bedre nettsikkerheten. Dokumentet omtaler generelle tiltak IT-administratorer bør iverksette eller vurdere, og noen av Googles egne anbefalte fremgangsmåter og veiledninger for produktene våre. I tillegg henviser det til sikkerhetstips og -tjenester fra andre selskaper. Administratorer bør gå gjennom all sikkerhetsveiledning som leveres av de relevante selskapene, og implementere de nyeste rådene, siden det ansvarlige selskapet er best egnet til å beskrive egne produkter og eventuelle endringer som kan ha skjedd.

Før du iverksetter tiltak i tråd med anbefalingene nedenfor, bør du også tenke over faktorene som er nevnt der:

Ting du bør ta med i vurderingen

1. **Beskyttelse av elevene.**
   Hver skole har sine behov, og noen grupper kan trenge ekstra tiltak for å beskytte sikkerheten og ivareta personvernet. Mange undervisningsverktøy har funksjoner som kan hjelpe med aldersbasert tilgang, som begrensning av upassende innhold eller sikring av posisjonsdata eller kontaktinformasjon.
2. **Hvilke typer data du lagrer.**
   Hvis du lagrer sensitive data, bør du kanskje kryptere dem eller lagre dem på et eget sted.
3. **Enhetstypene og implementeringsmodellen du bruker.**
   Enheter og appene på dem bør få automatiske oppdateringer for best mulig sikkerhet, og de bør kryptere data og isolere kontoer for å sikre at brukerne kun har tilgang til sin egen informasjon.
4. **Retningslinjene til skolen, skoledistriktet, kommunen eller fylket.**
   Det kan hende skolen din har konkrete retningslinjer for bruk av teknologi. Du må sørge for at alle sikringstiltak er iverksatt i henhold til disse retningslinjene.

Hver dag blir
100 millioner
forsøk på nettfisking blokkert av Gmail.

Hver uke blir
300,000
utrygge nettsteder identifisert av Google.

Hver dag får
74 millioner
brukere hjelp via Google Passordlagring.

Hvert år styrker
700 millioner
mennesker sikkerheten sin med Sikkerhetssjekk.

Generelle sikkerhetsråd

Bruk sikker autentisering

Sikker autentisering må prioriteres høyt av skoler og andre institusjoner. I fjerde kvartal av 2022 var kontoer med svak eller ingen legitimasjon ansvarlige for 48 % av alle årsaksfaktorer ved sikkerhetsbrudd. Implementering av noen viktige anbefalinger kan bidra til å bekrefte at brukerne er personene de utgir seg for å være, og begrense tilgangen til informasjon basert på hver brukers rolle.

IT-administratorer bør ta i bruk obligatorisk totrinnsbekreftelse og gå over til autentisering uten passord (for eksempel passnøkler) der det er mulig, og spesielt når noen skal ha ekstern tilgang til utdanningsinstitusjonens systemer. Med totrinnsbekreftelse får nettkontoer et ekstra sikkerhetslag, slik at det blir mye vanskeligere for angripere å få tilgang.

Skoler bruker mange ulike enhetstyper og implementeringsmodeller, og nivået på tekniske ferdigheter i grunnskoler og videregående skoler er varierende. Konto- og enhetssikkerhet varierer mellom ulike brukerroller og -typer med definerte anbefalte fremgangsmåter: IT-administratorer, lærere og ansatte, eldre elever som bruker tildelte enheter, og yngre elever som bruker delte enheter. Vi omtaler konkrete anbefalinger for hver av gruppene nedenfor.

Det finnes flere autentiseringsmetoder som kan anbefales i de fleste situasjoner:

- **Sterke passord**
  Be brukerne om å lage sitt eget passord første gang de logger på, og krev en viss lengde og kompleksitet. Lange passordfraser gir et ekstra sikkerhetselement på grunn av lengden og bruk av komplekse tegn. Brukerne bør ikke pålegges å bytte passord regelmessig, fordi det oppmuntrer til bruk av enkle passord eller uvesentlige endringer (som å oppdatere ett tegn).
- **Totrinnsbekreftelse**
  Med totrinnsbekreftelse blir kontoen beskyttet med et ekstra trinn – ofte noe brukeren har med seg, som en sikkerhetsnøkkel eller en app på mobilen som lager en engangs bekreftelseskode. Selv om alle former for totrinnsbekreftelse gir kontoer ekstra sikkerhet, bør administratorer unngå bruk av bekreftelseskoder som sendes via SMS eller anrop, siden de kan være utsatt for angrep basert på telefonnumre.
- **Autentisering uten passord**
  Passnøkler er tryggere og enklere enn passord. Brukerne kan logge på apper og nettsteder med en PIN-kode, et mønster, en biometrisk sensor (som fingeravtrykk eller ansiktsgjenkjenning) eller en sikkerhetsnøkkel. På den måten slipper de å huske og administrere passord. Selv om disse løsningene kanskje ikke egner seg i alle utdanningsinstitusjoner, erstatter de i stadig større grad tradisjonelle autentiseringsformer, og de gir raskere og tryggere pålogging. Med passnøkler beskyttes brukerne mot nettfiskingsangrep fordi de bare fungerer på nettstedene og appene de er registrert for.
- **Global pålogging**
  Med global pålogging kan brukerne få tilgang til flere apper og nettsteder med samme legitimasjon. Når brukerne bare trenger å huske ett sett med legitimasjonsopplysninger, er det mindre sannsynlig at de skriver dem ned. Og når skoler ikke må administrere flere sett med legitimasjonsopplysninger for brukerne, kan de spare penger på kostnader til IT-brukerstøtte. Google Workspace for Education har innebygd støtte for global pålogging, slik at brukerne kan bruke Google-kontolegitimasjonen sin til å logge på tredjepartsapper, eller bruke legitimasjonen fra en annen leverandør til å logge på Google-kontoen sin.
- **Passordlagring**
  Løsninger for passordlagring hjelper brukerne med å lage sterke, unike passord for ulike kontoer og tjenester de bruker i løpet av skole- eller arbeidsdagen (der de ikke bruker global pålogging). De hjelper ikke med å logge på operativsystemet på enheter, men de kan holde styr på passord etter at brukeren har logget på. Google-brukere kan bruke passordlagring i Chrome på alle plattformer, ChromeOS og Android.

Egne delsett eller kombinasjoner av disse autentiseringsalternativene kan brukes for ulike gruppers unike behov, basert på rollen de har i utdanningsinstitusjonen, typen systemer og data de har tilgang til, og hvor gamle de er.

Skoleadministratorer

Systemene og mye av dataene for grunnskoler og videregående skoler blir styrt av administratorer. Beskyttelse av administratorkontoer er helt avgjørende for hele systemets sikkerhet – fra infrastruktur via kontodata til enheter som administreres av institusjonen. Derfor bør de bruke gullstandarden for autentisering, inkludert sterke passord, en robust løsning for passordlagring og totrinnsbekreftelse. Hvert av disse elementene danner et lag med beskyttelse, og kombinert gir de den beste sikkerheten for administratorkontoen og bedriftstjenestene.

- Administratorer må bruke en fysisk sikkerhetsnøkkel eller en kryptografisk sikker metode for totrinnsbekreftelse som krever en godkjent enhet og forespørsler. Dette kan omfatte en tjeneste som Google Autentisering eller en annen app som genererer engangskoder for bekreftelse. Chromebook-enheter produsert etter 2019 med en TPM-brikke, har en strømknapp som kan brukes til totrinnsbekreftelse.
- Administratorer bør bruke en klarert løsning for passordlagring som støtter totrinnsbekreftelse, til å lagre passord for ulike tjenester.

Lærere og ansatte som bruker tildelte enheter

I likhet med administratorer har lærere og ansatte tilgang til sensitive data, men de har ikke kontroll over den digitale infrastrukturen, og de tekniske ferdighetene varierer mer.

- Lærere og ansatte som bruker Chromebook, bør få muligheten til å logge på med biometrisk bekreftelse der det er tillatt ved lov, for eksempel med fingeravtrykk.
- Administratorer bør ta i bruk obligatorisk totrinnsbekreftelse og gå over til autentisering uten passord der det er mulig, og alltid når ansatte logger på utdanningsinstitusjonens systemer utenfra.

Eldre elever som bruker tildelte enheter (vanligvis 4. klassetrinn og oppover)

Eldre elever har lært mer om hvordan de skal beskytte seg, og de er vanligvis i stand til å bruke mer beskyttende metoder for autentisering som egner seg for typen tjenester de ofte bruker. De bør kun ha tilgang til egen konto og informasjon som er delt med dem.

- Elever som bruker Chromebook, bør ha muligheten til å opprette en PIN-kode for en spesifikk enhet for raskere pålogging på den. Det er ikke sikkert at biometriske alternativer egner seg eller er mulig i mange skolemiljøer.
- Hver elev bør få hjelp til å opprette et unikt passord som ikke inneholder personopplysninger (for eksempel navn, klasserom eller fødselsdato). Elevene bør få opplæring i hvordan bruk av passordfraser kan gjøre passordet både mer komplekst og lettere å huske.

Yngre elever som bruker delte enheter (vanligvis til og med 3. klassetrinn)

De yngste elevene lærer fortsatt hvordan de bruker undervisningsteknologi, og de bør ha en enkel autentiseringsmetode som egner seg til bruk med begrensede tjenester og data.

- Skoler som bruker passordalternativer fra tredjeparter for de yngste elevene og elever som ikke kan logge på med passord, for eksempel QR-koder eller bildepålogging, bør ha forholdsregler for sikkerhet, siden disse alternativene er mindre sikre. Administratorer bør endre elevers passord og oppdatere koden hver gang en kode har gått tapt eller potensielt blitt formidlet til andre.
- Skoler bør lære både elever og foreldre hvor viktig det er å holde passord hemmelig og oppbevare andre typer legitimasjon, for eksempel QR-koder, på en sikker måte.
- For tildelte enheter som nettbrett, kan en egen PIN-kode for hver enhet brukes som en alternativ, sikker autentiseringsmetode.

Bruk passende sikkerhetsinnstillinger

Skoleenheter og -nettverk er godt synlige og verdifulle mål for angripere verden over, så det er helt avgjørende å bruke best mulige sikkerhetstiltak for å forhindre tap av tjenester, ressurser, tid og penger. Systemadministratorer bør implementere effektive og passende sikkerhetsfunksjoner i produktene institusjonen bruker, men de må også sørge for at systemene likevel er enkle å bruke for lærere, ansatte og elever. Viktige sikkerhets- og personverninnstillinger bør konfigureres slik at enkeltbrukere ikke kan slå dem av eller endre dem, og andre innstillinger bør ha beskyttende standardinnstillinger angitt av administratoren. Det er svært viktig å bruke så gode sikkerhetstiltak som mulig for å forhindre tap av tjenester, ressurser, tid og penger. Hvis dere bruker Chromebook, finner du forslag til enhetsregler i det siste kapittelet.

Til slutt: Bygg inn «dataminimering» i skolens praksis ved å begrense tillatte årsaker og tilgjengelige metoder for innhenting, bruk og videreformidling av personopplysninger proporsjonalt med det som er nødvendig for å levere tjenesten, eller som på andre måter er i tråd med forholdets kontekst.

Apper og oppdateringer

Begrens hvilke apper brukerne har lov til å installere, og reduser antallet til et minimum, siden hver app som installeres på en enhet, er en mulig angrepsvektor som kan utnyttes. Bruk om mulig apper fra pålitelige kilder. Du kan for eksempel anbefale at brukerne ser etter bekreftelsesmerket i Google Play-butikken for å sikre at de laster ned de offisielle appene som har gjennomgått en sikkerhetsvurdering. All modifisering av OS eller maskinvare (jailbreaking eller bruk av rottilgang) skaper betydelige sikkerhetshull og bør unngås.

Tilgang og innsyn

Administratorer bør sørge for at brukerne bare har tilgang til dataene, programvaren, tjenestene og systemene de trenger for å gjøre jobben sin eller lære effektivt. Dette bidrar til å begrense utilsiktet tilgang og spore hvem som har tilgang til hvilke ressurser. Vær spesielt oppmerksom på svært sensitive data, for eksempel brukernes personlig identifiserende informasjon (PII), og systemer (som HR, lønnssystemer, karaktersetting, sikkerhet og konfigurering). Du kan spore hvilke brukere som har tilgang til dataene, og i hvilke omstendigheter, ved å begrense tilgangen til enheter skolen eier. Du kan også sørge for at kun bestemte ansatte har tilgang.

Gå gjennom reglene for deling av data i samarbeidsverktøy for å forhindre upassende eller overdreven deling og uautorisert tilgang. Begrens eller blokker deling utenfor miljøet (spesielt for elever), og slå på regler som overvåker deling av sensitivt innhold.

Tap eller tyveri av enheter

Selv om du mister en enhet, betyr ikke det nødvendigvis tap av data. Administratorer bør standardisere en plan for å sikre tilgang til informasjon og dokumenter hvis en enhet forsvinner eller blir stjålet. Dette kan for eksempel være lagring av dokumenter i nettskyen. Last ned og skriv ut reservekoder for prosessene for totrinnsbekreftelse, slik at det ikke blir avbrudd i kontotilgangen.

Når enheter rapporteres som mistet eller stjålet, må du sørge for at de fjernlåses hvis det er mulig, og at tilknyttede kontoer låses eller merkes for å sikre at de ikke brukes til å få uautorisert tilgang. Chromebook-enheter kan fjernutviskes hvis de går tapt, og Google Workspace for Education-kontoer kan overvåkes for mistenkelig aktivitet eller om nødvendig sperres (låses).

Avansert beskyttelse for brukere med høy risiko

For brukere som er veldig synlige og har tilgang til sensitiv informasjon (for eksempel Google Workspace for Education-administratorer), tilbyr Google Avansert beskyttelse-programmet. Med Avansert beskyttelse-programmet får brukerne ekstra beskyttelse mot målrettede angrep, for eksempel forsøk på nettfisking, skadelige nedlastinger og passordbrudd. Avansert beskyttelse-programmet er utviklet spesielt for å stoppe målrettede nettangrep på Google-kontoer. Det bruker automatisk sterk autentisering og sikkerhetsnøkler, og det begrenser tredjepartstilgang til kontodata. Andre leverandører av nettkontoer tilbyr også ekstra kontobeskyttelse for brukere med høy risiko, og administratorer og ansatte bør alltid bruke disse mulighetene hvis de har tilgang til personopplysninger eller teknologisystemer.

Oppdater og oppgrader systemene

Et av de viktigste tiltakene alle kan iverksette for å beskytte seg, er å holde operativsystemet og appene på enheten oppdatert. Dette er enda viktigere for skoler, siden de er en så viktig del av barns utdanning og hverdagsliv. De fleste angrep med skadelig programvare har vært Windows-baserte, både på utdanningsinstitusjoner og i andre sammenhenger med høy risiko. Dette inkluderer SolarWinds, løsepengevirusangrepet på Los Angeles Unified School District, hackingen av Little Rock School District, databruddet på Microsoft Exchange Server, angrepet med løsepengevirus på Albuquerque School District og det nylige Microsoft-sikkerhetsbruddet i føderale offentlige organer. Dette er et annet område der bruk av nettskybaserte produkter og tjenester bør gjøre administratorens jobb enklere ved å redusere angrepsflaten og sikre at systemene og appene holdes oppdatert automatisk.

Oppgrader til et moderne operativsystem, og hold det oppdatert

Den nyeste versjonen av et operativsystem (OS) inneholder vanligvis nye sikkerhetsfunksjoner som bidrar til å forhindre kjente angrepsvektorer. Du bør slå på funksjoner for automatisk oppdatering i enhetens OS. Hvis det ikke er mulig, kan du laste ned og installere patcher (feilrettinger) og oppdateringer fra en pålitelig leverandør minst én gang i måneden.

Chromebook-enheter kjører ChromeOS, så de får ofte automatiske oppdateringer med de nyeste sikkerhetspatchene. Dermed tas de siste nyvinningene innen sikkerhet i bruk tidlig. I tillegg bekrefter enhetene integriteten til det skrivebeskyttede operativsystemet før oppstart. Dataene som lagres på enheten, krypteres også, slik at de beskyttes mot uautorisert tilgang. Alle nettsider og apper kjøres i en egen sandkasse, slik at eventuell skadelig programvare ikke kan spres til andre deler av enheten.

Hvis skolen din ikke er klar for å gå over til Chromebook, er ChromeOS Flex en versjon av ChromeOS som er utviklet for å modernisere skolens enheter. Med ChromeOS Flex får alle en ensrettet og moderne undervisnings- og læringsopplevelse med proaktive, innebygde muligheter for administrering av sikkerheten og nettskyen. Flex kan gi automatisk beskyttelse og blokkere skadelige kjørbare filer og apper, uten at du trenger å kjøpe ny maskinvare.

Oppgrader til en moderne nettleser, og hold den oppdatert

Det er viktig at nettleseren også er oppdatert og sikker. Moderne nettlesere har mer avanserte sikkerhetsfunksjoner og kan gi brukeren meldinger om hvordan de enkelt slår dem på. De kan også konfigureres av administratorer slik at disse funksjonene slås på som standard på institusjonens datamaskiner og bidrar til å beskytte sensitiv informasjon som overføres via internett. Nettleseren må holdes oppdatert. Uansett om det er til jobb, læring eller andre aktiviteter på nettet, gir en oppdatert, moderne nettleser disse fordelene:

- **Den bruker robust sikkerhet,** inkludert isolering av nettsteder og beskyttelse for sikker surfing som forhindrer at brukere utilsiktet åpner farlige nettsteder.
- **Den har muligheter for automatiske oppdateringer** slik at nettleseren får sikkerhetsoppdateringer raskt.
- **Den sørger for sikre tilkoblinger.** Moderne nettlesere bruker som regel Transport Layer Security (TLS), og brukeren kan klikke ved siden av nettadressen og sjekke at tilkoblingen er merket som sikker.

Chrome er utviklet med sikkerhet i tankene, og sikkerhetsfunksjoner som Safe Browsing (sikker surfing) er slått på som standard. I tillegg har den en integrert løsning for passordlagring som kan fylle ut passord automatisk for deg på nettet, slik at det blir lett å bruke sterke passord.

Bruk systemer som varsler og overvåker i sanntid

Systemer som varsler og overvåker i sanntid, kan hjelpe skoler med å oppdage og reagere på trusler raskt – før de får gjort skade. Det er viktig å sørge for at sikkerhetssystemer kjører i bakgrunnen, der de registrerer og loggfører sikkerhetshendelser fra alle systemer. AI-verktøy er spesielt godt egnet til å gå gjennom de store mengdene innhentede data og finne avvik og mønstre. Dette kan brukes til å oppdage trusler raskere og enklere, og til å behandle og håndtere sårbarheter. På den måten kan IT-administratorer eller ansatte prioritere aktivitetene som må gjennomgås.

Skoler kan bruke varslings- og overvåkningsfunksjoner som er innebygd i samarbeids- og kommunikasjonsprogramvaren de bruker mest, for eksempel Google Workspace for Education. De kan også implementere separate løsninger for SIEM (administrasjon av sikkerhetsinformasjon og -hendelser).

Systemer for varsling og overvåkning i sanntid kan spore mange forskjellige aktiviteter for skolens nettverk, enheter, apper, brukere og data. Dette kan være brukerpåloggінger, tilgang til filer, mulige inntrengninger, vellykkede eller mislykkede forsøk på tyveri av data samt administratoraktiviteter.

Hvis systemet registrerer mistenkelig aktivitet, kan et varsel sendes til skolens IT-ansatte. Dette betyr at administratorer kan etterforske saken og iverksette tiltak for å håndtere trusselen.

I tillegg kan verktøy for varsling og overvåkning brukes til å få bedre forståelse av truslene skoler står overfor. Ved å analysere data fra disse sanntidssystemene kan skoler finne trender og mønstre som kan hjelpe dem med å beskytte seg bedre.

Her er noen anbefalte fremgangsmåter for bruk av systemer for varsling og overvåkning – inkludert SIEM-systemer (administrasjon av sikkerhetsinformasjon og -hendelser):

1. **Definer sikkerhetsmål**
   Identifiser informasjonen og systemene som er viktigst for skolen, og hvilke typer trusler som utgjør den største risikoen for dem. Deretter finner du ut hvilke data som må innhentes for å følge med på de aktuelle truslene.
2. **Samle inn de riktige dataene, og bruk egnet konfigurering**
   Det er viktig å samle inn de rette dataene og konfigurere apper på en måte som håndterer de mest relevante sikkerhetsmålene. Dette kan inkludere data fra brannmurer, innholdsfiltre, systemer for oppdaging av inntrengning, nettjenere og andre sikkerhetsenheter, i tillegg til kommunikasjons- og samarbeidsprogramvare, systemer for elevinformasjon og læringsplattformer.
3. **Undersøk og reager på varsler**
   Når overvåkningssystemet genererer et varsel, er det viktig å undersøke saken og iverksette aktuelle tiltak. Dette kan innebære at flere ulike team samarbeider om å undersøke kilden til varselet, avgjøre om det er falsk alarm eller iverksette tiltak for å håndtere trusselen. Slike tiltak kan for eksempel være sperring av kontoer, tilbakestilling av brukerpassord, bruk av karantene for e-post, sletting av e-post, endring av filtillatelser eller utvisking av enheter.

Lær opp lærere, ansatte og elever

Grunnskoler og videregående skoler bør jobbe for å øke skolemiljøets bevissthet rundt sikkerhet og skape bedre sikkerhetsvaner blant brukerne ved hjelp av kampanjer og partnerskap. Det er avgjørende å informere lærere, ansatte og elever om betydningen av sikkerhet for å kunne hjelpe dem med å beskytte seg på nettet, og det bidrar dessuten til å hindre alvorlige trusler mot nettsikkerheten. Lær dem hvordan de bruker produktene og tjenestene institusjonen tilbyr, hvordan de oppdager og rapporterer trusler som nettfiskings-e-poster, og – viktigst av alt – hva de kan gjøre for å forhindre denne typen angrep. Skoler, skoledistrikter, kommuner og fylker bør jobbe for å øke skolemiljøets bevissthet rundt sikkerhet og skape bedre sikkerhetsvaner blant brukerne ved hjelp av kampanjer og partnerskap.

Trygg bruk av enheter og programvare

Administratorer kan samarbeide med lærere og eksperter om å utvikle pensum om nettsikkerhet som er egnet for de ulike aldersgruppene. Dette kan hjelpe elevene med å forstå hvordan de kan bruke enheter, programvare og systemer på en trygg og sikker måte. Hvis du lager opplæringsmateriell med skolens eller distriktets logo, kan det gjøre anbefalingene mer gjenkjennelige for elevene og lærerne. Men du kan også bruke ferdigprodusert materiell, for eksempel Be Internet Awesome på Safety.Google eller materiellet på Khan Academy, og tilpasse det etter behov. Disse programmene kan hjelpe brukerne med å holde seg trygge uansett hvor de er – på skolen eller hjemme.

Gjenkjenning av trusler

Det er viktig å lære opp lærere, ansatte og elever i gjenkjenning av trusler for å beskytte dem. Barn må lære hvordan de skiller trusler fra det trygge, for det er ikke sikkert at de vet hvordan de kan se om ting er ekte. Det finnes noen typer trusler de bør kunne kjenne igjen og forstå hvordan de rapporterer, og administratorer bør fokusere på emnene de tror de får mest igjen for. Vær obs på at opplæringen ikke bare skal lære brukerne å kjenne igjen trusler, men også å handle. Vanlige trusler brukerne bør kunne kjenne igjen, er blant annet løsepengevirus, nettfisking, sosial manipulering, skadelig programvare og svindel – men hvis bestemte trusler er vanligere på den aktuelle institusjonen, er det viktig å sørge for at hele skolemiljøet er informert om dem.

Sikker data- og fildeling

Lærere og ansatte bør få opplæring i hva som er passende deling av filer og data, og hvordan de kan kjenne igjen upassende forespørsler via e-post. En avgjørende faktor er å sørge for at sensitive personopplysninger bare deles eller behandles når det er nødvendig, og med ekstra beskyttelseslag for dataene. De må for eksempel aldri deles via e-post eller med eksterne parter. De bør bruke funksjoner for forebygging av datatap (inkludert i ChromeOS og Workspace for Education) til å advare brukere og forhindre at de deler filer med sensitive data (for eksempel personnumre) eller kopierer og limer inn sensitivt innhold utenfor domenet.

Googles tilnærming i praksis: Enheter og tjenester for utdanning

Kjøp av programvare er et av de mest effektive verktøyene skoledistrikter har for å beskytte seg. Programvare bør ha robust arkitektur og design med sikkerhet innebygd i hvert eneste lag for å redusere risikoen for sårbarheter til et minimum. Ved å kreve at skoler kjøper sikker programvare eller programvare fra selskaper med en dokumentert tradisjon for god sikkerhet, kan den generelle nettrisikoen reduseres betydelig. Hos Google har vi for eksempel forsterket ChromeOS, samtidig som vi kontinuerlig implementerer mer proaktive og intelligente løsninger som bruker styrken fra ekspertisen vår innen maskinlæring, nettsky og identitet.

Google Workspace for Education

Google Workspace for Education er en samling med Google-verktøy og -tjenester som er spesielt tilpasset skoler, for å styrke samarbeidet, effektivisere undervisningen og opprettholde et trygt læringsmiljø. Google for Education-produktene og -tjenestene beskytter kontinuerlig brukere, enheter og data mot stadig mer kompliserte trusler. De inneholder verktøy som varsel- og sikkerhetssentre, et arkiv for e-discovery, administrering av identiteter og tilgang samt forebygging av datatap.

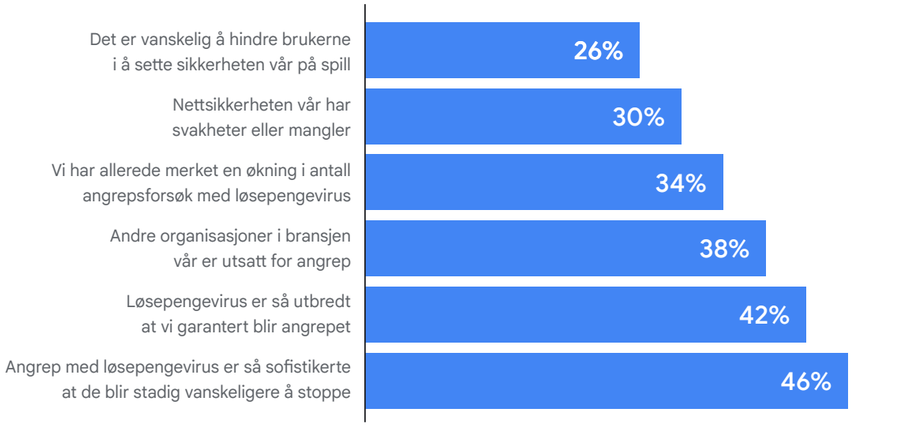
Vi har samlet nyttig materiell hvis Google Workspace for Education er nytt for deg, og mye av innholdet der kan hjelpe deg med å konfigurere ting i henhold til disse anbefalingene. I denne hurtigstartveiledningen for IT-konfigurering finner du hjelp med å komme i gang med Google Workspace for Education.

Google jobber hele tiden med å utvikle produkter som ivaretar elevers og læreres personvern, og sørge for førsteklasses sikkerhet for institusjonene som bruker dem. Du kan føle deg trygg på at Google for Education-produktene og -tjenestene kontinuerlig beskytter brukere, enheter og data mot stadig mer kompliserte trusler. I denne delen finner IT-administratorer en gjennomgang av sikkerhetsanbefalingene våre ved bruk av Google for Education-produkter.

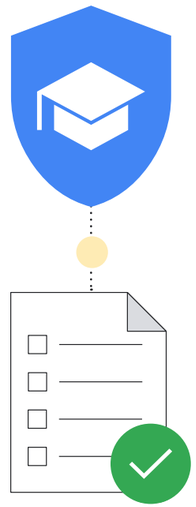
Sjekklister for sikkerhet

Gjennomgå sjekklistene for sikkerhet for å finne ut mer om hvordan du styrker sikkerheten og personvernet for institusjonen din. Skoler med Standard- og Plus-utgaven av Google Workspace for Education kan også bruke Sikkerhetstilstand-siden til å holde øye med konfigureringen av innstillingene i administrasjonskonsollen. Du kan for eksempel sjekke statusen for innstillinger som automatisk videresending av e-poster, enhetskryptering, delingsinnstillinger for Disk og mye mer. Om nødvendig kan du justere innstillingene for domenet basert på generelle sikkerhetsretningslinjer og anbefalte fremgangsmåter, samtidig som du veier disse retningslinjene opp mot organisasjonens forretningsbehov og retningslinjer for håndtering av risikoer.

Hvorfor utdanningssektoren forventer å bli angrepet



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



Her er noen andre nyttige tips for å sikre at du får mest mulig utbytte av beskyttelsen som er innebygd i Google Workspace for Education:

Konfigurer organisasjonsenheter (OE-er)

Alle i Google Workspace for Education-kontoen din trenger ikke å ha de samme innstillingene. Organisasjonsenheter er brukergrupper du kan tildele ulike tjenester, innstillinger og tillatelser. Du kan for eksempel bruke totrinnsbekreftelse for lærere og ansatte, mens unge elever får en autentiseringsmetode som egner seg for dem. Konfigurer egne organisasjonsenheter for ansatte, lærere og elever, slik at du kan bruke ulike regler for hver enkelt brukergruppe. God struktur er svært viktig for effektiv og fleksibel administrering av Google Workspace for Education-kontoen.

Konfigurer regler for passord og beskyttelse for administratorkontoer

Som nevnt er brukerautentisering en avgjørende del av institusjonens sikkerhet. Derfor har administratorer fleksible administreringsmuligheter for autentisering, slik at du kan sørge for at brukerne har velegnet og sikker kontobeskyttelse. Angi regler for passord for å sikre at brukerne lager sterke passord, og vurder å kreve totrinnsbekreftelse der det passer, basert på de anbefalte grupperingene i delen om global pålogging. Du kan ta i bruk obligatorisk totrinnsbekreftelse for en undergruppe med brukere (gi dem tid til å konfigurere det) og implementere totrinnsbekreftelse via flere ulike metoder. Dette kan være sikkerhetsnøkler (sikrest), en forespørsel fra Google (ved hjelp av Googles apper på Android og iOS), en app som generer bekreftelseskoder (for eksempel Google Autentisering), eller tekstmeldinger eller telefonanrop (men dette er den minst sikre metoden).

Hvis organisasjonen din bruker en annen identitetsleverandør enn Google, kan du konfigurere global pålogging via en tredjeparts identitetsleverandør. Du kan fortsatt bruke totrinnsbekreftelse med global pålogging for administratorkontoer som ikke tilhører superadministratorer, hvis du foretrekker det.

Slå tjenester på eller av

Administratorer kan bruke Google Administrasjonskonsoll til å styre hvilke Google-tjenester brukerne får tilgang til med Google Workspace for Education-kontoen sin. Du kan styre tilgangen til Google-tjenester som Kalender, Disk og Meet ved å slå tjenester på eller av per organisasjonsenhet (OE) (du kan også slå på tjenester ved bruk av grupper). I tillegg kan du gå gjennom forskjellene mellom kjernetjenester og tilleggstjenester i Workspace før du slår på tilleggstjenester som YouTube, Google Maps og Blogger. Vi anbefaler at administratorer konfigurerer tilgang til Google-tjenester basert på alder. Vær oppmerksom på at brukere som er klassifisert som under 18 år, har automatiske begrensninger i noen Google-tjenester når de er logget på Google Workspace for Education-kontoen sin.

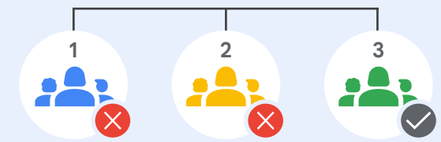
Du kan også bruke kontekstsensitiv tilgang (tilgjengelig i Workspace for Education Standard og Plus) til å tillate eller nekte tilgang til Google-apper som Gmail, Disk og Kalender basert på enhetens IP-adresse, geografiske opprinnelse, sikkerhetsregler eller OS. Du kan for eksempel tillate Disk for datamaskiner kun på bedriftseide enheter i bestemte land eller regioner.

Metoder for å gi brukere tilgang til tjenester

I Google Administrasjonskonsoll kan du slå av tilgangen til en Google-tjeneste, for eksempel Google Disk, for en organisasjonsenhet. Hvis noen av brukerne i den aktuelle organisasjonsenheten må bruke Disk, har du to valg:

1. Du kan flytte brukerne til en organisasjonsenhet som Disk er slått på for.
2. Du kan legge til brukerne i en tilgangsgruppe og slå på Disk for denne gruppen. Alle medlemmene har tilgang til tjenesten selv om den er slått av for organisasjonsenheten deres.

Organisasjonsenheter



Google Disk er slått av for organisasjonsenhet 1 og 2.

I en tilgangsgruppe

En **gruppe brukere** i organisasjonsenhet 1 og 2 kan likevel bruke Google Disk.

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

Angi regler for deling og oppbevaring av data

Som administrator kan du styre om brukerne kan dele Google Disk-filer og -mapper med folk utenfor organisasjonen. Dette kan bidra til å forhindre utilsiktet eller for vidstrakt deling av data og filer, og dermed forhindre datalekkasjer. Atskillelse av filer og disker, oppretting av organisasjonsenheter og drift i henhold til prinsippet om minst mulig rettigheter er viktig for å forhindre at angripere beveger seg videre gjennom nettverket hvis de infiltrerer én konto. Jo mindre data og nettverkstilgang potensielle angripere får tilgang til, desto mindre skade kan de forårsake.

Slå av ekstern fildeling for elever (eller begrens ekstern deling til kun tillatte domener), og velg «Bare mottakerne» for «Tilgangskontroll». Hvis du tillater at noen eller alle brukere kan dele filer utenfor domenet, bør du slå på en advarsel når brukerne gjør dette. I tillegg bør du slå av publisering av filer på nettet og kreve at eksterne samarbeidspartnere logger på med en Google-konto.

I tillegg kan Workspace for Education Standard- og Plus-kunder bruke målgrupper og klareringsregler til å angi delingsanbefalinger og -begrensninger på et mer granulært nivå. Med målgrupper kan du for eksempel sette standardmålgruppen for deling av linker fra lærere til «lærere og ansatte» i stedet for alle i institusjonen. Med klareringsregler kan du blokkere barneskoleelever fra å dele filer med eldre elever.

Gå gjennom retningslinjene for delte disker for å sikre at kun de riktige brukerne kan opprette delte disker, og forhindre eksterne brukere fra å lese delte disker. Vi anbefaler at du bare lar administratorer (eller ansatte og lærere) opprette delte disker, og at du administrerer tilgangen til delte disker nøye.

Vurder å begrense tilgang til katalogen og deling av kontakter der det er mulig, enten ved å slå av kontaktdeling for enkelte eller alle brukere, eller ved å opprette egendefinerte kataloger for å begrense hvilke brukere som er synlige for hvem.

Konfigurer regler for forebygging av datatap (FDT) i Disk og Gmail for å oppdage og blokkere sensitiv informasjon. Det finnes forhåndsdefinerte regler som kan brukes til å beskytte vanlige typer sensitiv informasjon (som bank- eller kredittkortnumre). Du kan også opprette egendefinerte regler basert på nøkkelord, ordlister og regulære uttrykk.

Administrer Gmail-innstillinger

Gmail er en av kjernetjenestene i Google Workspace for Education, og den har mange administratorinnstillinger for å beskytte institusjonen og brukerne der.

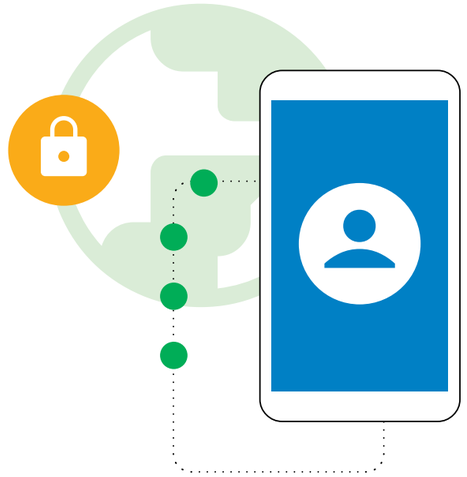
Forhindre søppelpost, forfalskning og nettfisking med Gmail-autentisering. Tilpass innstillingene for søppelpostfilteret – du kan blant annet gjøre autentisering av avsender obligatorisk for alle godkjente avsendere og slå av omgåelse av søppelpostfilteret for interne avsendere.

Slå av POP/IMAP-tilgang om mulig, og slå på utvidet skanning av meldinger før levering og avansert beskyttelse mot nettfisking og skadelig programvare. Hvis du tillater eksterne e-poster for noen av eller alle brukerne, kan du slå på advarsler om eksterne mottakere.

Google Workspace for Education Standard- og Plus-kunder kan også bidra til å beskytte mot skadelig programvare og løsepengevirus ved å konfigurere regler for oppdaging av skadelige vedlegg ved hjelp av sikkerhetssandkassen.

Apper fra tredjeparter

Bruk innebygde arbeidsflyter for godkjenning til å godkjenne apper fra tredjeparter som får tilgang til kontodata via API-er. Dette bidrar til å forhindre at uautoriserte data deles med apper fra tredjeparter som ikke er godkjente for skolebruk.



Rapporter og overvåkning

Som administrator kan du se rapporter og logghendelser i Google Administrasjonskonsoll for å gå gjennom aktivitet i organisasjonen, for eksempel mulige sikkerhetsrisikoer, hvem som logger på og når, og hvordan brukere oppretter og deler innhold. Du kan se data på domenenivå og granulære detaljer på brukernivå i diagrammer og tabeller. Se rapporter og revisjonslogger (inkludert varselsenteret) for å identifisere sikkerhetsrisikoer, analysere bruken av tjenestene, diagnostisere konfigureringsproblemer og mye mer.

Google Workspace for Education Standard og Plus-administratorer kan bruke sikkerhetsoversikten til å få et overblikk over ulike sikkerhetsrapporter, identifisere trender og sammenligne gjeldende og historiske data. Dette kan være fildeling i Disk, aktiviteter knyttet til nettsøppel, nettfisking og skadelig programvare i Gmail, mistenkelige påloggінger på brukerkontoer og mistenkelige enhetsaktiviteter. De fleste bruks-, aktivitets- og revisjonslogger – inkludert administrator-, Disk Meet- og Chat-logghendelser – er tilgjengelige i seks måneder.

Bruk sikkerhetssenteret

Google Workspace for Education Plus- og Standard-administratorer kan bruke sikkerhetssenteret, med avansert sikkerhetsinformasjon og -statistikk, som gir ekstra innsyn i og kontroll over sikkerhetsproblemer som berører domenet ditt.

I sikkerhetssenteret finner du verktøyet for sikkerhetsundersøkelser, som kan hjelpe administratorer med å identifisere, kategorisere og håndtere sikkerhets- og personvernproblemer, for eksempel nettfiskingsangrep, upassende fildeling, mistenkelig bruker- og enhetsaktivitet og mye mer..

Google Workspace er verdens sikreste skybaserte kommunikasjons- og samarbeidspakke.

0

aktivt utnyttede sårbarheter i programvare i Workspace siden november 2021*

50%

potensiell innsparing på forsikringspremie for nettsikkerhet ved bruk av Workspace

Halvparten

Halvparten så mange sikkerhetshendelser for organisasjoner som bruker Workspace, sammenlignet med Microsoft 365

Godt under halvparten

Godt under halvparten så mange sikkerhetshendelser for organisasjoner som bruker Workspace, sammenlignet med Microsoft Exchange

* Ifølge CISA er dette betydelig mindre enn andre produktivitetsleverandører i dette markedssegmentet.

Google Chromebook for utdanning

Chromebook er svært sikre, skalerbare og brukervennlige datamaskiner for elever og lærere, takket være de innebygde sikkerhetsfunksjonene som fungerer fra første gang du slår dem på. Det har aldri vært rapportert noe angrep med løsepengevirus på ChromeOS-enheter i bedrifter, på skoler eller hos enkeltpersoner. Chromebook beskytter skoler mot stadig nye trusler med oppdaterte funksjoner, og oppdateringene skjer automatisk i bakgrunnen, slik at brukerne kan fortsette å jobbe innen noen sekunder.

Automatiske OS- og appoppdateringer med innebygd beskyttelse mot skadelig programvare

Angripere prøver hele tiden å utnytte feil og smutthull i operativsystemer, nettlesere og populære apper for å installere skadelig programvare og stjele brukerdata. Chromebook er bygget med integrert sikkerhet fra grunnen av og holder OS og apper oppdatert for å beskytte deg og brukerne dine. Og skybaserte apper trenger aldri programvareoppdateringer på samme måte som lokale apper. Den Google-utviklede sikkerhetsbrikken i Chromebook bidrar til å holde dem trygge, beskytte brukerens identitet og sikre systemets integritet.

Chromebook-enhetene i enhetsflåten din kjører automatisk de nyeste oppdateringene av beskyttelsen mot skadelig programvare. Elever og lærere beskyttes mot dataangrep gjennom innebygde sikkerhetsfunksjoner som datakryptering, bekreftet oppstart, sandkasser og automatiske oppdateringer.

Sikre brukerdata

Når du logger på en Chromebook med Google-kontoen din, lagres alle dataene dine i krypterte filer, slik at ingen andre på enheten kan se dataene dine eller logge på apper med kontoen din. Derfor er det veldig enkelt og sikkert for elevene å dele enheter i klasserommet, og skolen kan redusere de totale datakostnadene. Chrome Education-oppgraderingen, som er en lisens for enhetsadministrering, har mer avanserte sikkerhetsfunksjoner med ekstra innsyn.

Sikkerhetsregler for eksterne brukeradministrerte enheter

Skoleadministratorer kan konfigurere ChromeOS-regler og installere/oppdatere apper eksternt ved hjelp av Google Administrasjonskonsoll. Én IT-administrator kan bare klikke på en knapp for å oppdatere reglene for og konfigureringen av flere hundre tusen Chromebook-enheter på et øyeblikk.

Dette sikrer at

- Elevene bare får tilgang til innhold og apper som er godkjent av skolen
- Alle apper og utvidelser oppdateres med de nyeste sikkerhetsfeilrettingene
- Brukere ikke kan kopiere, overføre eller dele skoledata utenfor enheten
- Avgjørelser tas basert på data, med tilpassede sikkerhetsanbefalinger fra Google for håndtering av sikkerhetstrusler
- Håndtering av retningslinjer for sikkerhet og administrering av identiteter og tilgang for alle brukere skjer sentralt i administrasjonskonsollen.

Noen regler administratorer bør vurdere å konfigurere:

Enhetsregler

- **Gjestemodus**
  Vi anbefaler at du slår av Gjestemodus på enhetene, slik at elever og lærere må logge på med sin egen påloggingsinformasjon i stedet for å bruke enheten anonymt.
- **Påloggingsbegrensninger**
  Det kan hende du ikke vil at elever og lærere skal kunne logge på skolens Chromebook-enheter med personlige Gmail-kontoer. Bruk påloggingsbegrensninger som gjør at kun kontoer i Workspace-domenet ditt kan logge på enheter som bare brukes av elever.
- **Bruker- og enhetsrapportering**
  Administratorer bør vurdere å slå på bruker- og enhetsrapportering, slik at de kan innhente statistikk om hvor ofte Chromebook-enhetene brukes, hvem som bruker dem, og hvilken stand maskinvaren er i.
- **Tvungen ny registrering**
  Det er avgjørende at Chromebook-enheter som tilhører skolen, forblir på skolen, med mindre de blir deprovisjonert av en administrator. Administratorer bør vurdere å slå på tvungen ny registrering av Chromebook-enheter, slik at enhetene alltid blir registrert på nytt hvis de skulle bli utvisket eller forsøkt stjålet.

Brukerregler

- **Inkognitomodus**
  Elevene må få hjelp med å lykkes når de bruker skolens Chromebook-enheter. Dette inkluderer å begrense dem til bruk av den autentiserte nettleseren, slik at nettinnholdsfiltre kan holde dem unna upassende nettsteder. Administratorer bør slå av inkognitomodus, slik at elevene ikke kan omgå nettfiltre.
- **Proxy-modus**
  Noen skoler bruker proxy-tjenere til nettfiltrering, og det er viktig at du slår av brukernes mulighet til å endre proxy-innstillingene selv.
- **Multipålogging**
  Hvis brukerne har lov til å logge på en sekundærkonto mens de bruker skolens Chromebook-enheter og Workspace-kontoer, kan det gjøre det lett for en bruker å trekke ut sensitive elev- eller skoledata til den sekundære kontoen. Administratorer bør vurdere å slå av multipålogging.
- **Nettleserlogg**
  Det kan være lurt å slå av elevenes mulighet til å tømme nettleserloggen. Hvis en nettsikkerhetshendelse skulle oppstå, kan disse nettleserloggene være nyttige i en eventuell etterforskning.

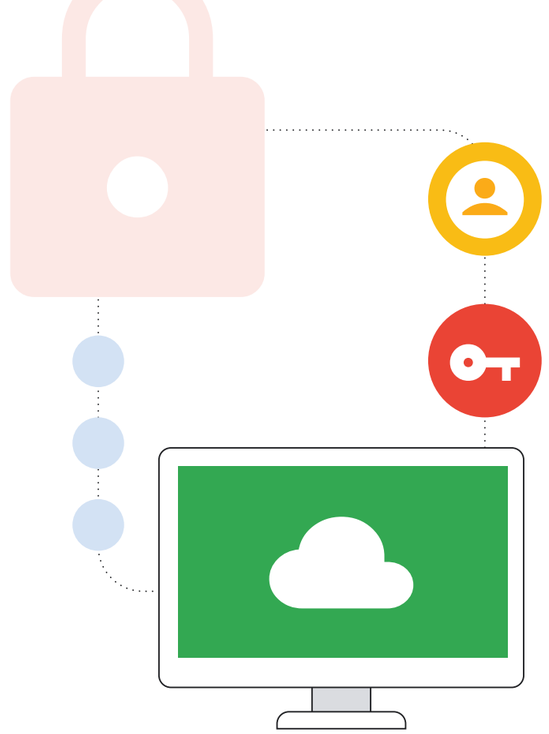
Denne listen er et godt utgangspunkt for å sikre nettverkene mot de vanligste feiltrinnene som fører til alvorlige sikkerhetshendelser. Du finner andre anbefalte sikkerhetsregler i sjekklisten for sikkerhet.

Administrering av endepunkter for sikker bruk – når og hvor som helst

Med systemet for ekstern administrering av regler for ChromeOS kan skolens administratorer bruke sikkerhetsinnstillinger og kjøre sikkerhetsverktøy, for eksempel systemer for innholdsfiltrering, på enheten i stedet for på skolens nettverkstjenere. Dette sikrer at elevene får de samme sikkerhetsfordelene på skolens Chromebook-enheter hjemme som de får på skolen. Dette blir stadig viktigere etter hvert som skoler går over til digitale skolebøker og nettbaserte læringsverktøy, slik at elevene må ta med seg datamaskiner hjem for å gjøre lekser.

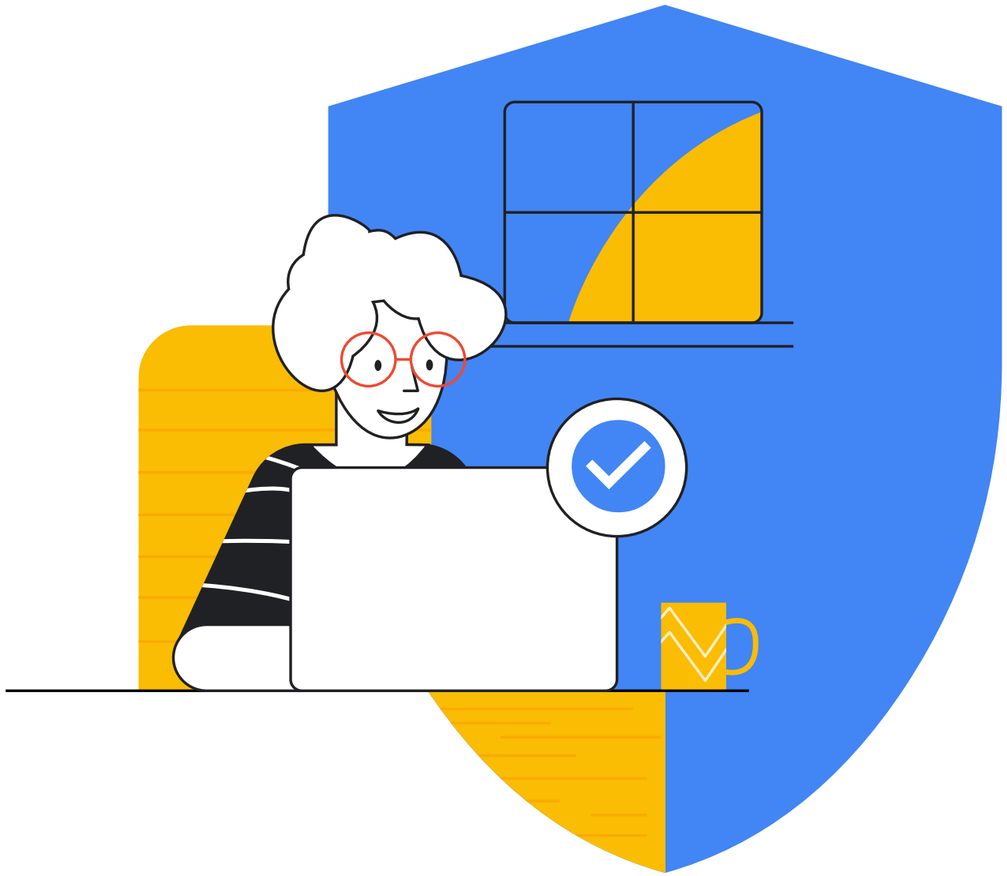
Konklusjon

Utfordringene med å sikre grunnskoler og videregående skoler mot sikkerhetshendelser er kompliserte, men det er vel verdt å investere i å beskytte deg selv, elever, lærere, ansatte og hele økosystemet på nettet. Punktene som dekkes i dette dokumentet er et godt utgangspunkt, men hver skole må tilpasse anbefalingene etter sine unike behov og fortsette å følge med på ny teknologi og et trussellandskap i stadig utvikling. Denne ressursen gir et godt grunnlag for et sikkerhetsprogram for skoler, med ressurser for veien videre og implementerbare gjøremål. I tillegg har Google et bredt utvalg av ressurser, opplæring og dyktige nettsikkerhetseksperter som kan hjelpe skoler og organisasjoner med å følge denne håndboken og med ny teknologi, inkludert AI. Googles produkter er skreddersydd for utdanning og tilbyr ferdigløsninger for mange av de fallgruvene innen nettsikkerhet som dette dokumentet omhandler.
Vi samarbeider gjerne med deg under planleggingen og implementeringen av sikkerhetsprogrammene dine.



Ressursliste

- [1]Google. «Tips to Stay Safe & Secure Online.» Google Sikkerhetssenter, https://safety.google/security/security-tips/. Åpnet 6. oktober 2022.
- [2]NIST. «Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.» NIST Technical Series Publications, 16. april 2018, https://doi.org/10.6028/NIST.CSWP.04162018. Åpnet 6. oktober 2022.
- [3]Microsoft. «Microsoft AccountGuard Program.» Microsoft AccountGuard Program, https://www.microsoftaccountguard.com/en-us/. Åpnet 6. oktober 2022.
- [4]Google. «Avansert beskyttelse-programmet.» Google Avansert beskyttelse-programmet, https://landing.google.com/advancedprotection. Åpnet 6. oktober 2022.
- [5]Google. «Google Sikkerhetssenter.» Google Sikkerhetssenter – hold deg tryggere på nettet, https://safety.google. Åpnet 6. oktober 2022.
- [6]Meta. «Basics: Help Secure Your Account.» Help Secure Your Account, https://www.facebook.com/gpa/resources/basics/security. Åpnet 6. oktober 2022.
- [7]Meta. «Facebook Protect.» Facebook, https://www.facebook.com/gpa/facebook-protect. Åpnet 6. oktober 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. Åpnet 6. oktober 2022.
- Passnøkler: https://developers.google.com/identity/passkeys
- CISAs «Protecting Our Future Cybersecurity K-12»-rapport https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAO-rapport https://www.gao.gov/products/gao-20-644
- Hvis du vil ha mer informasjon om hvordan Google for Education kan hjelpe deg med å beskytte institusjonen din, kan du gå til personvern- og sikkerhetssenteret for Google for Education.
- Nettfiskingsrapport fra Zcaler



Google for Education

Safer with Google