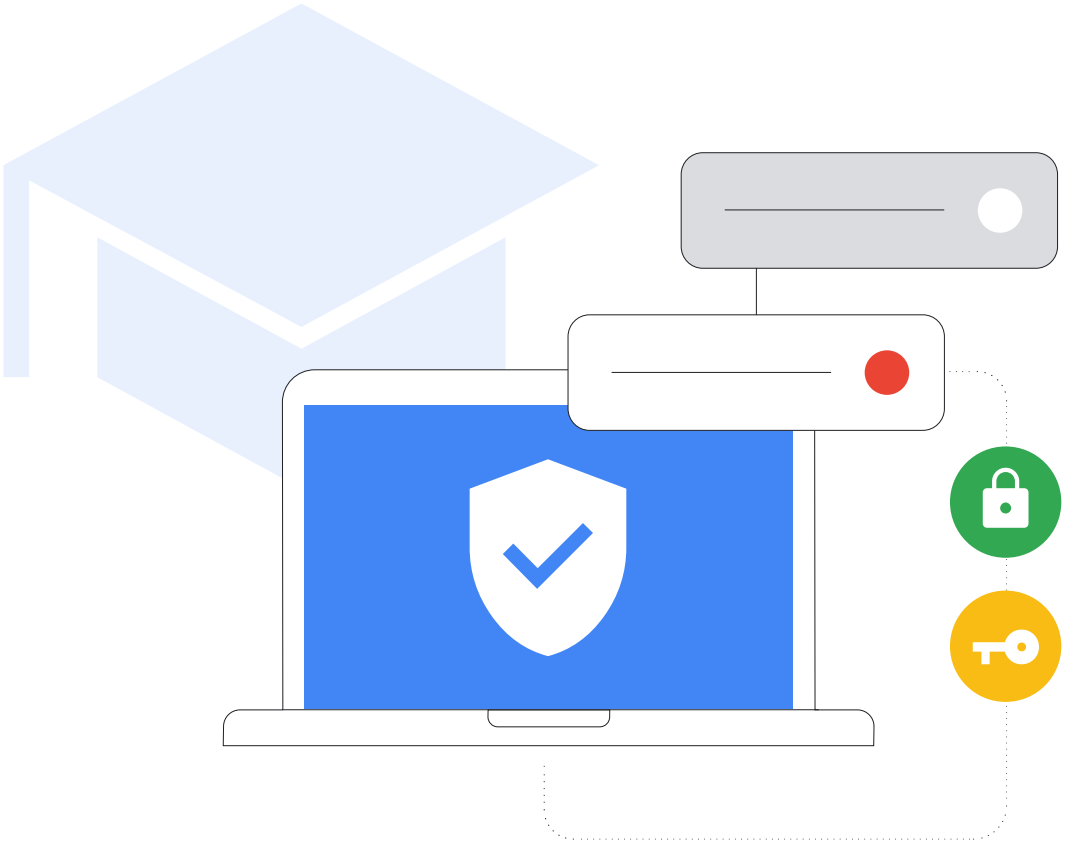
Google for Education

K-12 Guidebok för cybersäkerhet

Uppdaterad i augusti 2023



Safer with Google

Detaljerad översikt

Som CISA:s rapport *Protecting Our Future*[1] betonar är det viktigt för grund- och gymnasieskolan att satsa på cybersäkerhet för att skydda elever, deras familjer, lärare, personal och communityer. I det här dokumentet finns riktlinjer och rekommenderade metoder för hur skolans IT-administratörer ska ställa in och konfigurera maskinvara och program på grund- och gymnasieskolor för att stärka cybersäkerheten. Det innefattar både allmänna rekommenderade metoder och specifik vägledning för Googles produkter och tjänster. Googles målsättning är att ordna informationen som finns i världen och göra den tillgänglig och användbar överallt. Det är en av drivkrafterna bakom vårt arbete i Google for Education-teamet – vi tar fram verktyg för undervisning och lärande. Vi ska gå igenom lärdomar från det arbetet i den här guiden.

Vi tillhandahåller rekommenderade säkerhetsmetoder efter ämne som ger djupgående information om konfigurerings-, inställnings- och riskhanteringsstrategier. Dessutom går vi igenom Googles inställning till cybersäkerhet för våra tjänster, i synnerhet våra utbildningsverktyg. Vi anser att våra produkter erbjuder ett enastående inbyggt skydd mot vanliga attacker. I den detaljerade vägledningen i det här dokumentet specificerar vi däremot inte några produkter och tjänster.

Risken

Skolor är vanliga mål för cyberattacker. Skadliga aktörer försöker utnyttja de datarika miljöerna på skolorna för egen vinning. 46 % av alla skolor som ännu inte har utsatts anser att det bara är en tidsfråga eftersom utpressningsvirusen blir allt smartare och svårare att stoppa. Och 42 % av skolorna anser att utpressningsvirusen är så vanliga att en attack är oundviklig. När skolvärlden snabbt tvingades övergå till distansundervisning 2020 skapades luckor i cybersäkerheten som gjorde att skolorna blev sårbara för attacker.

Försvaret

Attackerna kan mildras. Trots att det inte finns någon teknik som eliminerar risken helt kan utbildningssektorn samarbeta med leverantörer inom utbildningsteknik och tillämpa rekommenderade metoder som skapar en säker och heltäckande inställning för att minska risken avsevärt. Med rätt försiktighetsåtgärder och policyer för att skydda användare och enheter samt säkerställa dataintegritet, kan utbildningsinstitutioner bli bättre på att hantera riskerna och mildra attacker.

Viktiga rekommendationer:

- **ANVÄND SÄKER AUTENTISERING** för att hålla känsliga uppgifter säkra, skydda e-postmeddelanden, filer och annat innehåll och förhindra att obehöriga användare får åtkomst till utbildningssystem. Tillämpa rekommenderade metoder för användarautentisering, till exempel starka lösenord och tvåstegsverifiering (2SV), nycklar och lösenordshanterare i den mån det går, särskilt för IT-administratörer och personal som jobbar med känsliga uppgifter.
- **TILLÄMPA LÄMPLIGA SÄKERHETSINSTÄLLNINGAR** för att hålla användarna, datan och miljön säker. Googles produkter är säkra som standard, men det är viktigt att administratörer använder och konfigurerar nätverk och system för att se till att de är skyddade. Skydda skolorna genom att tillämpa principer för nolltillit och minsta behörighet. Användarna ska endast ha åtkomst till de program, data, appar och system de behöver för att göra ett effektivt jobb.
- **UPPDATERA OCH UPPGRADERA DINA SYSTEM** för att säkerställa att användarna är skyddade mot de senaste hoten. Använd moderna operativsystem (OS) och webbläsare för att säkerställa att användarna kör de senaste programversionerna på alla enheter (eller godkända stabila versioner) och att de uppdateras automatiskt. Du kan öka skyddet genom att uppgradera till en säkrare lösning, till exempel Chromebook. Inga utpressningsvirus har någonsin identifierats på ChromeOS-enheter.
- **AKTIVERA VARNINGS- OCH ÖVERVAKNINGSSYSTEM I REALTID** för att höja säkerhetsnivån och mildra potentiella problem snabbt. Du kan använda de här inbyggda funktionerna i ditt primära samarbets- och kommunikationsprogram, till exempel Google Workspace for Education, eller implementera separata lösningar för säkerhetsloggning och övervakning. Säkerställ omfattande spårning av aktiviteter för skolans nätverk, enheter, appar, användare och data. Övervaka kontoinloggningar, fildelning, e-postvolym (särskilt försök till nätfiske och skadlig programvara), enhetsaktivitet och konfigurationsändringar. Håll varnings- och övervakningslösningen uppdaterad så du får varningar om hot, viktiga händelser och systemändringar.
- **UTBILDA LÄRARE, PERSONAL OCH ELEVER** i hur de ska använda enheter och program på ett säkert sätt, känna igen och rapportera potentiella hot och dela data på rätt sätt för att skydda sig mot några av de vanligaste attackerna. Skolor och skolområden kan skapa varumärkt utbildningsmaterial med tillgängliga material som leder till en gedigen verktygslåda för skolor.

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

Specifika rekommendationer för användare av Googles produkter:

Googles produkter som Google Workspace for Education och Chromebooks kan förbättra skolans cybersäkerhet och göra alla rekommendationerna enkla att implementera. Tillsammans tillhandahåller de en heltäckande lösning som hjälper till att skydda användarnas integritet och ger förstklassig säkerhet för din skola.

De här strategierna tillsammans med ytterligare riktlinjer i följande artikel utgör en bra grund för säkerhet inom grund- och gymnasieskolan.

Googles inställning till utbildning

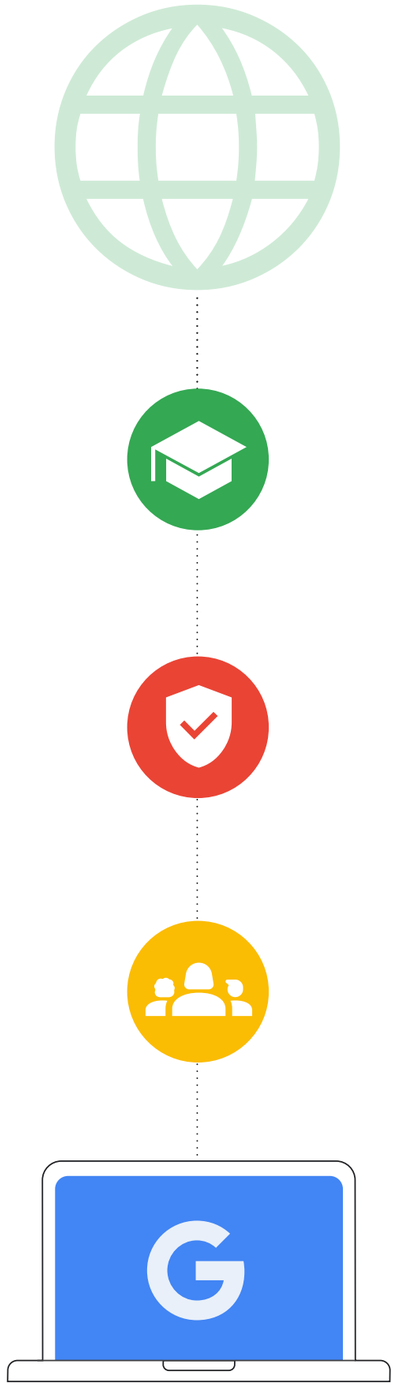
Googles målsättning är att ordna informationen i världen och göra den tillgänglig och användbar överallt, inte minst inom utbildningssektorn. Vi i Google for Education-teamet gör det genom att ta fram verktyg som Chromebooks och Google Classroom som gör det enkelt och tryggt för elever och lärare att skapa, dela och organisera eget innehåll och få åtkomst till och använda utbildningsresurser och onlineverktyg.

Skolor förtjänar teknik som är säker och privat som standard, som säkerställer att du har kontrollen med innehåll och information som är tillförlitlig. Med produkter som Chromebooks och Google Workspace for Education får skolorna ledande säkerhet som iakttar de högsta globala utbildningsstandarderna. IT-administratörer får full synlighet och enkel kontroll av deras data- och säkerhetspolicyer och eleverna kan ägna sig helt åt lärande i en tryggare digital miljö med åldersbaserat innehåll som mildrar spam och cyberhot.

Vi har prioriterat inbyggda säkerhetsfunktioner och inställningar, de högsta nivåerna av integritetsstandarder och alternativ för mer proaktiva säkerhetsverktyg för att säkerställa tryggt lärande för alla. ChromeOS-enheter mildrar hot mot skolor. Det är det bästa försvaret mot utpressningsvirus som är det främsta hotet mot skolorna, eftersom Chromebooks aldrig har drabbats av ett framgångsrikt utpressningsvirus mot Chromebooks.

Samtidigt är Google Workspace for Education en av världens populäraste och säkraste molnbaserade kommunikations- och samarbetssviter. I det sista avsnittet nedan kan du läsa mer om hur de upprätthåller cybersäkerheten sett till rekommendationerna.

Den här artikeln är uppdelad i två avsnitt: det första avsnittet är praktiska och allmänna säkerhetsriktlinjer för grund- och gymnasieskolor oavsett produkter. Det andra avsnittet handlar om specifika konfigurationer med Google for Education-produkter som Google Workspace for Education och Chromebooks. I båda avsnitten finns uppgifter som håller dig och eleverna trygga online.



Inledning

Både enheter och nätverk på grund- och gymnasieskolor löper hög risk att drabbas av cyberattacker. Det är av högsta vikt att grund- och gymnasieskolor tillämpar bästa möjliga säkerhet för att skydda eleverna och förhindra att data, tjänster, resurser, tid och pengar försvinner, vilket kan ske till följd av sådana attacker. (Källa)

Den här guiden är ett verktyg för att betona rekommenderade metoder kring cybersäkerhet för skolans administratörer och system för att hålla miljöerna trygga. Genom att införliva metoderna kan grund- och gymnasieskolor mildra eller förhindra allvarliga och kostsamma cyberattacker mot utbildningssystem och skydda elever, familjer, lärare och personal.

Cyberattacker mot skolor ökar i både frekvens och allvarlighetsgrad. Enligt K-12 Cybersecurity Resource Center inträffade över 1 300 offentligt redovisade cyberincidenter i USA bland utbildningsorganisationer i alla 50 delstater mellan 2016 och 2021. Dagens utbildningsledare måste skydda elevernas, lärarnas och personalens data och personuppgifter samt institutionens system och information. Det är en omfattande uppgift, i synnerhet eftersom utbildningssektorn traditionellt sett har haft det svårt att hålla jämna steg inom cybersäkerhet jämfört med andra sektorer.

Framgångsrika cyberattacker, till exempel utpressningsvirus, nätfiske, skadliga program och annat kan leda till storskaliga dataintrång av uppgifter som kan kopplas till en specifik person (PII), kostsamma utbetalningar (den genomsnittliga utbetalningen av lösensumma har ökat med 500 % till 812 260 USD sedan 2020) och orsakar långa avbrott för undervisning och andra skolaktiviteter. En lyckad attack med utpressningsvirus stängde ner ett helt skolsystem. Det påverkade hela samhället eftersom det tog flera dagar innan eleverna kunde återvända till skolan. Med begränsade resurser och finansiering är grund- och gymnasieskolor ett primärt mål om inga satsningar görs på ökad cybersäkerhet.

Kommunikation, samarbete och partnerskap leder till den bästa cybersäkerheten. I det här dokumentet har vi samlat Googles säkerhetstips, ramen för cybersäkerhet från National Institute for Standards and Technology (NIST) och 2023 års verktyg och rekommendationer för grund- och gymnasieskolan från den amerikanska myndigheten CISA, vilka är vedertagna källor för cybersäkerhetsrutiner. Det här dokumentet tar upp vanliga steg som IT-administratörer bör genomföra eller överväga, några av Googles egna rekommenderade metoder och vägledning för våra produkter och hänvisar till säkerhetstips och tjänster som erbjuds av andra företag. Administratörer bör granska all säkerhetsvägledning av relevanta företag och implementera deras senaste vägledning eftersom det ansvariga företaget bäst kan beskriva sina egna produkter och eventuella förändringar som kan ha skett.

Innan du vidtar åtgärder grundade i rekommendationerna nedan ska du även fundera kring detta:

Tänk på följande

1. **Skydda elevgruppen.**

   Skolorna är olika och vissa grupper kan kräva ytterligare steg för att skydda säkerheten och integriteten. Många utbildningstekniska verktyg har åtkomstfunktioner för olika åldrar, till exempel att det går att begränsa olämpligt innehåll eller se till att plats- och kontaktuppgifter är privata.

2. **Vilka datatyper du lagrar.**

   Lagrar du känsliga uppgifter kanske du vill kryptera datan eller lagra den på en annan plats.

3. **Vilka typer av enheter du använder och implementeringsmodell.**

   Enheter och deras appar bör få automatiska uppdateringar för att maximera säkerheten, kryptera data och isolera konton för att säkerställa att användarna bara har åtkomst till sin egen information.

4. **Policyerna för skolan, skolområdet eller regionen.**

   Skolan kan ha specifika policyer för teknikanvändning. Du behöver kontrollera att alla säkerheter konfigureras i enlighet med policyerna.

Varje dag blockeras
100 miljoner
nätfiskeförsök i Gmail.

Varje vecka upptäcks
300,000
osäkra webbplatser av Google.

Varje dag får
74 miljoner
användare hjälp av Googles Lösenordshantering.

Varje år stärker
700 miljoner
personer säkerheten med hjälp av Säkerhetskontroll.

Allmän säkerhetsvägledning

Använda säker autentisering

Säker autentisering måste vara högsta prioritet för skolor och andra institutioner. Under det fjärde kvartalet 2022 stod svaga konton eller konton utan användaruppgifter för 48 % av alla angreppsfaktorer vid intrång. Genom att implementera viktiga rekommendationer kan man verifiera att användarna är de som de utger sig för att vara och begränsa åtkomsten till information som är lämplig för varje användares roll.

IT-administratörer bör tillämpa användningen av tvåstegsverifiering (2SV) (även känt som tvåfaktorsautentisering (2FA) och övergå till lösenordsfri autentisering (nycklar) i den mån det går, i synnerhet när någon får fjärråtkomst till skolans system. 2SV skapar ett extraskikt av säkerhet för dina onlinekonton, vilket gör det mycket svårare för angriparna att få åtkomst.

Det finns många olika typer av enheter och implementeringsmodeller som används av skolor i dag och det finns varierande teknisk kompetens i grund- och gymnasieskolemiljön. Konto- och enhetssäkerhet varierar i de olika användarrollerna och typerna med fastställda rekommenderade metoder: IT-administratörer, lärare och personal, äldre elever som använder tilldelade enheter och yngre elever som använder delade enheter. Vi diskuterar specifika rekommendationer för varje grupp nedan.

Det finns flera olika typer av autentiseringsmetoder som är rekommenderade metoder i de flesta miljöerna:

- **Starka lösenord**
  Uppmana användarna att skapa ett eget lösenord vid första inloggning och kräv tekniskt att lösenordet ska ha en viss längd och komplexitet. Längre lösenfraser skapar ett extra lager av säkerhet på grund av längd och användning av komplexa tecken. Användarna ska inte behöva byta lösenord regelbundet eftersom det uppmuntrar dem att använda enklare lösenord eller göra oväsentliga ändringar (som att uppdatera ett tecken).
- **Tvåstegsverifiering (2SV)**
  2SV skyddar konton med ett andra steg, ofta något användarna har med sig, till exempel en säkerhetsnyckel eller app på en mobil som skapar en kod för engångsverifiering. Trots att alla slags tvåstegsverifieringar skapar kontosäkerhet ska administratörer undvika att använda verifieringskoder som skickas per sms eller samtal som kan vara sårbara för attacker baserade på telefonnummer.
- **Lösenordsfri autentisering**
  Nycklar är ett säkrare och enklare alternativ till lösenord. Användarna kan logga in på appar och webbplatser med pinkod, mönster, biometrisk sensor (till exempel fingeravtryck eller ansiktsigenkänning) eller säkerhetsnyckel, vilket gör att de slipper komma ihåg och hantera lösenord. Dessa kanske inte är lämpliga i alla sammanhang inom utbildning, men de ersätter i allt större utsträckning traditionella former av autentisering och skapar tryggare och snabbare inloggningar. Nycklar skyddar användare från nätfiskeattacker eftersom de endast fungerar på registrerade webbplatser och appar.
- **Enkel inloggning (SS)**
  Med SSO kan användarna få åtkomst till flera appar och webbplatser med en enda uppsättning användaruppgifter. När användarna bara behöver komma ihåg en uppsättning användaruppgifter är sannolikheten mindre att de skriver upp dem. När skolorna inte behöver hantera flera uppsättningar användaruppgifter kan de dessutom spara pengar på kostnader för IT-support och kundtjänst. Google Workspace for Education har inbyggt stöd för SSO, så användare kan logga in på appar från tredje part med sina användaruppgifter i Google-kontot eller använda en annan leverantörs användaruppgifter för att logga in på sina Google-konton.
- **Lösenordshantering**
  Med lösenordshantering kan användarna skapa starka, unika lösenord för konton och tjänster som de använder under skol- och arbetsdagar (när man inte använder SSO). Lösenordshantering hjälper inte till att logga in på en enhets operativsystem menkan hantera lösenord när användaren har loggat in. Google-användare kan använda Google Lösenordshantering i Chrome på valfri plattform, ChromeOS och Android.

De unika behoven hos olika grupper gynnas av specialiserade delar eller kombinationer av autentiseringsinställningarna efter deras roll inom en utbildningsinstitution, de typer av system och data de har åtkomst till och deras ålder.

Skolans administratörer

Administratörerna styr systemen och mycket av datan för grund- och gymnasieskolorna. Skyddet av deras konton är viktigt för säkerheten i hela systemet: från infrastruktur till kontouppgifter och enheter som administreras av institutionen. Därför ska de tillämpa det starkaste inom autentisering, till exempel starka lösenord, en pålitlig lösenordshantering och 2SV. Var och en av dessa ger ett skyddslager och tillsammans tillhandahåller de den starkaste säkerheten för administratörskontot och företagstjänsterna.

- Administratörerna bör använda en fysisk säkerhetsnyckel eller en kryptografiskt säker 2SV-metod som kräver en tillförlitlig enhet och promptar. Detta kan inkludera en tjänst som Google Authenticator eller annan app som skapar engångsverifieringskoder. Chromebooks släppta efter 2019 med en TPM-krets har en av/på-knapp som kan användas för tvåfaktorautentisering.
- Administratörerna bör använda tillförlitlig lösenordshantering med stöd för 2SV för att lagra sina lösenord för olika tjänster.

Lärare och personal som använder tilldelade enheter

Precis som administratörer har lärare och personal åtkomst till känsliga uppgifter, men de styr inte den digitala infrastrukturen och har mer varierande teknisk kompetens.

- Lärare och personal med Chromebooks bör ges alternativet att logga in med biometrisk verifiering där det är juridiskt tillåtet, till exempel med fingeravtryck.
- Administratörer bör tillämpa 2SV och övergå till lösenordsfri autentisering i den mån det går och när personal får fjärråtkomst till utbildningsinstitutionens system.

Äldre elever som använder tilldelade enheter (vanligen årskurs 4 och uppåt)

Äldre elever har bättre koll på hur de ska skydda sig själva och brukar kunna använda autentisering med högre skydd, vilket lämpar sig för den typen av tjänster som de troligen använder. De ska bara ha åtkomst till sitt eget konto och den information som har delats med dem.

- Elever med Chromebooks bör ges alternativet att skapa en enhetsspecifik pinkod för att logga in på den enheten. Biometriska alternativ kanske inte är lämpliga eller genomförbara i många skolmiljöer.
- Alla elever ska få stöd att skapa ett unikt lösenord som inte innehåller personliga uppgifter (till exempel namn, klass eller födelsedag). Eleverna bör få lära sig hur användningen av lösenfraser skapar komplexitet samtidigt som lösenordet blir lätt att komma ihåg.

Unga elever som använder delade enheter (vanligen förskoleklasser)

De yngsta eleverna lär sig fortfarande hur de ska använda sig av utbildningsteknik och gynnas av enkel autentisering som lämpar sig för begränsade tjänster och data.

- Skolor som använder lösenord från tredje part, som QR-koder eller bildinloggning för sina yngsta elever och personer som inte kan logga in med lösenord, bör iaktta försiktighet med säkerheten eftersom metoderna inte är lika säkra. Administratörerna bör modifiera en elevs lösenord och uppdatera koden om en kod har kommit bort eller andra har sett den.
- Skolorna bör utbilda både eleverna och föräldrarna om vikten av att hålla lösenord hemliga och att lagra alternativa användaruppgifter som QR-koder säkert.
- För tilldelade enheter som surfplattor kan en enhetsspecifik pinkod användas som alternativ säker autentiseringsmetod.

Tilldela lämpliga säkerhetsinställningar

Skolenheter och nätverk är mål med hög synlighet och högt värde för angripare i hela världen, så det är viktigt att tillämpa bästa möjliga säkerhet för att förhindra att tjänster, resurser, tid och pengar går förlorade. Systemadministratörer bör implementera effektiva och lämpliga säkerhetsfunktioner som finns tillgängliga i de produkter som skolorna använder, men även se till att systemet förblir enkelt att använda för lärare, personal och elever. Viktiga säkerhets- och integritetsinställningar bör konfigureras så individuella användare inte kan inaktivera eller modifiera dem och andra inställningar bör ha skyddsstandarder som har konfigurerats av administratörer. Det är viktigt att tillämpa bästa möjliga säkerhet för att förhindra att tjänster, resurser, tid och pengar går förlorade. Använder du Chromebooks kan du se våra förslag för hur du konfigurerar enhetspolicyer i det sista avsnittet.

Slutligen kan du bygga in uppgiftsminimering för individers personuppgifter. Det gör du genom att begränsa syftena, insamlingssätten, användningen och yppandet till vad som är rimligen nödvändigt och proportionerligt för att kunna tillhandahålla tjänsten eller vad som i övrigt är konsekvent med relationens kontext.

Appar och uppdateringar

Begränsa och minimera de appar dina användare kan installera. Varje app som installeras på en enhet är en potentiell attack-bärare. Använd appar från tillförlitliga källor i största möjliga mån. Du kan rekommendera att användarna kontrollerar verifieringsmärket i Google Play Butik för att säkerställa att användarna laddar ned de officiella apparna som har genomgått säkerhetsgranskning. Eventuella OS- eller maskinvarumodifieringar (jailbreaking eller rooting) introducerar betydande säkerhetsbrister och ska undvikas.

Åtkomst och synlighet

Administratörer bör säkerställa att användarna endast har åtkomst till data, program, tjänster och system som de behöver för att göra sina jobb och lära sig effektivt. På så sätt kan man begränsa oavsiktlig åtkomst och hålla koll på vem som har åtkomst till vilka resurser. Uppmärksamma känsliga uppgifter, till exempel PII och system (som HR, lönetjänster, betygsättning, säkerhet och konfiguration) genom att granska vilka användare som får åtkomst till uppgifterna och under vilka omständigheter genom att begränsa åtkomst till skolägda enheter och säkerställa att endast specifika användare i personalen har åtkomst.

Granska datadelningspolicyerna i samarbetsverktyg för att förebygga olämplig eller onödig och obehörig åtkomst. Begränsa eller blockera delning utanför miljön (i synnerhet för elever) och aktivera policyer som övervakar delning av känsligt innehåll.

Enhetsförlust eller stöld

Att tappa bort en enhet behöver inte betyda att du förlorar data. Administratörerna bör standardisera en plan för att säkerställa åtkomst till information och dokument vid enhetsförlust eller stöld, till exempel upprätthålla dokument i en molnmiljö. Ladda ned och skriv ut reservkoder för dina 2SV-processer för att förhindra avbrott i kontoåtkomsten.

När en enhet rapporteras försvunnen eller stulen ska du säkerställa att enheten har fjärrlås och att kopplade konton blir låsta eller flaggade så de inte används för att få obehörig åtkomst. Chromebooks kan fjärrensas om de försvinner och Google Workspace for Education-konton kan övervakas för misstänkt aktivitet eller stängas av (låsas) vid behov.

Avancerat skydd för högriskanvändare

För användare med hög synlighet och känsliga uppgifter (till exempel Google Workspace for Education-administratörer) tillhandahåller Google programmet Avancerat skydd (APP). APP ger användarna ytterligare skydd mot riktade attacker, till exempel nätfiskeförsök, skadliga nedladdningar och lösenordsbrott. APP är särskilt framtaget för att förhindra riktade onlineattacker mot Google-konton och använder automatiskt stark autentisering, säkerhetsnycklar och begränsar extern åtkomst till data. Andra onlinekontoleverantörer tillhandahåller starka kontoskydd för högriskanvändare. Administratörer och personal ska alltid använda dem om de har åtkomst till personliga uppgifter eller tekniksystem.

Uppdatera och uppgradera dina system

Bland det viktigaste man kan göra för att skydda sig själv är att hålla enhetens operativsystem och appar uppdaterade. Det här är ännu viktigare för grund- och gymnasieskolor eftersom de är en så viktig del av elevens utbildning och dagliga liv. De flesta attackerna med skadlig programvara i både utbildningssammanhang och andra högrisksammanhang har varit Windows-baserade, till exempel SolarWinds, utpressningsviruset i Los Angeles Unified School District, hackningen i Little Rock School District, dataintrånget i Microsoft Exchange Server, utpressningsviruset i Albuquerque School District och det senaste Microsoft-intrånget på federala myndigheter.

Det här är ytterligare ett användningsområde där molnprodukter och tjänster bör göra administratörens arbete enklare genom att minska attackytan och säkerställa att deras system och appar uppdateras automatiskt.

Uppgradera till ett modernt operativsystem och håll det uppdaterat

Den senaste versionen av operativsystem brukar innefatta nya säkerhetsfunktioner som förhindrar kända attack-bärare. Du bör aktivera en automatisk uppdateringsfunktion i enhetens operativsystem. Om automatiska uppdateringar är omöjliga kan du ladda ned och installera programkorrigeringar och uppdateringar från en betrodd leverantör minst varje månad.

Chromebooks körs på ChromeOS, så de har frekventa automatiska uppdateringar med de senaste säkerhetskorrigeringarna. Det möjliggör snabb implementering av de senaste innovationerna inom säkerhet de verifierar integriteten i det skrivskyddade operativsystemet före start. Dessutom krypterar de all data som lagras på enheten och skyddar den från obehörig åtkomst och kör varje webbplats och app i en separat sandlåda. Så om en webbplats eller app infekteras med skadlig programvara kan den inte spridas till andra delar av enheten.

Är skolan inte redo att övergå till Chromebooks är ChromeOS Flex en version av ChromeOS som har tagits fram för att modernisera skolans enheter. ChromeOS Flex tillhandahåller alla med en sammanslagen, modern undervisnings- och inlärningsupplevelse med proaktiv inbyggd säkerhet och molnbaserade hanteringsfunktioner. Flex kan tillhandahålla automatiserat skydd och blockera skadliga körbara filer och program utan att ersätta den befintliga maskinvaran.

Uppgradera till en modern webbläsare och håll den uppdaterad

Det är viktigt att säkerställa att även webbläsaren är uppdaterad och säker. Moderna webbläsare erbjuder mer avancerade säkerhetsfunktioner och kan uppmana användare att enkelt aktivera dem. De kan även konfigureras av administratörer som aktiverar funktionerna som standard på institutionens datorer, vilket skyddar konfidentialiteten i känsliga uppgifter vid överflyttning på internet. Webbläsaren bör hållas uppdaterad. En modern webbläsare gör följande vare sig du ägnar dig åt arbete, lärande eller andra onlineaktiviteter:

- **Tillämpar pålitlig säkerhet** med webbplatsisolering och skydd för säker webbplatssökning som förhindrar att användare råkar öppna farliga webbplatser.
- **Aktiverar automatiska uppdateringar** för att säkerställa att webbläsaren får säkerhetsuppdateringar snabbt.
- **Säkerställer att anslutningen är säker.** Moderna webbläsare bör använda Transport Layer Security och användarna kan kontrollera att anslutningen har markerats som säker genom att klicka bredvid webbadressen.

Chrome har tagits fram med säkerheten i åtanke. Säkerhetsfunktioner som säker webbsökning är aktiverade som standard. Dessutom finns integrerad lösenordshantering som kan fylla i lösenord automatiskt när du söker på webben så att du enkelt kan använda starka lösenord.

Aktivera varnings- och övervakningssystem i realtid

Med varnings- och övervakningssystem i realtid kan skolorna identifiera och svara snabbt på hot innan de gör skada. Det är viktigt att säkerställa att säkerhetsverktyg som samlar och loggar säkerhetshändelser i dina system körs i bakgrunden. AI-verktyg är bra på att gå igenom stora mängder insamlad data och hitta avvikelser och mönster som kan användas för att snabbare och enklare identifiera hot och behandla och åtgärda sårbarheter. På så sätt kan man prioritera vilka aktiviteter som måste granskas av IT-administratören eller personalen.

Skolor kan använda varnings- och övervakningsfunktioner som är inbyggda i deras primära samarbets- och kommunikationsprogram, till exempel Google Workspace for Education eller implementera separata säkerhetsinformations- och händelsehanteringslösningar (SIEM-lösningar).

Varnings- och övervakningssystem i realtid kan spåra en rad aktiviteter i ett skolnätverk, enheter, appar, användare och data, till exempel användarinloggningar, åtkomst till filer, potentiella intrång, stöld eller stöldförsök av data och administratörsaktiviteter.

Upptäcker systemet misstänkt aktivitet kan det skicka en avisering till skolans IT-personal. På så sätt kan administratörerna undersöka problemet och vidta åtgärder för att mildra hotet.

Varnings- och övervakningsverktyg kan användas för att få djupare förståelse för hoten som skolorna står inför. Genom att analysera data från system i realtid kan skolorna identifiera trender och mönster som gör att de får ett bättre skydd.

Här är några rekommenderade metoder för varnings- och övervakningssystem (inkl. SIEM):

1. **Fastställ era säkerhetsmål**
   Identifiera vilken information och vilka system som är viktigast för skolan och vilka typer av hot som utgör största risken för dem. Arbeta sedan för att identifiera den data ni behöver samla in för att övervaka hoten.
2. **Samla in rätt data och konfigurera på rätt sätt**
   Det är viktigt att samla in rätt data och konfigurera att apparna tar itu med de mest relevanta säkerhetsmålen. Det kan innefatta data från brandväggar, innehållsfilter, system för detektering av intrång, webbservrar och andra säkerhetsenheter tillsammans med kommunikations- och samarbetsprogram, skolans informationssystem och lärplattformar.
3. **Undersök och reagera på varningar**
   När övervakningssystemet genererar en varning är det viktigt att undersöka problemet och vidtalämpliga åtgärder. Det kan innebära att samla flera team för att undersöka källan till varningen, fastställa om det är en falsk positiv eller vidta åtgärder för att mildra hotet, till exempel stänga av konton, återställa användarnas lösenord, sätta i karantän eller radera e-postmeddelandet, ändra filbehörigheter eller rensa enheter.

Utbilda lärare, personal och elever

Grund- och gymnasieskolor bör satsa på att skapa medvetenhet kring säkerhet och skolcommunityns vanor genom kampanjer och partnerskap som stärker användarna. Genom att utbilda lärare, personal och elever om vikten av säkerhet kan de skydda sig själva online, vilket förhindrar allvarliga cybersäkerhetshot. Lär dem hur de ska använda de produkter och tjänster som finns på institutionen, hur de kan identifiera och rapportera hot som nätfiskemeddelanden och framför allt hur de ska göra för att förebygga sådana attacker. Skolor och distrikt bör satsa på att skapa medvetenhet kring säkerhet och skolcommunityns vanor genom kampanjer och partnerskap som stärker användarna.

Använda enheter och program på ett säkert sätt

Administratörer kan samarbeta med lärare och experter för att ta fram läroplaner för cybersäkerhet på åldersadekvata nivåer. Målet är att eleverna ska förstå hur de använder enheter, program och system på ett säkert sätt. Genom att skapa utbildningsmaterial för skola eller distrikt får rekommendationerna för lärare och elever ett sammanhang. Ni kan även dra nytta av tillgängligt material, till exempel Be Internet Awesome som finns i Googles säkerhetscenter och Khan Academy och skräddarsy efter era behov. Programmen ser till att användarna säkra var de än är – i skolan eller i communityn.

Identifiera hot

En viktig del av att hålla lärare, personal och elever trygga är att lära dem att identifiera hot. Det är viktigt att lära barn hur de ser om något är ett hot eller inte eftersom de kanske inte vet hur man avgör om något är legitimt. Det finns några typer av hot som de bör kunna identifiera och känna till hur man rapporterar. Administratörerna bör fokusera på de områden och åtgärder som de anser ger störst effekt i förhållande till insatsen. Utbildning ska inte bara lära användarna att känna igen hotet men även att åtgärda det. Vanliga hot som användarna bör kunna identifiera innefattar utpressningsvirus, nätfiske, social manipulering, skadlig programvara och bedrägerier, men om vissa hot är vanliga inom en viss institution är det värt att säkerställa att skolgemenskapen känner till dem.

Säker data- och fildelning

Lärare och personal bör få utbildning i hur filer och data delas och kunna identifiera olämpliga begäranden per e-post. De bör se till att känsliga personliga uppgifter endast delas eller behandlas vid behov och med ytterligare säkerhetsskikt för datan, till exempel att aldrig delas via e-post eller med externa parter. De bör använda funktioner för att förebygga dataförlust (som ingår med ChromeOS och Workspace for Education) för att varna och förhindra att slutanvändare delar filer med känsliga uppgifter (som personnummer) eller kopierar och klistrar in känsligt innehåll utanför domänen.

Googles strategi i praktiken: Enheter och tjänster för Education

Programupphandling är ett av de mest kraftfulla verktygen ett skoldistrikt har för att skydda sig själv. Programvaran ska vara strukturerad och framtagen för att minimera risken för sårbarheter med inbyggd säkerhet i varje lager. Genom att kräva att skolorna köper in säkra program eller program från företag med dokumenterad säkerhetserfarenhet kan den cyberrisken i stort minskas väsentligt. På Google har vi till exempel förstärkt ChromeOS samtidigt som vi fortsätter implementera mer proaktiva, intelligenta lösningar som drar nytta av vår expertis inom maskininlärning, molnet och identitetsexpertis.

Google strävar efter att skapa produkter som skyddar elevers och lärares integritet och förser skolan med förstklassig säkerhet. Du kan vara säker på att Google for Educations produkter och tjänster kontinuerligt skyddar användare, enheter och data från allt mer komplexa hot. I det här avsnittet går vi igenom säkerhetsrekommendationer för skolans IT-administratörer vid användning av Google for Education-produkter.

Google Workspace for Education

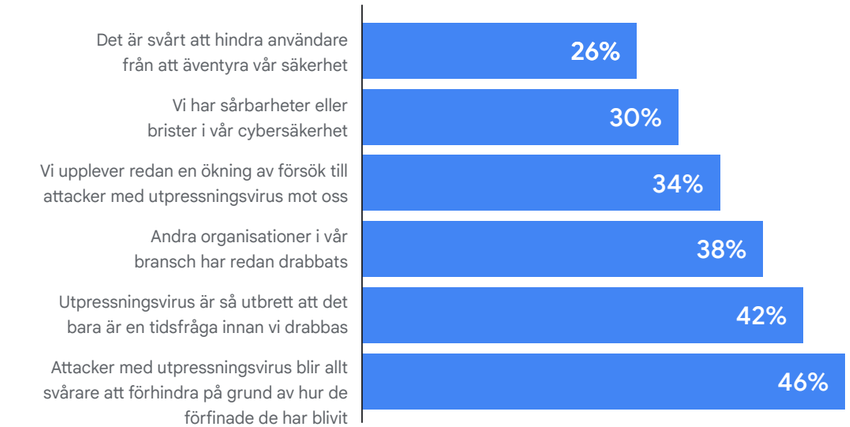
Google Workspace for Education är en uppsättning verktyg och tjänster från Google som har skapats särskilt för skolor och hemundervisning, för samarbete och för smidig och trygg undervisning. Produkter och tjänster från Google for Education skyddar användare, enheter och data från komplexa hot och tillhandahåller verktyg som varnings- och säkerhetscenter, ett arkiv för elektronisk bevisanskaffning, identitets- och åtkomsthantering och förebyggande av dataförlust.

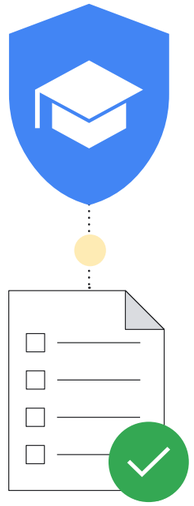
Vi har samlat användbart material om du precis har kommit igång med Google Workspace for Education. Mycket av det kan hjälpa dig göra inställningar i enlighet med rekommendationerna med den här vägledningen. Läs Snabbstartsguide för IT-konfigurering om du behöver hjälp med att komma igång med Google Workspace for Education.

Säkerhetschecklistor

Gå igenom säkerhetschecklistorna för att lära dig mer om hur du stärker säkerheten och integriteten på din skola. Skolor med Google Workspace for Education-utgåvorna Standard och Plus kan även använda sidan säkerhetsstatus för att övervaka konfigurationen av inställningar i Administratörskonsolen. Du kan till exempel kontrollera status för inställningar som automatisk vidarebefordran av e-post, enhetskryptering, inställningar för delning av enheter och mycket annat. Om det behövs kan du göra anpassningar av domänens inställningar utifrån allmänna säkerhetsriktlinjer och metodtips, samtidigt som du balanserar dessa riktlinjer med organisationens affärsbehov och riskhanteringspolicy.

Därför förväntar sig utbildningssektorn att drabbas





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

Här följer andra användbara tips för att se till att du maximerar de inbyggda skydden i Google Workspace for Education:

Konfigurera organisationsenheter (OE)

Det är ingen bra idé att ge alla användare på Google Workspace for Education-kontot samma inställningar. Organisationsenheter är användargrupper och du kan ge olika tjänster, inställningar och behörigheter till olika användare, till exempel med 2SV för lärare och personal och åldersanpassad autentisering för unga elever. Konfigurera separata organisationsenheter för personal, lärare och elever för att tillämpa olika policyer på varje användargrupp. Det är viktigt att du har en noggrant utformad struktur så du kan hantera Google Workspace for Education-kontot så smidigt och flexibelt som möjligt.

Konfigurera lösenordspolicyer och skydd för administratörskonton

Som vi nämnt är autentisering en viktig del av att hålla institutionen säker. Därför har vi konfigurerat flexibla sätt att hantera autentisering för administratörer som gör att du kan se till att användarna har lämpliga och säkra kontoskydd. Ange lösenordspolicyer för att säkerställa att användarna skapar starka lösenord och överväg att kräva 2SV i tillämpliga fall baserat på rekommenderade grupperingar i avsnittet om säker inloggning. Du kan tillämpa 2SV för en del användare (och ge dem tid att konfigurera det) och implementera 2SV med en rad metoder, till exempel säkerhetsnycklar (de säkraste), ett meddelande från Google (med Googles appar på Android och iOS), generatorer för att verifiera appar (som Google Authenticator) och sms eller telefonsamtal (vilket är den minst säkra metoden).

Om organisationen använder en annan identitetsleverantör (IdP) än Google kan du konfigurera Single Sign On (SSO) via en identitetsleverantör från tredje part. Om du vill kan du fortfarande använda 2SV med SSO för konton som inte är avancerade administratörer.

Aktivera och inaktivera tjänster

Administratörer kan styra vilka av Googles tjänster användarna kan få åtkomst till med sitt Google Workspace for Education-konto från Googles administratörskonsol. Du kan styra åtkomst till Googles tjänster, till exempel Kalender, Drive och Meet genom att aktivera och inaktivera tjänsterna efter organisationsenhet (du kan även aktivera tjänster med grupper). Du kan även granska skillnader mellan Workspace Core och tilläggstjänster innan du aktiverar tilläggstjänster som YouTube, Google Maps och Blogger. Administratörerna uppmuntras ge åtkomst till Googles tjänster baserat på ålder. Tänk på att användare som klassificeras som under 18 år automatiskt har begränsningar i vissa av Googles tjänster när de är inloggade på sina Google Workspace for Education-konton.

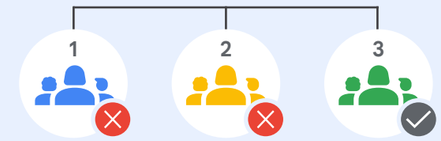
Du kan använda sammanhangsmedveten åtkomst (tillgänglig i Workspace for Education Standard och Plus) för att tillåta och blockera åtkomst till Googles appar som Gmail, Drive och Kalender baserat på enhetens IP-adress, geografiska ursprung, säkerhetspolicyer eller operativsystem. Du kan till exempel tillåta Drive för datorn på företagsägda enheter i specifika länder/regioner.

Metoder för att ge användare åtkomst till tjänster

I Googles administratörskonsol kan du inaktivera en organisationsenhets åtkomst till en Google-tjänst, till exempel Google Drive. Behöver användare i organisationsenheten använda Drive har du två alternativ:

1. Du kan flytta användarna till en organisationsenhet där Drive är aktiverat.
2. Du kan lägga till användarna i en åtkomstgrupp och aktivera Drive för gruppen. Alla medlemmar har åtkomst till tjänsten, även om deras organisationsenhet har tjänsten inaktiverad.

Organisationsenheter



Google Drive är avstängt för organisationsenhet 1 och 2.

Inom en åtkomstgrupp

Men en **grupp användare** inom organisationsenhet 1 och 2 kan använda Google Drive med

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

Konfigurera datadelningspolicyer och lagringsregler

Som administratör kan du styra om användarna får dela Google Drive-filer och mappar med personer utanför organisationen. Det kan förebygga oavsiktlig eller alltför omfattande delning av data och filer, vilket förebygger dataläckage. Uppdelning av filer och enheter som skapar organisationsenheter och att jobba med principen för minsta behörighet är viktigt för att förebygga att angriparna tar sig igenom flera nätverk om de lyckas infiltrera ett konto. Ju mindre data och nätverksåtkomst en potentiell angripare har åtkomst till, desto mindre skada kan ske.

Inaktivera extern fildelning för elever (eller begränsa extern delning endast till tillåtna domäner) och ställ in Åtkomstkontroll på Endast mottagare. Tillåter ni att vissa eller alla användare delar filer utanför domänen ska du aktivera en varning när en användare gör det. Dessutom ska du inaktivera filpublicering på webben och kräva att externa samarbetspartner loggar in med ett Google-konto.

Dessutom kan kunder med Workspace for Education Standard och Plus använda Målgrupper och Förtroenderegler för att ställa in delningsrekommendationer och begränsningar på en mer detaljerad nivå. Med Målgrupper kan du ställa in standardmålgruppen för länkdelning för lärare som Lärare och personal i stället för alla på institutionen. Med Förtroenderegler kan du blockera grundskoleelever från att dela filer med gymnasieelever.

Granska policyer för delade enheter för att säkerställa att endast lämpliga användare kan skapa delade enheter och förhindra externa användare från att få åtkomst till delade enheter. Vi rekommenderar att du endast tillåter att administratörer (eller personal och lärare) skapar delade enheter och att du hanterar delad enhetsåtkomst noggrant.

Du kan överväga att begränsa katalogsynlighet och kontaktdelning antingen genom att inaktivera kontaktdelning för vissa eller alla användare eller genom att skapa anpassade kataloger för att begränsa vilka användare som visas för vilka.

Konfigurera policyer för förebyggande av dataförlust (DLP) i Drive och Gmail för att identifiera och blockera känsliga uppgifter. Det finns redan färdigetablerade policyer som kan utnyttjas för att skydda allmänna känsliga uppgifter (till exempel bankkonto- och kreditkortsnummer). Du kan även skapa anpassade policyer baserade på sökord, ordlistor och reguljära uttryck.

Hantera Gmail-inställningar

Gmail är en av tjänsterna i Google Workspace for Education och det finns många inställningar som administratörer kan dra nytta av för att skydda sin institution och sina användare. Förhindra skräppost, identitetsförfalskning och nätfiske med Gmail-autentisering. Anpassa inställningar för skräppostfilter, till exempel kräv autentisering för alla godkända avsändare och inaktivera skräppostfilter för interna avsändare.

Inaktivera POP/IMAP-åtkomst när det är möjligt och aktivera förbättrad meddelandeskanning före leverans och avancerat skydd mot nätfiske och skadlig programvara. Tillåter ni externa e-postmeddelanden för vissa eller alla användare kan du aktivera varningar om externa mottagare.

Google Workspace for Education Standard och Plus-kunder kan också skydda mot skadlig programvara och utpressningsvirus genom att konfigurera regler för att identifiera skadliga bilagor med Säkerhetssandlåda.

Appar från tredje part

Använd inbyggda godkännandeflöden för att godkänna appar från tredje part som ger åtkomst till kontodata via API:er. Det här förebygger att obehörig data delas med appar från tredje part som inte har godkänts för skolanvändning.

Rapporter och övervakning

Som administratör kan du visa rapporter och logghändelser i Googles administratörskonsol för att granska aktivitet i organisationen, till exempel potentiella säkerhetsrisker, se vem som loggar in och när och förstå hur användarna skapar och delar innehåll. Du kan visa data på domännivå tillsammans med detaljer på användarnivå via diagram och tabeller. Visa rapporter och granskningsloggar (inklusive varningscenter) för att identifiera säkerhetsrisker, analysera serviceanvändning, diagnosticera konfigurationsproblem, spåra användaraktivitet och mycket annat.

Administratörer för Google Workspace for Education Standard och Plus kan använda sig av säkerhetsöversikten och visa en översikt över olika säkerhetsrapporter, identifiera trender och jämföra aktuell och historisk data, till exempel fildelning i Drive, skräppost, nätfiske och aktivitet med skadlig programvara i Gmail, misstänkta inloggningar på användarkonto och misstänkta enhetsaktiviteter. Det mesta av användningen, aktiviteten och granskningsloggarna, till exempel administration, Drive, Meet och händelser i chattloggen samt säkerhetsrapporter, finns tillgängliga i sex månader.

Använda säkerhetscentret

Administratörer för Google Workspace for Education Plus och Standard kan utnyttja säkerhetscentret som tillhandahåller avancerad säkerhetsinformation och analyser och utökad synlighet och kontroll av säkerhetsprogram som påverkar domänen.

I säkerhetscentret finns verktyget för säkerhetsutredning som kan hjälpa administratörer att identifiera, utvärdera och vidta åtgärder för säkerhets- och integritetsproblem, till exempel nätfiskeattacker, olämplig fildelning, misstänkt användar- och enhetsaktivitet och mycket annat.

Google Workspace är världens säkraste molnbaserade kommunikations- och samarbetssvit

0

aktivt exploaterade programvarusårbarheter i Workspace sedan november 2021*

50%

potentiella besparingar på försäkringspremier gällande cybersäkerhet genom att använda Google Workspace

2x färre

säkerhetsincidenter för organisationer som använder Workspace jämfört med Microsoft 365

2.5x färre

säkerhetsincidenter för organisationer som använder Workspace jämfört med Microsoft Exchange

*Enligt CISA är detta betydligt lägre än för andra produktivitetsleverantörer i den här sektorn.

Google Chromebooks for Education

Chromebooks är säkra, skalbara och lättanvända datorer för elever och lärare tack vare Chromebooks inbyggda säkerhetsfunktioner. Det finns inga rapporterade utpressningsvirusattacker mot ChromeOS-enheter som används av företag, skolor eller privatpersoner. Chromebooks skyddar skolor från föränderliga hot genom uppdaterade funktioner och uppdateringarna sker automatiskt i bakgrunden så att användarna kan fortsätta jobba på bara några sekunder.

Automatiska uppdateringar av operativsystem och appar med inbyggt skydd mot skadlig programvara

Angriparna försöker konstant utnyttja fel och kryphål i operativsystem, webbläsare och populära appar för att installera skadlig programvara och stjäla användaruppgifter. För att skydda dig och dina användare håller Chromebooks OS och appar uppdaterade eftersom det är säkert med säkerhetsuppdateringar. Molnprogram kräver inga programuppdateringar på samma sätt som lokala appar. Säkerhetschippet från Google på Chromebooks skyddar enheterna, användarnas identitet och säkerställer systemintegritet.

Chromebooks kör de senaste uppdateringarna för skydd mot skadlig programvara automatiskt. Elever och pedagoger är skyddade mot cyberhot med inbyggda säkerhetsfunktioner som datakryptering, verifierad uppstart, sandlådor och automatiska uppdateringar.

Skydda användaruppgifter

När du loggar in på en Chromebook med ditt Google-konto lagras all data i krypterade filer och säkerställer att ingen annan på enheten kan se din data eller logga in på appar med ditt konto. Det gör det väldigt enkelt och säkert för elever att dela enheter i ett klassrum och för skolor att minska sin totala kostnad för datoranvändning. För mer avancerade säkerhetsfunktioner erbjuder licensen för enhetshantering Chrome Education Upgrade förbättrad synlighet.

Säkerhetspolicyer för användarhanterade fjärrenheter

Skolans administratörer kan konfigurera Chrome OS-policyer och installera/uppdatera appar på distans med Googles administratörskonsol. Med bara ett klick kan en enda IT-administratör uppdatera policyerna och konfigurationerna av hundratusentals Chromebooks på ett ögonblick.

Det säkerställer att

- Elever bara kan få åtkomst till innehåll och appar som skolan har godkänt
- Alla appar och tillägg uppdateras med de senaste säkerhetskorrigeringarna
- Användarna inte kan kopiera, överföra eller dela skolans data från enheterna
- Skolan kan fatta databaserade beslut med anpassade säkerhetsrekommendationer från Google för att hantera säkerhetshot
- Skolan kan hantera säkerheten och policyerna för identitets- och åtkomsthantering för alla användare i administratörskonsolen.

Exempel på policyer som administratörerna kanske vill konfigurera är:

Enhetspolicyer

- **Gästläge**
  Vi rekommenderar att ni inaktiverar enheternas gästläge så eleverna och lärarna måste logga in med sina egna användaruppgifter i stället för att använda enheten anonymt.
- **Inloggningsbegränsningar**
  Ni kanske inte vill att elever och lärare loggar in på skolans Chromebooks med sina personliga Gmail-konton. Tillämpa inloggningsbegränsningar så de begränsas till endast er Workspace-domän för enheter som används endast av elever.
- **Användar- och enhetsrapportering**
  Administratörer bör överväga att aktivera användar- och enhetsrapportering så de kan samla in mätvärden på hur ofta Chromebooks används, vem som använder dem och maskinvarans skick.
- **Tvingad återregistrering**
  Det är viktigt att en Chromebook som tillhör en skola stannar i skolan om den inte avregistreras av en administratör. Administratörer bör överväga att aktivera återregistrering av Chromebooks så en Chromebook alltid registrerar sig själv igen som om den hade rensats eller det hade skett ett stöldförsök.

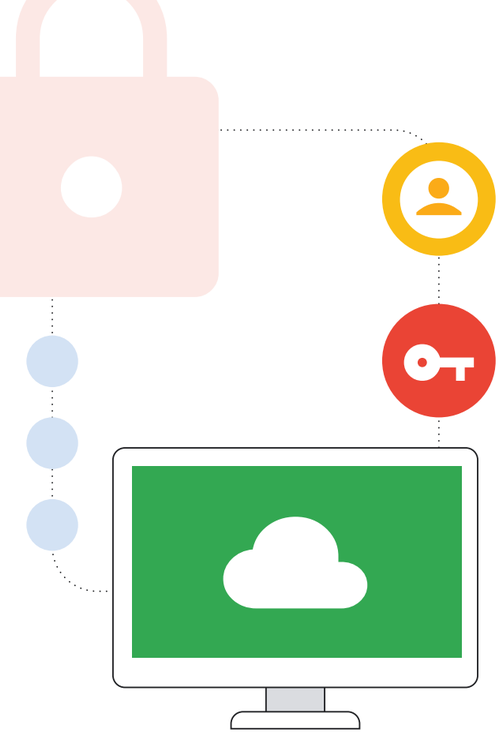
Användarpolicyer

- **Inkognitoläge**
  Eleverna ska ges möjlighet att använda skolans Chromebooks effektivt. Det innebär att de begränsas till den autentiserade webbläsaren så att webbinnehållsfilter håller dem borta från olämpliga webbplatser. Administratörer ska inaktivera Inkognitoläge så eleverna inte ska kunna kringgå webbfilter.
- **Proxyläge**
  Vissa skolor kan använda proxylägen för webbfiltrering men det är viktigt att inaktivera möjligheten för användarna att själva ändra proxyinställningarna.
- **Åtkomst med multiinloggning**
  Om användarna får logga in på ett sekundärt konto samtidigt som de använder skolans Chromebooks och Workspace-konton kan användaren enkelt stjäla känsliga elev- eller skoluppgifter till det sekundära kontot. Administratörerna bör överväga att blockera åtkomst med multiinloggning.
- **Webbläsarhistorik**
  För elever kan det vara bra att inaktivera möjligheten att rensa webbhistoriken. Om en internetsäkerhetsincident skulle uppstå kan historikloggarna vara till nytta vid en undersökning.

Den här listan är en bra utgångspunkt för att säkerställa att nätverken är skyddade mot de vanligaste misstagen som leder till stora cyberincidenter. Andra ytterligare rekommenderade säkerhetspolicyer finns i Säkerhetschecklistan.

Slutpunktshantering för säker användning var och när som helst

Med fjärrsystemet för policyhantering i Chrome OS kan administratörerna tillämpa säkerhetsinställningar och köra säkerhetsverktyg som innehållsfiltreringssystem på enheten i stället för på skolans nätverksservrar. Det säkerställer att eleverna får samma säkerhetsförmåner på skolans Chromebooks hemma som i klassrummet. Det här blir allt viktigare eftersom skolor övergår till digitala skolböcker och onlineverktyg och därför behöver skicka med datorerna hem för att eleverna ska kunna göra läxan.

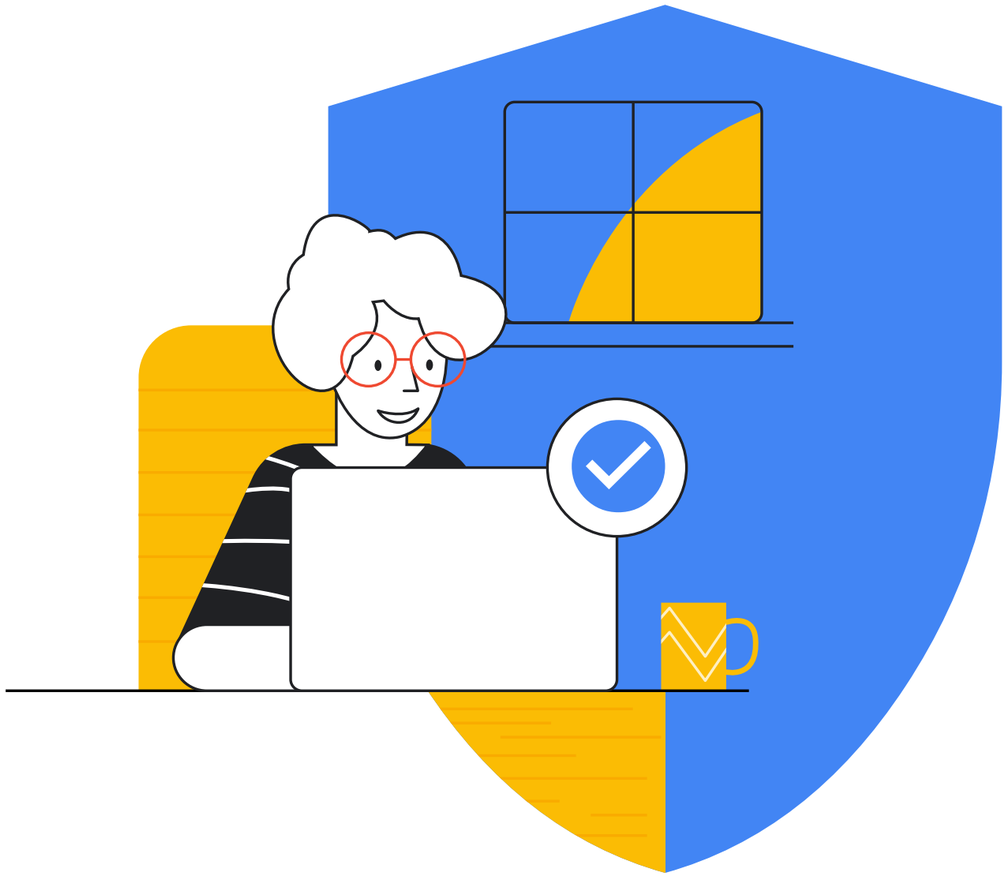


Sammanfattning

Det är komplicerat att skydda grund- och gymnasieskolor från cyberincidenter, men det är väl värt investeringen för att skydda dig själv, eleverna, lärarna, personalen och det övergripande ekosystemet online. Det vi har gått igenom i det här dokumentet är en bra start. Varje skola behöver dock anpassa rekommendationerna efter sina unika behov och fortsätta utvecklas allteftersom hoten och tekniken växer fram. Det du har här är en stabil grund för alla säkerhetsprogram för grundskole- och gymnasienivå. Härifrån kan du fundera ut nästa steg och vilka åtgärder som kan implementeras. Google har även en rad resurser, utbildningar och skickliga specialister inom cybersäkerhet som kan hjälpa skolor och organisationer med den här guideboken och med ny teknik som AI. Googles produkter har skräddarsytts för utbildning och erbjuder färdiga lösningar för många av fallgroparna inom cybersäkerhet som har tagits upp i det här dokumentet. Vi ser fram emot att jobba med dig när du tar fram och implementerar säkerhetsprogram.

Resurslista

- [1]Google. ”Tips to Stay Safe & Secure Online.” Googles säkerhetscenter, https://safety.google/security/security-tips/. Åtkomst 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. Åtkomst 6 oktober 2022.
- [3]Microsoft. Microsofts AccountGuard-program Microsoft AccountGuard Program, https://www.microsoftaccountguard.com/en-us/. Åtkomst 6 oktober 2022.
- [4]Google. Programmet Avancerat skydd Google Advanced Protection Program, https://landing.google.com/advancedprotection. Åtkomst 6 oktober 2022.
- [5]Google. Googles säkerhetscenter. Googles säkerhetscenter – Skydda elever och lärare online, https://safety.google. Åtkomst 6 oktober 2022.
- [6]Meta. ”Basics: Help Secure Your Account.” Skydda kontot, https://www.facebook.com/gpa/resources/basics/security. Åtkomst 6 oktober 2022.
- [7]Meta. ”Facebook Protect.” Facebook, https://www.facebook.com/gpa/facebook-protect. Åtkomst 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. Åtkomst 6 oktober 2022.
- Nycklar: https://developers.google.com/identity/passkeys
- Rapporten CISA Protecting Our Future Cybersecurity K-12 https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAO-rapport https://www.gao.gov/products/gao-20-644
- Läs mer om hur Google for Education kan hjälpa dig skydda institutionen i Google for Educations integritets- och säkerhetscenter.
- Nätfiskerapport från Zcaler



Google for Education

Safer with Google