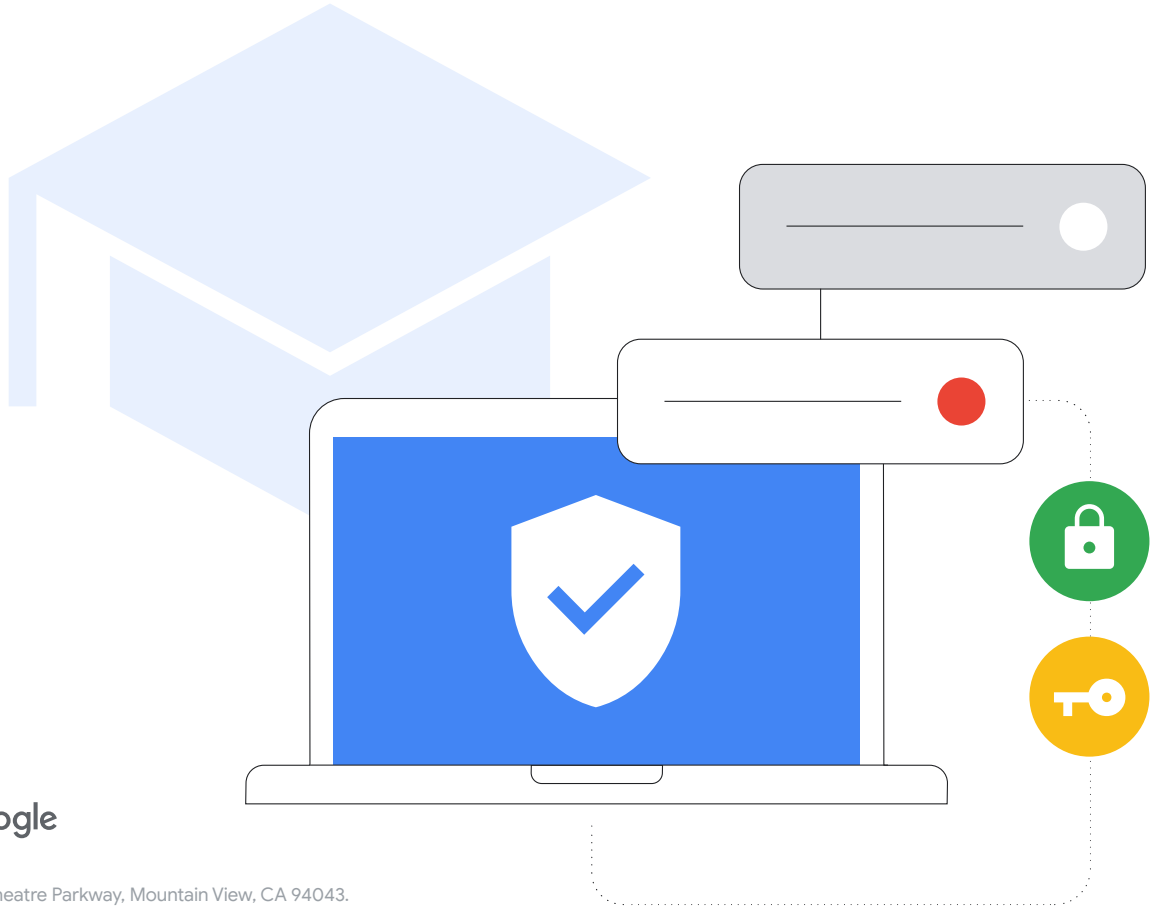
Google for Education

Guida sulla cybersicurezza per l'istruzione primaria e secondaria



Safer with Google

Sintesi

Come evidenzia il report Protecting Our Future[1] della CISA, pe gli istituti di istruzione primaria e secondaria è fondamentale investire in cybersicurezza per proteggere gli studenti, le famiglie, gli insegnanti, il personale non docente e la comunità. Questo documento contiene suggerimenti e best practice per gli amministratori IT scolastici su come preparare e configurare hardware e software negli istituti di istruzione primaria e secondaria per rafforzare la cybersicurezza. Include sia delle best practice generiche sia suggerimenti specifici per i prodotti e servizi Google. La missione di Google è organizzare le informazioni di tutto il mondo in modo da renderle universalmente accessibili e fruibili . Questo approccio è alla base del lavoro del team di Google for Education al momento di creare strumenti progettati per l'insegnamento e l'apprendimento. In questa guida vogliamo condividere ciò che abbiamo imparato nel nostro lavoro.

Le nostre best practice sulla sicurezza sono suddivise per argomenti, in modo da proporre un'analisi più approfondita del le strategie di configurazione, impostazione e riduzione del rischio. Spieghiamo anche in che modo Google tutela la cybersicurezza per i nostri servizi, in particolare per gli strumenti dedicati all'istruzione. Pur fornendo suggerimenti dettagliati in questo documento a prescindere dal prodotto o dal servizio, riteniamo che i nostri prodotti offrano una protezione integrata di livello superiore contro gli attacchi più comuni.

Rischi

Gli istituti scolastici sono tra i target principali degli attacchi informatici compiuti da hacker che cercano di sfruttare illecitamente i sistemi ad alto contenuto di dati presenti nelle scuole. Il 46% delle scuole che non sono ancora state attaccate ritengono che prima o poi lo saranno perché gli attacchi ransomware stanno diventando sempre più sofisticati e difficili da fermare. E il 42% di queste scuole ritiene che ransomware sono così comuni che un attacco è semplicemente inevitabil . La necessità da parte delle scuole di passare rapidamente alla didattica a distanza nel 2020 ha contribuito sensibilmente a far emergere le lacune della cybersicurezza, lasciando le scuole vulnerabili a possibili attacchi.

Misure di prevenzione

Questi attacchi possono essere limitati. Sebbene non esistano tecnologie che eliminano definitivamente i rischi, il settore dell'educazione e i fornitori di tecnologia educativa possono collaborare per adottare e implementare delle best practice per sviluppare un approccio sicuro, affidabile e completo mirato a ridurre in modo significativo i rischi. Grazie alla definizione di misure e prassi per salvaguardare gli utenti, proteggere i dispositivi e garantire la privacy dei dati, gli istituti scolastici possono gestire meglio i rischi e limitare gli attacchi.

Consigli chiave

- **USA L'AUTENTICAZIONE SICURA** per salvaguardare le informazioni sensibili, proteggere le email, i file e altri contenuti ed evitare che utenti non autorizzati possano accedere ai sistemi didattici. Adotta le best practice per l'autenticazione degli utenti, tra cui l'uso di password efficaci, verifica in due passaggi (V2P), passkey e gestori delle password se possibile, in particolare per gli amministratori IT e per il personale che ha a che fare con informazioni sensibili.
- **APPLICA LE IMPOSTAZIONI DI SICUREZZA ADEGUATE** per proteggere gli utenti, i dati e l'ambiente. Sebbene i prodotti Google siano protetti per impostazione predefinita, è fondamentale che gli amministratori utilizzino e configurino in modo adeguato le reti e i sistemi per garantire che siano protetti. Per mettere al sicuro le scuole, occorre applicare i principi della Zero Trust e dei privilegi minimi: gli utenti devono poter accedere solo al software, ai dati, alle applicazioni e ai sistemi di cui hanno bisogno per lavorare in modo efficace.
- **AGGIORNA ED ESEGUI L'UPGRADE DEI SISTEMI** per far sì che gli utenti siano protetti dalle minacce più recenti. Usa sistemi operativi e browser moderni per garantire che gli utenti utilizzino le versioni software più recenti in tutti i dispositivi (oppure versioni stabili e approvate a lungo termine) e che i software vengano aggiornati automaticamente. L'upgrade a una soluzione più sicura, ad esempio i Chromebook, può rafforzare la sicurezza. Nei dispositivi ChromeOS non sono mai stati registrati attacchi ransomware.
- **USA SISTEMI DI MONITORAGGIO E AVVISO IN TEMPO REALE** per migliorare la postura di sicurezza e limitare rapidamente potenziali problemi. Puoi usare queste funzionalità integrate nei software principali di collaborazione e comunicazione, ad esempio Google Workspace for Education, oppure eseguire il deployment di soluzioni separate per il logging e il monitoraggio della sicurezza. Assicura il monitoraggio completo di tutte le attività relative a rete, dispositivi, applicazioni, utenti e dati della scuola. Monitora login agli account, condivisione dei file, volume delle email (in particolare i tentativi di phishing e malware), attività dei dispositivi e modifiche alla configurazione. Mantieni aggiornata la soluzione di monitoraggio e avviso che usi in modo da ricevere notifiche su minacce, eventi critici e variazioni del sistema.
- **ADDESTRA INSEGNANTI, PERSONALE NON DOCENTE E STUDENTI** in modo che sappiano usare dispositivi e software in modo sicuro, riconoscere e segnalare potenziali minacce e condividere i dati in modo adeguato per rafforzare la protezione contro alcuni degli attacchi più comuni. Le scuole o i distretti scolastici possono creare materiali didattici proprietari, nonché usare quelli già pronti e disponibili pubblicamente per avere un toolkit completo per gli istituti.

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

Important Note: This document provides guidance to better secure K-12 institutions, but no guidance can guarantee complete protection from bad actors, and Google does not take responsibility for the implementation or effectiveness of steps mentioned in this guidance. Additionally, nothing in this document should be followed if it is inconsistent with guidance provided by a government officials' employer.

Consigli specifici per gli utenti dei prodotti Google: prodotti come Google Workspace for Education e i Chromebook possono migliorare la cybersicurezza delle scuole e semplificare la messa in pratica di questi consigli. Se combinati, offrono una soluzione completa per proteggere la privacy degli utenti e garantire una sicurezza di primissimo livello per l'istituto.

Queste strategie, insieme ad altri consigli forniti nel seguente documento, sono un ottimo punto di partenza per la sicurezza degli istituti di istruzione primaria e secondaria.

L'Approccio di Google all'istruzione

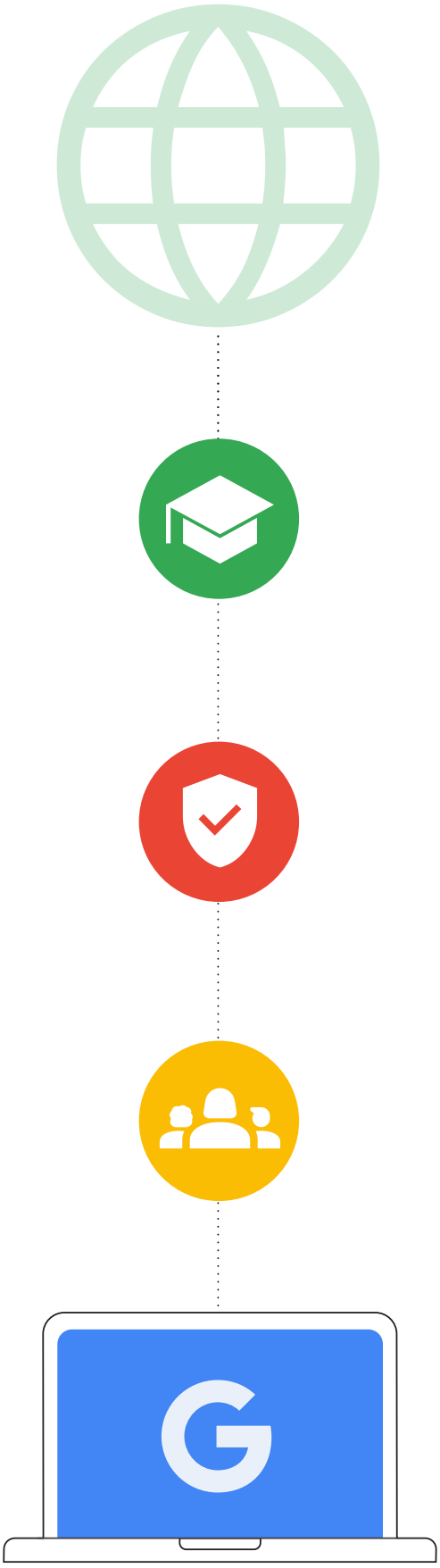
La missione di Google è organizzare le informazioni di tutto il mondo in modo da renderle universalmente accessibili e fruibili, il che è particolarmente utile per il settore dell'istruzione. Il team di Google for Education mira a raggiungere questo obiettivo sviluppando prodotti come Chromebook e Google Classroom che offrono a tudenti e insegnanti un modo semplice e sicuro per creare, condividere e organizzare i propri contenuti, nonché usare le risorse didattiche e gli strumenti online.

Le tecnologie impiegate nelle scuole devono essere progettate in modo tale da tutelare la sicurezza e la privacy consentire il controllo completo e fornire contenuti e informazioni affidabili. Grazie a prodotti come Chromebook e Google Workspace for Education, le scuole hanno una sicurezza di primissimo livello che è conforme ai più elevati standard mondiali nel campo dell'istruzione. Inoltre, gli amministratori IT possono avere una visuale completa e un controllo semplificato dei dati e dei criteri di sicurezza, mentre gli studenti possono dedicarsi completamente all'apprendimento all'interno di un ambiente digitale più sicuro che propone contenuti basati sull'età e riduce al minimo lo spam e le minacce informatiche.

Abbiamo dato la priorità a funzionalità e controlli di sicurezza incorporati, standard elevatissimi per la privacy e strumenti di protezione più proattivi al fine di garantire un ambiente di l'apprendimento sicuro per tutti. I dispositivi ChromeOS attenuano in modo più significativo e minacce per le scuole e sono la miglior difesa contro il pericolo principale per gli istituti, ovvero il ransomware, dato che non sono mai stati registrati attacchi di questo tipo sui Chromebook.

A questo aggiungiamo che Google Workspace for Education è una delle suite di comunicazione e collaborazione basata su cloud più popolare e sicura al mondo. Per ulteriori informazioni su come ogni soluzione protegge la cybersicurezza relativamente ai consigli offerti qui, consulta l'ultima sezione.

Questo documento è suddiviso in due parti. La prima è dedicata a consigli generali e pratici sulla sicurezza per gli istituti di istruzione primaria e secondaria a prescindere dai prodotti, mentre la seconda contiene suggerimenti specifici sulla configurazione per gli istituti che usano i prodotti di Google for Education, come Google Workspace for Education e Chromebook. Entrambe queste sezioni forniscono informazioni su come garantire la sicurezza online delle scuole e degli studenti.



Introduzione

Sia i dispositivi che le reti degli istituti di istruzione primaria e secondaria sono a rischio di attacchi informatici. È fondamentale che gli istituti di istruzione primaria e secondaria garantiscano la miglior sicurezza possibile per proteggere gli studenti ed evitare la perdita di dati, servizi, risorse, tempo e denaro che potrebbe essere causata da questi attacchi.. (Fonte)

Questa guida è uno strumento per promuovere l'implementazione di best practice relative alla cybersicurezza per amministratori e sistemi scolastici al fine di salvaguardare meglio l'ambiente. Grazie all'applicazione di queste best practice, gli istituti di istruzione primaria e secondaria possono limitare o prevenire attacchi informatici gravi e costosi contro i sistemi didattici, e proteggere studenti, famiglie, insegnanti e personale non docente.

Gli attacchi informatici contro le scuole sono sempre più frequenti e gravi. Secondo il K-12 Cybersecurity Resource Center, tra il 2016 e il 2021 sono stati denunciati pubblicamente oltre 1300 attacchi informatici contro organizzazioni che operano nel campo dell'istruzione in tutti e 50 gli stati degli USA. Oggi, la dirigenza scolastica deve proteggere i dati e le informazioni personali di studenti, insegnanti e personale non docente, nonché i sistemi e le informazioni dei propri istituti. Non è facile, soprattutto considerando che nel campo dell'istruzione è stato sempre più difficile tenersi aggiornati in materia di cybersicurezza rispetto ad altri settori.

Attacchi informatici come ransomware, phishing, malware e così via, qualora dovessero riuscire, possono comportare a violazione su larga scala di informazioni che consentono l'identificazione personale, determinare spese ingenti (il costo del riscatto per ransomware è aumentato di cinque volte dal 2020 fino a raggiungere gli 812.260 $) e rallentare il normale svolgimento dei corsi e delle attività didattiche. Di recente, un attacco ransomware ha bloccato un intero sistema scolastico, causando un effetto a catena in tutta la comunità in quanto gli studenti non hanno potuto andare a scuola per giorni. Avendo risorse e fondi limitati, gli istituti di istruzione primaria e secondaria continueranno a essere un bersaglio principale, a meno che non aumentino gli investimenti in cybersicurezza.

La cybersicurezza è sempre più efficace se applicata mediante la comunicazione, la collaborazione e le partnership. Questo documento è stato redatto prendendo come riferimento le raccomandazioni i Google per la sicurezza e la protezione dei sistemi, il Cybersecurity Framework del National Institute for Standards and Technology (NIST), e il toolkit e i consigli forniti dalla CISA n 2023 in merito alla cybersicurezza per l'istruzione primaria e secondaria, tutte fonti estremamente attendibili per le pratiche di cybersicurezza. Questo documento descrive le procedure che gli amministratori IT devono (valutare di) seguire e alcune delle best practice e delle linee guida di Google per i suoi prodotti, oltre ai suggerimenti sulla sicurezza del report Protecting Our Future: Cybersecurity for K-12 | CISA e ai servizi offerti da altre società. Gli amministratori dovrebbero mettere in pratica tutti i consigli sulla sicurezza forniti dalle aziende interessate e implementare le linee guida più recenti, dato che l'azienda responsabile è la più adatta a descrivere i propri prodotti ed eventuali modifiche apportate.

Prima di agire sulla base dei consigli riportati di seguito, è bene prendere in considerazione anche i seguenti fattori:

Considerazioni

1. **Protezione degli studenti.**
   Ogni scuola ha esigenze specifiche e potrebbero essere necessari ulteriori passaggi per garantire la sicurezza e la privacy di determinati gruppi studenteschi. Molti strumenti per la tecnologia educativa hanno funzionalità che consentono l'accesso in base all'età, ad esempio limitando contenuti inappropriati o rendendo privati i dati sulla posizione o di contatto.
2. **Tipi di dati archiviati.**
   Se archivi dati sensibili, conviene criptarli o archiviarli in una posizione a parte..
3. **Tipi di dispositivi in uso e modello di deployment.**
   Occorre aggiornare automaticamente i dispositivi e le applicazioni al loro interno per massimizzare la sicurezza, criptare i dati e isolare gli account in modo che gli utenti accedano solo alle proprie informazioni.
4. **Norme di scuole, distretti scolastici o regionali.**
   Le scuole potrebbero applicare delle norme specifiche in merito all'uso della tecnologia. È necessario verificare che tutte le misure protettive siano configurate in conformità a queste norme.

Ogni giorno, Gmail blocca

100 millioni

di tentativi di phishing.

Ogni settimana, Google identifica

300,000

siti web non sicuri.

Ogni giorno,

74 millioni

di utenti ricevono aiuto dal Gestore delle password di Google.

Ogni anno,

700 millioni

di persone rafforzano la propria sicurezza grazie al Controllo sicurezza.

Usare l'autenticazione sicura

L'autenticazione sicura deve essere una delle priorità per le scuole e altri istituti. Nel quarto trimestre del 2022, gli account poco sicuri o senza la protezione di credenziali hanno rappresentato il 48% di tutti i fattori di compromissione che hanno portato a violazioni dei sistemi. Mettere in pratica alcuni suggerimenti chiave può essere utile per verificare l'effettiva identità degli utenti, nonché per limitare l'accesso alle informazioni in base al ruolo di ogni utente.

Gli amministratori IT dovrebbero applicare la verifica in due passaggi (V2P) (chiamata anche autenticazione a due fattori (2FA)) e passare all'autenticazione senza password (ovvero mediante passkey) ove possibile, in particolare nei casi in cui qualcuno acceda in remoto ai sistemi dell'istituto scolastico. La verifica in due passaggi aggiunge un ulteriore livello di sicurezza agli account online, in modo da rendere più difficile l'accesso da parte di utenti malintenzionati.

Esistono vari tipi di dispositivi e modelli di deployment usati oggigiorno dalle scuole, nonché diversi livelli di capacità tecnica negli ambienti per l'istruzione primaria e secondaria. La sicurezza di account e dispositivi varia a seconda dei ruoli e dei tipi di utenti con best practice specifiche: amministratori IT, insegnanti e personale non docente, studenti più grandi che usano dispositivi assegnati e studenti più giovani che usano dispositivi condivisi. Di seguito vengono descritti i consigli specifici per ogni gruppo.

Esistono vari tipi di metodi di autenticazione consigliati nella maggior parte degli scenari:

- **Password efficaci:**
  G li utenti devono creare la propria password al primo accesso, con requisiti minimi di lunghezza e complessità. Le passphrase lunghe garantiscono una maggiore sicurezza grazie all'uso di un numero maggiore di caratteri, anche con una combinazione complessa. Non conviene chiedere agli utenti di cambiare regolarmente le password poiché ciò potrebbe spingerli a creare password più semplici o ad apportare modifiche di minima entità, ad esempio cambiare un solo carattere.
- **Verifica in due passaggi (V2P):**
  Q uesto tipo di verifica protegge gli account con un secondo passaggio. Si tratta spesso di qualcosa che l'utente ha a disposizione, ad esempio una chiave di sicurezza o un'app su un cellulare che crea un codice di verifica una tantum. Sebbene qualsiasi tipo di verifica V2P aumenti la sicurezza degli account, gli amministratori dovrebbero evitare l'uso di codici di verifica inviati via messaggio o chiamata, in quanto ciò potrebbe aprire le porte ad attacchi basati sul numero di telefono.
- **Autenticazione senza password:**
  Le passkey sono un'alternativa più sicura e semplice rispetto alle password. Gli utenti possono accedere alle app e ai siti web mediante PIN, pattern o sensore biometrico (ad esempio un sistema di riconoscimento delle impronte o del volto) oppure toccando una chiave di sicurezza, in modo che non debbano ricordare e gestire le password. Sebbene questi metodi non siano appropriati per ogni contesto didattico, stanno sempre più sostituendo le modalità tradizionali di autenticazione e rendono l'accesso più sicuro e rapido. Le passkey proteggono gli utenti da attacchi di phishing poiché funzionano solo su app e siti web registrati.
- **Single Sign-On (SSO):**
  Il protocollo SSO consente agli utenti di accedere a più applicazioni e siti web con un singolo set di credenziali. Se gli utenti devono ricordare un solo set di credenziali, è meno probabile che le scrivano. Inoltre, se le scuole non devono gestire più set di credenziali per gli utenti, possono risparmiare denaro in termini di assistenza IT e help desk. L'accesso SSO è nativo in Google Workspace for Education, perciò è possibile usare le credenziali dell'Account Google per accedere ad applicazioni di terze parti oppure usare quelle di un altro provider per accedere ai propri Account Google.
- **Gestori di password:**
  I gestori di password consentono agli utenti di creare password e servizi efficaci e univoci da usare quotidianamente durante le attività scolastiche e lavorative (se non si usa l'accesso SSO). Non aiutano ad accedere al sistema operativo di un dispositivo, ma possono gestire le password dopo che l'utente ha effettuato l'accesso. Gli utenti di Google possono usare Gestore delle password in Chrome su qualsiasi piattaforma, ChromeOS e Android.

Per soddisfare le esigenze specifiche dei vari gruppi, sono disponibili sottoinsiemi o combinazioni speciali di questi metodi di autenticazione, a seconda del ruolo all'interno dell'istituto scolastico, del tipo di sistemi in uso, dei dati a cui accedono gli utenti e della loro età.

Amministratori scolastici

Gli amministratori controllano i sistemi e la maggior parte dei dati di un istituto di istruzione primaria e secondaria. Proteggere i propri account è di fondamentale importanza per la sicurezza dell'intero sistema: dall'infrastruttura ai dati degli account, fino ai dispositivi gestiti dall'istituto. Di conseguenza, devono adottare le soluzioni migliori in termini di autenticazione, tra cui l'uso di password efficaci, un gestore delle password molto sicuro e la verifica V2P. Combinando queste best practice, si ottiene il livello massimo di protezione e sicurezza per l'account amministratore e i servizi aziendali. .

- Gli amministratori dovrebbero utilizzare una chiave di sicurezza fisica o un metodo V2P crittograficamente sicuro che richieda un dispositivo attendibile e prompt. Può trattarsi, ad esempio, di un servizio come Google Authenticator o di un'altra app che crei codici di verifica monouso. I Chromebook rilasciati dopo il 2019 con un chip TPM sono dotati di un pulsante di accensione che può essere utilizzato per l'autenticazione a due fattori.
- Gli amministratori dovrebbero usare un gestore delle password affidabile che supporti la verifica V2P per archiviare le password per i vari servizi.

Insegnanti e personale non docente che usano dispositivi assegnati

Come per gli amministratori, gli insegnanti e il personale non docente possono accedere a dati sensibili, ma non controllano l'infrastruttura digitale e hanno competenze tecniche più variegate.

- Insegnanti e personale non docente che usano i Chromebook dovrebbero poter scegliere di accedere con la verifica biometrica, ad esempio mediante le impronte digitali, se permesso dalla legge.
- Gli amministratori dovrebbero applicare la verifica in due passaggi e passare all'autenticazione senza password ove possibile e nei casi in cui un membro del personale acceda in remoto ai sistemi dell'istituto scolastico.

Studenti più grandi che usano dispositivi assegnati (di solito a partire dalla quarta elementare)

Gli studenti più grandi hanno una maggiore consapevolezza di come proteggersi e di solito sono in grado di usare meccanismi di autenticazione più protettivi, il che è appropriato per i tipi di servizi che è probabile che utilizzino. Dovrebbero poter accedere solo al proprio account e alle informazioni condivise con loro.

- Gli studenti che usano i Chromebook dovrebbero poter scegliere di creare un PIN specifico per il dispositivo per velocizzare l'accesso. Le opzioni biometriche potrebbero non essere appropriate o applicabili in molti ambienti scolastici.
- Ogni studente dovrebbe ricevere assistenza nella creazione di una password univoca che non includa informazioni personali (come nome, aula della classe o data di nascita). Agli studenti occorre insegnare in che modo l'uso delle passphrase può garantire una maggiore complessità delle password, pur rendendole facili da ricordare.

Studenti più giovani che usano dispositivi assegnati (di solito fino alla terza elementare)

Gli studenti più giovani ancora stanno imparando a usare le tecnologie educative, per questo conviene che utilizzino un'autenticazione semplice, adeguata all'uso con servizi e dati limitati.

- Le scuole che usano soluzioni alternative di terze parti per le password, ad esempio codici QR o accesso tramite immagine per gli studenti più giovani o che non possono accedere con le password, dovrebbero usare delle precauzioni poiché questi metodi sono meno sicuri. Gli amministratori dovrebbero modificare la password di uno studente e aggiornare il codice se questo viene perso o viene divulgato ad altre persone.
- Le scuole dovrebbero informare studenti e genitori circa l'importanza di mantenere segrete le password e di conservare in modo sicuro credenziali alternative come i codici QR.
- Nel caso di dispositivi assegnati come tablet, è possibile usare un PIN specifico del dispositivo come metodo alternativo di autenticazione sicura.

Applicare le impostazioni di sicurezza adeguate

Le reti e i dispositivi scolastici sono un target molto visibile e di grande valore per gli hacker di tutto il mondo, perciò è fondamentale applicare le misure di sicurezza più efficaci possibili per evitare perdite di servizi, risorse, dati e denaro. Gli amministratori di sistema dovrebbero implementare funzionalità di sicurezza efficaci e appropriate nei prodotti usati dagli istituti, ma anche fare in modo che i sistemi continuino a essere facili da usare per insegnanti, personale non docente e studenti. Occorre configurare impostazioni importanti per sicurezza e privacy, ad esempio l'impossibilità da parte dei singoli utenti di disattivare o modificare le impostazioni. Inoltre, l'amministratore deve definire valori predefiniti protettivi per altre impostazioni. È fondamentale applicare le misure di sicurezza più efficaci possibili per evitare perdite di servizi, risorse, dati e denaro. Per chi usa i Chromebook, l'ultima sezione contiene i nostri consigli per impostare i criteri relativi ai dispositivi.

Infine, conviene integrare la "minimizzazione dei dati" nelle prassi in atto limitando gli scopi e i mezzi di raccolta, uso e divulgazione delle informazioni personali delle persone per quanto ragionevolmente necessario e adeguato per fornire il servizio o secondo quanto previsto nel contesto della relazione con gli utenti.

Applicazioni e aggiornamenti

Conviene limitare al minimo le app che gli utenti possono installare, dato che ogni applicazione installata su un dispositivo può essere un vettore di attacco che può essere sfruttato. Se possibile, si consiglia di usare applicazioni di origini attendibili. Ad esempio, è opportuno consigliare agli utenti di controllare la presenza del badge di verifica nel Google Play Store per avere la certezza di scaricare applicazioni ufficiali che sono state sottoposte a un controllo della sicurezza. Eventuali modifiche al sistema operativo o all'hardware (jailbreaking o rooting) introducono importanti problemi alla sicurezza e andrebbero evitate.

Accesso e visibilità

Gli amministratori devono fare in modo che gli utenti possano accedere solo ai dati, ai software, ai servizi e ai sistemi di cui hanno bisogno per svolgere le proprie mansioni o attività di apprendimento in modo efficace. Ciò consente di limitare gli accessi non intenzionali e di monitorare gli utenti che accedono a risorse specifiche. Occorre fare particolare attenzione ai dati più sensibili, ad esempio le informazioni sensibili degli utenti (PII), e ai sistemi (come quelli per risorse umane, salari, voti, sicurezza e configurazione) mediante la verifica degli utenti che possono accedere ai dati e le circostanze in cui possono farlo, il tutto limitando l'accesso ai dispositivi di proprietà delle scuole. Inoltre, occorre assicurarsi che possano accedere solo membri specifici del personale.

Controlla i criteri di condivisione dei dati negli strumenti di collaborazione per evitare di condividerli in modo inappropriato o eccessivo, nonché impedire accessi non autorizzati. Limita o blocca la condivisione al di fuori dell'ambiente scolastico (in particolare per gli studenti) implementa delle norme per monitorare la condivisione di contenuti sensibili.

Furto o perdita del dispositivo

Perdere un dispositivo non vuole dire perdere anche i dati. Gli amministratori dovrebbero sviluppare un piano standard per consentire l'accesso a informazioni e documenti in caso di perdita o furto di un dispositivo, ad esempio conservando i documenti in un ambiente cloud. Scarica e stampa i codici di backup per i processi V2P al fine di evitare l'interruzione dell'accesso agli account.

Se un dispositivo viene segnalato come perso o rubato, assicurati che venga bloccato da remoto, se possibile, e che gli account associati vengano bloccati o contrassegnati per fare in modo che non vengano usati per accedere in modo non autorizzato. I contenuti dei Chromebook persi possono essere cancellati da remoto e gli account Google Workspace for Education possono essere monitorati per verificare eventuali attività sospette oppure sospesi (bloccati), se necessario.

Protezione avanzata per utenti ad alto rischio

Per gli utenti che hanno un'alta visibilità e informazioni sensibili (compresi gli amministratori di Google Workspace for Education), Google offre il programma di protezione avanzata (PPA). Questo programma garantisce agli utenti un'ulteriore protezione da attacchi mirati come i tentativi di phishing, nonché download dannosi e violazioni delle password. Il PPA è progettato specificatamente per impedire attacchi online mirati agli Account Google e utilizza automaticamente l'autenticazione avanzata e le chiavi di sicurezza, oltre a limitare l'accesso di terze parti ai dati degli account. Altri provider di account online forniscono protezioni avanzate per gli utenti ad alto rischio, perciò amministratori e personale non docente devono usarle sempre se hanno accesso a informazioni personali o sistemi tecnologici.

Aggiornare ed eseguire l'upgrade dei sistemi

Uno degli aspetti più importanti per proteggersi è mantenere aggiornati il sistema operativo e le applicazioni del dispositivo. Ciò è ancor più importante per gli istituti di istruzione primaria e secondaria, poiché hanno un ruolo fondamentale nell'istruzione e nella vita quotidiana dei bambini. La maggior parte degli attacchi malware in entrambi i livelli didattici e in altri contesti ad alto rischio ha sfruttato il sistema Windows, tra cui SolarWinds, l'attacco ransomware al Los Angeles Unified School District, la violazione dei sistemi del Little Rock School District, la violazione dei dati di Microsoft Exchange Server, l'attacco ransomware all'Albuquerque School District e la recente violazione degli account email di alcune agenzie federali tramite Microsoft. Questo è un altro aspetto per il quale l'uso di prodotti e servizi basati sul cloud dovrebbe semplificare le attività degli amministratori, poiché riduce la superficie di attacco e garantisce che sistemi e applicazioni vengano aggiornati automaticamente.

Passare a un sistema operativo moderno e mantenerlo aggiornato

La versione più recente di qualsiasi sistema operativo di solito include nuove funzionalità di sicurezza per prevenire vettori di attacco noti. È opportuno attivare l'aggiornamento automatico all'interno del sistema operativo del dispositivo oppure, qualora non sia consentito, scaricare e installare patch e aggiornamenti da un fornitore attendibile almeno una volta al mese.

I Chromebook vengono eseguiti su ChromeOS, perciò vengono aggiornati spesso e in modo automatico con le ultime patch di sicurezza per adottare rapidamente le innovazioni più recenti in termini di sicurezza. Inoltre, permettono di verificare l'integrità del sistema operativo di sola lettura prima dell'avvio. Possono anche criptare tutti i dati archiviati nel dispositivo e li proteggono da accessi non autorizzati. Inoltre, ogni pagina web e applicazione viene eseguita in una sandbox a parte in modo che se un'app o un sito web subisce un attacco da malware, questo non può propagarsi in altre parti del dispositivo

Se una scuola non è pronta per passare ai Chromebook, ChromeOS Flex è una versione di ChromeOS che permette di modernizzare i dispositivi della scuola. ChromeOS Flex offre a tutti gli utenti un'esperienza di insegnamento e apprendimento unificata e moderna con sicurezza proattiva e incorporata, oltre a funzionalità di gestione basate su cloud. Flex può fornire una protezione automatizzata e bloccare le app e gli eseguibili dannosi senza sostituire l'hardware esistente.

Eseguire l'Upgrade a un browser moderno e mantenerlo aggiornato

È importante anche aggiornare e proteggere il browser. I browser moderni offrono funzionalità di sicurezza più avanzate che possono essere attivate su richiesta dagli utenti o configurate dagli amministratori in modo che diventino predefinite sui computer degli istituti. Ciò consente di proteggere la riservatezza delle informazioni sensibili che passano su internet. Il browser deve essere sempre aggiornato. A prescindere dalle attività svolte (lavorative, didattiche o di altro tipo online), un browser moderno aggiornato:

- **Userà una sicurezza efficace,,** tra cui l'isolamento dei siti e la navigazione protetta, per evitare agli utenti di visitare inavvertitamente siti web dannosi
- **Attiverà gli aggiornamenti automatici** per garantire che nel browser vengano implementate tempestivamente le nuove funzionalità per la sicurezza
- **Garantirà che la connessione sia sicura.** I browser moderni dovrebbero usare il protocollo Transport Layer Security in modo che gli utenti possano fare clic accanto all'URL per verificare se la connessione è contrassegnata come sicura

Chrome è stato progettato avendo come priorità la sicurezza, con funzionalità predefinite e già attivate come la navigazione sicura. Inoltre, il gestore delle password integrato può compilare automaticamente le password durante la navigazione nel web, in modo da usare facilmente password efficaci.

Usare sistemi di monitoraggio e avviso in tempo reale

I sistemi di monitoraggio e avviso in tempo reale consentono alle scuole di identificare le minacce e rispondere prontamente prima che possano causare danni. È importante garantire che gli strumenti di sicurezza vengano eseguiti in background in modo da raccogliere e registrare gli eventi di sicurezza nei sistemi. Gli strumenti basati sull'IA sono particolarmente utili per analizzare grandi quantità di dati raccolti per trovare anomalie e tendenze, il che potrebbe permettere di rilevare in modo più rapido e semplice le minacce, nonché elaborare e risolvere le vulnerabilità. Ciò consente di dare la priorità alle attività che devono essere controllate dagli amministratori o dal personale IT.

Le scuole possono usare le funzionalità di avviso e monitoraggio incorporate nel software principale di collaborazione e comunicazione, ad esempio Google Workspace for Education, oppure eseguire il deployment di soluzioni SIEM (Security Information and Event Monitoring) separate.

I sistemi di monitoraggio e avviso in tempo reale possono tenere traccia di varie attività relative a rete, dispositivi, applicazioni, utenti e dati della scuola, ad esempio accesso degli utenti, accesso ai file, potenziali intrusioni, furto riuscito o tentato di dati e attività degli amministratori.

Se il sistema rileva attività sospette, può inviare un avviso al personale IT di una scuola. In questo modo, gli amministratori possono esaminare il problema e intervenire per contrastare la minaccia.

Inoltre, gli strumenti di avviso e monitoraggio permettono di capire meglio le minacce che le scuole devono affrontare. Analizzando i dati raccolti da questi sistemi in tempo reale, le scuole possono rilevare tendenze e pattern he aiutano a rendere più efficaci le misure di protezione.

Ecco alcune best practice per usare i sistemi di avviso e monitoraggio (incluse le soluzioni SIEM):

1. **Definire gli obiettivi per la sicurezza**
   Identifica le informazioni e i sistemi più importanti per la scuola e le minacce più gravi che potrebbero metterli a rischio. Poi cerca di trovare i dati da raccogliere per monitorare queste minacce.

2. **Raccogliere i dati giusti ed effettuare la configurazione in modo adeguato**
   È importante raccogliere i dati giusti e configurare le applicazioni in modo da raggiungere gli obiettivi di sicurezza più pertinenti. Potrebbero essere dati di firewall, filtri dei contenuti, sistemi di rilevamento delle intrusioni, server web e altri dispositivi di sicurezza, oltre a software di comunicazione e collaborazione, sistemi informatici scolastici e sistemi di gestione dell'apprendimento.

3. **Analizzare e rispondere agli avvisi**
   Quando il sistema di monitoraggio genera un avviso, è importante analizzare il problema e agire in modo adeguato. Ciò potrebbe includere l'investigazione dell'origine dell'avviso da parte di vari team per determinare se si tratta di un falso positivo oppure intraprendere delle azioni per contrastare la minaccia, ad esempio sospendere gli account, reimpostare le password degli utenti, mettere in quarantena o eliminare le email, cambiare le autorizzazioni dei file o cancellare i contenuti dei dispositivi.

Addestrare insegnanti, personale non docente e studenti

Gli istituti di istruzione primaria e secondaria dovrebbero migliorare le abitudini e la consapevolezza in merito ai temi della sicurezza tra le comunità scolastiche, il tutto mediante campagne e partnership in grado di aumentare le competenze degli utenti. Far capire a insegnanti, personale non docente e studenti l'importanza della sicurezza è fondamentale al fine di aiutarli a proteggersi online ed evitare minacce gravi di cybersicurezza. Insegna loro a usare i prodotti e i servizi disponibili nell'istituto e a individuare e segnalare le minacce come le email di phishing, oltre a spiegare cosa fare per evitare questi attacchi. Scuole e distretti scolastici dovrebbero migliorare le abitudini e la consapevolezza in merito ai temi della sicurezza tra le comunità scolastiche, il tutto mediante campagne e partnership in grado di aumentare le competenze degli utenti.

Come usare dispositivi e software in modo sicuro

Gli amministratori possono collaborare con insegnanti ed esperti per sviluppare programmi di cybersicurezza a livelli appropriati all'età per aiutare gli studenti a capire come usare i dispositivi, i software e i sistemi in modo sicuro. La creazione di materiali didattici proprietari della scuola o del distretto scolastico consente di contestualizzare i consigli per insegnanti e studenti, ma è possibile anche avvalersi di materiali già pronti e disponibili, come Vivi internet, al meglio su Safety.Google e la Khan Academy, per poi adattarli alle proprie esigenze. Questi programmi possono consolidare la sicurezza degli utenti ovunque si trovino, sia a scuola che nella propria comunità.

Riconoscere le minacce

Spiega a insegnanti, personale non docente e studenti che riconoscere le minacce è fondamentale per garantire la loro sicurezza. È importante insegnare ai bambini come capire se qualcosa rappresenta una minaccia o no, dato che potrebbero non saper distinguere la legittimità dei contenuti che vedono. Esistono alcuni tipi di minacce che dovrebbero saper riconoscere e segnalare. Inoltre, gli amministratori dovrebbero concentrarsi sugli aspetti che ritengono possano generare il maggior ritorno sull'investimento. È importante addestrare gli utenti non solo a riconoscere la minaccia, ma anche a prendere le misure del caso. Alcune tra le minacce più comuni che gli utenti dovrebbero riconoscere sono ransomware, phishing, ingegneria sociale, malware e frodi. Se, però, si ha la certezza che alcune siano prevalenti all'interno di un determinato istituto, conviene informare la comunità scolastica al riguardo.

Proteggere dati e condivisione file

Insegnanti e personale non docente dovrebbero essere addestrati a condividere i file e i dati, nonché a riconoscere le richieste inappropriate via email. Devono fare in modo che le informazioni personali sensibili siano condivise e trattate solo se necessario e con livelli aggiuntivi di protezione per i dati, ad esempio per non condividerli mai via mail o con parti esterne. Dovrebbero usare le funzionalità di prevenzione della perdita di dati (inclusi ChromeOS e Workspace for Education) per avvisare gli utenti finali e impedire che condividano file con dati sensibili (come numeri di previdenza sociale) o copino e incollino contenuti sensibili al di fuori del dominio.

L'approccio di Google in pratica: dispositivi e servizi per l'istruzione

L'approvvigionamento del software è uno dei metodi più efficaci che può sfruttare un distretto scolastico per proteggersi. Il software deve avere un'architettura solida ed essere progettato in modo da ridurre al minimo il rischio di vulnerabilità, con sicurezza integrata a ogni livello. Le scuole devono acquistare software sicuri o quanto meno da aziende con un solido background in termini di sicurezza per ridurre in modo significativo il rischio di attacchi informatici in generale. Google ha protetto ulteriormente ChromeOS, ad esempio continuando a implementare soluzioni più proattive e intelligenti che sfruttano la nostra vasta esperienza in termini di machine learning, cloud e identità.

Google si impegna a creare prodotti che proteggano la privacy degli studenti e degli insegnanti e forniscano al tuo istituto la migliore sicurezza possibile. Puoi avere la certezza che i prodotti e i servizi Google for Education proteggono costantemente utenti, dispositivi e dati da minacce sempre più insidiose. Questa sezione è dedicata agli amministratori IT delle scuole e fornisce raccomandazioni concernenti la icurezza durante l'utilizzo di prodotti Google for Education.

Google Workspace for Education

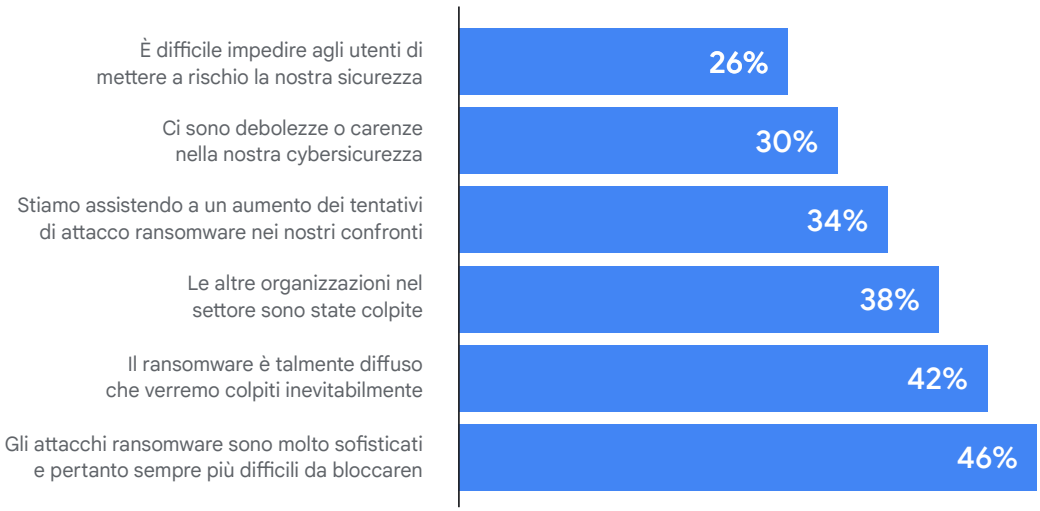
Google Workspace for Education è un insieme di strumenti e servizi Google pensati appositamente per le scuole allo scopo di favorire la collaborazione, semplificare l'apprendimento e proteggere le attività didattiche. I prodotti e i servizi Google for Education proteggono costantemente utenti, dispositivi e dati da minacce sempre più insidiose, oltre a offrire strumenti come i centri avvisi e sicurezza, un vault per eDiscovery, la gestione di identità e accessi, e la prevenzione della perdita di dati.

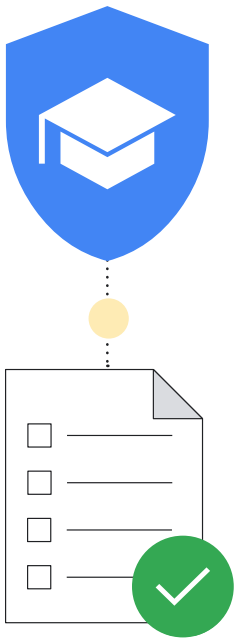
Abbiamo raccolto una serie di materiali utili per chi inizia a usare Google Workspace for Education al fine di aiutarli a configurare la soluzione seguendo le indicazioni qui fornite. Per assistenza su come iniziare a usare Google Workspace for Education, consulta questa guida rapida alla configurazione IT.

Elenchi di controllo per la sicurezza

Consulta gli elenchi di controllo per la sicurezza per scoprire come rafforzare la sicurezza e la privacy dell'istituto. Le scuole che hanno le versioni Standard e Plus di Google Workspace for Education possono anche usare la pagina Stato della sicurezza per monitorare la configurazione delle impostazioni della Console di amministrazione. Ad esempio, puoi controllare lo stato di impostazioni quali Inoltro automatico dell'email, Crittografia dei dispositivi, Impostazioni di condivisione per Drive e altro ancora. Se necessario, puoi modificare le impostazioni del dominio in base alle linee guida e best practice generali sulla sicurezza, adattandole alle esigenze aziendali e alle prassi di gestione dei rischi della tua organizzazione.

Motivi per cui il settore dell'istruzione si aspetta di ricevere attacchi





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

Ecco altri suggerimenti utili per assicurarsi di massimizzare le misure protettive incorporate in Google Workspace for Education:

Creare unità organizzative (UO)

È ovvio che tutti gli utenti di un account Google Workspace for Education devono avere le stesse impostazioni. Le unità organizzative sono gruppi che permettono di assegnare vari tipi di servizi, impostazioni e autorizzazioni a diversi utenti, ad esempio impostando l'accesso V2P per insegnanti e studenti e l'autenticazione adeguata all'età per gli studenti più giovani. È possibile creare unità organizzative a parte per personale non docente, insegnanti e studenti, in modo da applicare criteri specifici a ogni gruppo di utenti separatamente. Una struttura ben progettata è fondamentale per gestire in modo efficace e flessibile l'account Google Workspace for Education.

Configurare criteri per le password e protezioni per gli account degli amministratori

Come abbiamo già detto, l'autenticazione degli utenti è fondamentale per salvaguardare un istituto. Per questo motivo, abbiamo sviluppato dei metodi flessibili per gestire l'autenticazione per gli amministratori, al fine di garantire che gli utenti dispongano di misure adeguate ed efficaci per proteggere gli account. Imposta i criteri delle password per fare in modo che gli utenti creino password efficaci. Inoltre, può essere utile richiedere l'uso della verifica V2P, se appropriata e sulla base dei raggruppamenti consigliati nella sezione dedicata all'accesso sicuro. È possibile applicare forzatamente l'uso della verifica V2P per un sottoinsieme di utenti (dando loro il tempo necessario per configurarla), quindi implementare la verifica V2P usando vari metodi tra cui chiavi di sicurezza (il metodo più sicuro), un prompt di Google (mediante le app di Google su Android e iOS), generatori di app di verifica come Google Authenticator e messaggi o chiamate telefoniche (sebbene queste siano il metodo meno sicuro).

Se la tua organizzazione usa un provider di identità (IdP) diverso da Google, puoi configurare l'accesso Single Sign-On (SSO) mediante un provider di identità di terze parti. Puoi comunque usare la verifica V2P con SSO per account non appartenenti a super amministratori, se preferisci.

Attivare o disattivare i servizi

Gli amministratori possono decidere quali utenti dei servizi Google possono accedere al loro account Google Workspace for Education dalla Console di amministrazione Google. È possibile controllare l'accesso a servizi Google come Calendar, Drive e Meet attivando o disattivando i servizi in base all'unità organizzativa (i servizi possono essere attivati anche quando si usano i gruppi). È possibile anche controllare le differenze tra i servizi principali e aggiuntivi di Workspace prima di abilitarne altri come YouTube, Google Maps e Blogger. Gli amministratori dovrebbero configurare l'accesso ai servizi Google in base all'età e tenere ben presente che agli utenti designati come minori di 18 anni vengono applicate automaticamente delle limitazioni in alcuni servizi Google quando accedono al proprio account Google Workspace for Education.

È possibile anche usare l'accesso sensibile al contesto (disponibile in Workspace for Education Standard e Plus) per consentire o bloccare l'accesso ad app Google come Gmail, Drive e Calendar in base all'indirizzo IP, all'origine geografica, ai criteri di sicurezza o al sistema operativo di un dispositivo. Ad esempio, puoi consentire Drive per computer solo sui dispositivi di proprietà dell'azienda in regioni/paesi specifici.

Metodi per concedere agli utenti l'accesso ai servizi

Nella Console di amministrazione Google puoi disattivare l'accesso di un'unità organizzativa a un servizio Google, ad esempio Google Drive. Se alcuni utenti di quell'unità organizzativa devono utilizzare Drive, puoi scegliere tra due opzioni:

1. Spostare gli utenti in un'unità organizzativa in cui Drive è attivato.
2. Aggiungere gli utenti a un gruppo di accesso e attivare Drive per quel gruppo. Ogni membro potrà accedere al servizio, anche se è disattivato per la sua unità organizzativa.

Google Drive è disattivato per le unità organizzative 1 e 2.

All'interno di un gruppo di accesso

Tuttavia, **un gruppo di utenti** delle unità organizzative 1 e 2 può utilizzare Google Drive

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

Impostare criteri di condivisione dei dati e regole di conservazione

In qualità di amministratore, puoi decidere se gli utenti possono condividere i file e le cartelle di Google Drive con persone al di fuori dell'organizzazione. Ciò è utile per evitare di condividere inavvertitamente o in modo eccessivo dati e file, così da prevenire la perdita di dati. La separazione di file e Drive mediante la creazione di unità organizzative e l'implementazione del principio del privilegio minimo sono aspetti importanti per evitare che utenti malintenzionati si spostino da una rete all'altra se riescono a violare un account. Quanto più è limitato l'accesso ai dati e alla rete per un potenziale utente malintenzionato, minori saranno i danni che potrà causare

Disattiva la condivisione di file esterna per gli studenti (o limita la condivisione esterna solo ai domini autorizzati) e imposta "Controllo di accesso" su "Solo destinatari". Se consenti ad alcuni o a tutti gli utenti di condividere i file all'esterno del dominio, attiva un avviso quando ciò accade. Inoltre, disabilita la pubblicazione dei file sul web e richiedi ai collaboratori esterni di accedere con un Account Google.

Inoltre, i clienti di Workspace for Education Standard e Plus possono usare i segmenti di pubblico di destinazione e le regole di attendibilità per impostare consigli e limitazioni per la condivisione a un livello più granulare. Ad esempio, i segmenti di pubblico di destinazione consentono di impostare il pubblico predefinito per la condivisione dei link per gli insegnanti su "insegnanti e personale non docente", invece che su tutte le persone all'interno dell'istituto. Grazie alle regole di attendibilità, è possibile impedire agli studenti della scuola elementare di condividere file con studenti più grandi. .

Controlla i criteri dei Drive condivisi per assicurarti che solo gli utenti appropriati possano creare Drive condivisi, nonché per impedire a utenti esterni di accedere ai Drive condivisi. Si consiglia di permettere solo agli amministratori (o al personale non docente e agli insegnanti) di creare Drive condivisi e di gestire con grande attenzione l'accesso ai Drive condivisi.

Se possibile, conviene limitare la visibilità della directory e la condivisione dei contatti disattivando quest'ultima per alcuni o tutti gli utenti o creando directory personalizzate per limitare la visibilità degli utenti.Configura criteri per la prevenzione della perdita di dati (DLP) in Drive e Gmail al fine di rilevare e bloccare le informazioni sensibili. È possibile sfruttare criteri integrati per proteggere le informazioni sensibili più comuni, ad esempio numeri di conto bancario o di carta di credito. È possibile anche creare criteri personalizzati sulla base di parole chiave, elenchi di parole ed espressioni regolari (regex).

Gestione delle impostazioni di Gmail

Gmail è uno dei servizi principali all'interno di Google Workspace for Education. Gli amministratori possono definire molte impostazioni per proteggere gli istituti e gli utenti.

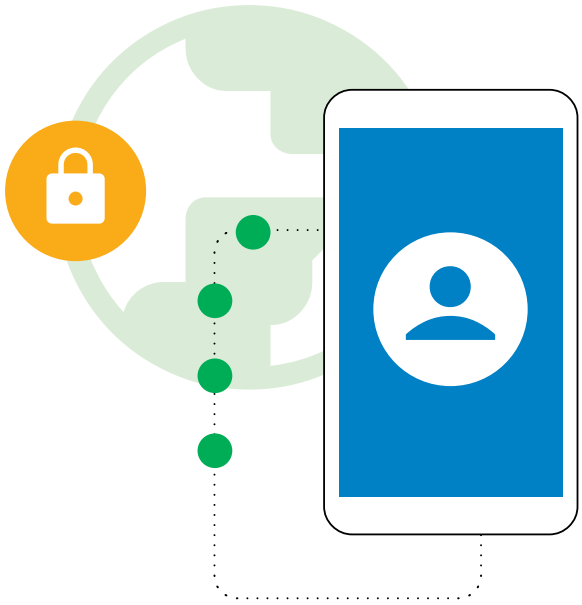
Previeni lo spam, lo spoofing e il phishing con l'autenticazione in Gmail. Personalizza le impostazioni per il filtro antispam, anche richiedendo l'autenticazione per tutti i mittenti approvati e disattivando la possibilità di bypassare i filtri antispam per i mittenti interni.

Disabilita l'accesso POP/IMAP, se possibile, e abilita la scansione avanzata dei messaggi prima della consegna, nonché la protezione avanzata contro phishing e malware. Se consenti le email esterne per alcuni o tutti gli utenti, puoi abilitare gli avvisi di destinatari esterni.

I clienti di Google Workspace for Education Standard e Plus possono anche migliorare la protezione da malware e ransomware impostando delle regole per rilevare allegati dannosi mediante la Sandbox per la sicurezza.

Applicazioni di terze parti

Usa flussi di lavoro incorporati per approvare le applicazioni di terze parti che possono accedere ai dati degli account mediante API. Ciò è utile per impedire la condivisione di dati non autorizzati con applicazioni di terze parti non approvate per l'uso scolastico.



Report e monitoraggio

In qualità di amministratore, puoi visualizzare i report e gli eventi dei log nella Console di amministrazione Google per controllare l'attività all'interno della tua organizzazione, ad esempio potenziali rischi alla sicurezza, nonché sapere chi accede in momenti specifici e capire in che modo gli utenti creano e condividono i contenuti. Puoi visualizzare i dati globali a livello di dominio nonché informazioni dettagliate a livello di utente tramite grafici e tabelle. Visualizza report e log di controllo (incluso il Centro avvisi) per identificare rischi alla sicurezza, analizzare l'utilizzo dei servizi, diagnosticare i problemi di configurazione, tenere traccia delle attività degli utenti e altro ancora.

Gli amministratori di Google Workspace for Education Standard e Plus possono avvalersi della dashboard per la sicurezza per avere una panoramica di vari report sulla sicurezza, identificare le tendenze e confrontare i dati attuali e storici, ad esempio la condivisione dei file in Drive, le attività relative a spam, phishing e malware in Gmail, gli accessi sospetti agli account utente e le attività sospette nei dispositivi. Gran parte dei log di controllo, utilizzo e attività (compresi gli eventi di log di Console di amministrazione, Drive, Meet e Chat), nonché i report sulla sicurezza, sono disponibili per sei mesi.

Utilizzare il Centro sicurezza

Gli amministratori di Google Workspace for Education Plus e Standard possono usare il Centro sicurezza, che offre informazioni e dati analitici avanzati sulla sicurezza, nonché ulteriori funzionalità di visibilità e controllo per i problemi di sicurezza che interessano il dominio.

Il Centro sicurezza include lo strumento di indagine sulla sicurezza, che gli amministratori possono usare per identificare, classificare e risolvere problemi relativi a sicurezza e privacy come attacchi phishing, condivisione inappropriata dei file, attività sospetta degli utenti e sui dispositivi e altro ancora.

Google Workspace è la suite di comunicazione e collaborazione cloud-native più sicura al mondo

0

vulnerabilità del software sfruttate attivamente in Workspace dal novembre 2021*

50%

50% di potenziale risparmio sui premi assicurativi delle polizze di sicurezza informatica con l'uso di Workspace

2x inferiore

Il numero degli incidenti di sicurezza registrato dalle organizzazioni che usano Workspace è 2 volte inferiore a quello delle aziende che utilizzano Microsoft 365

2.5x inferiore

Il numero degli incidenti di sicurezza registrato dalle organizzazioni che usano Workspace è 2,5 volte inferiore a quello delle aziende che utilizzano Microsoft Exchange

*Secondo CISA, questo parametro è notevolmente inferiore a quello degli altri fornitori di strumenti per la produttività che operano in questo settore.

Google Chromebooks for Education

I Chromebook sono computer molto sicuri, scalabili e facili da usare per studenti e insegnanti, grazie anche alle funzionalità incorporate e pronte all'uso per la sicurezza. In nessun dispositivo ChromeOS per aziende, scuole o consumatori sono mai stati registrati attacchi ransomware. I Chromebook consentono di proteggere gli istituti scolastici dalle minacce in costante evoluzione attraverso funzionalità sempre nuove e aggiornamenti eseguiti in modo automatico in background, in modo che gli utenti possano rimettersi al lavoro in pochi secondi.

Aggiornamenti automatici di sistema operativo e applicazioni con protezione incorporata contro il malware

Gli utenti malintenzionati tentano sempre di sfruttare bug e punti deboli di sistemi operativi, browser e app molto usate per installare malware e rubare i dati degli utenti. Per proteggere l'istituto e gli utenti, i Chromebook mantengono aggiornati il sistema operativo e le applicazioni grazie agli aggiornamenti automatici incorporati e predefiniti. Inoltre, le applicazioni cloud non richiedono mai aggiornamenti software, come invece accade per quelle installate localmente. Il chip di sicurezza di Google all'interno dei Chromebook consente di salvaguardare i dispositivi, proteggere l'identità degli utenti e garantire l'integrità del sistema.

Nei Chromebook del parco dispositivi vengono installati automaticamente gli aggiornamenti più recenti per proteggere il sistema da malware. Studenti e insegnanti sono protetti dalle minacce informatiche tramite funzionalità di sicurezza integrate come la crittografia dei dati, l'avvio verificato, la limitazione tramite sandbox e gli aggiornamenti automatici.

Proteggere i dati degli utenti

Quando accedi a un Chromebook con il tuo Account Google, tutti i dati sono archiviati in file criptati per fare in modo che nessun altro sul dispositivo possa vederli o accedere alle applicazioni usando il tuo account. In questo modo, gli studenti possono proteggere e condividere molto facilmente i dispositivi all'interno di una classe e le scuole possono ridurre il costo totale delle risorse informatiche. Per funzionalità di sicurezza più avanzate, Chrome Education Upgrade (la licenza per la gestione dei dispositivi) offre una maggiore visibilità.

Criteri di sicurezza dei dispositivi gestiti dagli utenti da remoto

Gli amministratori scolastici possono configurare criteri di ChromeOS e installare o aggiornare le applicazioni da remoto utilizzando la Console di amministrazione Google. Con un semplice clic su un pulsante, un singolo amministratore IT può aggiornare immediatamente i criteri e le configurazioni di centinaia di migliaia Chromebook.

In questo modo:

- Gli studenti possono accedere solo ad applicazioni e contenuti approvati dalla scuola
- Tutte le applicazioni e le estensioni vengono aggiornate con le ultime correzioni per la sicurezza
- Gli utenti non possono copiare, trasferire o condividere dati scolastici al di fuori del dispositivo
- È possibile prendere decisioni basate sui dati con consigli personalizzati offerti da Google per far fronte alle minacce alla sicurezza
- È possibile gestire centralmente i criteri per la sicurezza e la gestione di identità e accessi per tutti gli utenti direttamente dalla Console di amministrazione

Ecco alcuni dei criteri principali che gli amministratori farebbero bene a configurare:

Criteri relativi ai dispositivi

- **Modalità ospite**
  Si consiglia di disabilitare la modalità Ospite dei dispositivi in modo che studenti e insegnanti debbano accedere utilizzando le proprie credenziali, invece di usare il dispositivo in modo anonimo.
- **Limitazioni dell'accesso**
  Si potrebbe scegliere di non permettere a studenti e insegnanti di accedere ai Chromebook della scuola usando i propri account Gmail. Applica le limitazioni dell'accesso solo al dominio Workspace per i dispositivi usati esclusivamente dagli studenti.
- **Report sui dispositivi e sugli utenti**
  Gli amministratori farebbero bene ad attivare i report su dispositivi e utenti per raccogliere metriche sulla frequenza di utilizzo dei Chromebook, su chi li usa e sulla condizione dell'hardware.
- **Nuova registrazione forzata**
  È fondamentale che un Chromebook di proprietà di una scuola rimanga al suo interno, a meno che un amministratore non ne esegua il deprovisioning. Gli amministratori farebbero bene ad abilitare la nuova registrazione forzata dei Chromebook qualora dovessero essere cancellati o in caso di tentativo di furto.

Criteri relativi agli utenti

- **Modalità di navigazione in incognito**
  Gli studenti dovrebbero avere a disposizione tutti gli strumenti per lavorare bene quando usano i Chromebook scolastici. Ciò include l'uso esclusivo del browser autenticato, in modo che i filtri dei contenuti web possano escludere la visualizzazione di siti web inappropriati. Gli amministratori dovrebbero disabilitare la modalità di navigazione in incognito per evitare che gli studenti eludano i filtri web.
- **Modalità proxy**
  Shebbene alcune scuole possano usare i proxy per filtrare i contenuti del web, è importante impedire agli utenti di modificare autonomamente le impostazioni proxy.
- **Livello di accesso simultaneo dell'account**
  Se gli utenti sono autorizzati ad accedere a un account secondario mentre usano i Chromebook della scuola e gli account Workspace, potrebbero effettuare acilmente l'esfiltrazione di dati sensibili degli utenti o della scuola in un account secondario. Gli amministratori farebbero bene a bloccare il livello di accesso simultaneo dell'account.
- **Cronologia del browser**
  Potrebbe essere utile impedire agli studenti di cancellare la propria cronologia del browser. Se si dovesse verificare un incidente di sicurezza su internet, i log della cronologia potrebbero essere utili durante l'indagine.

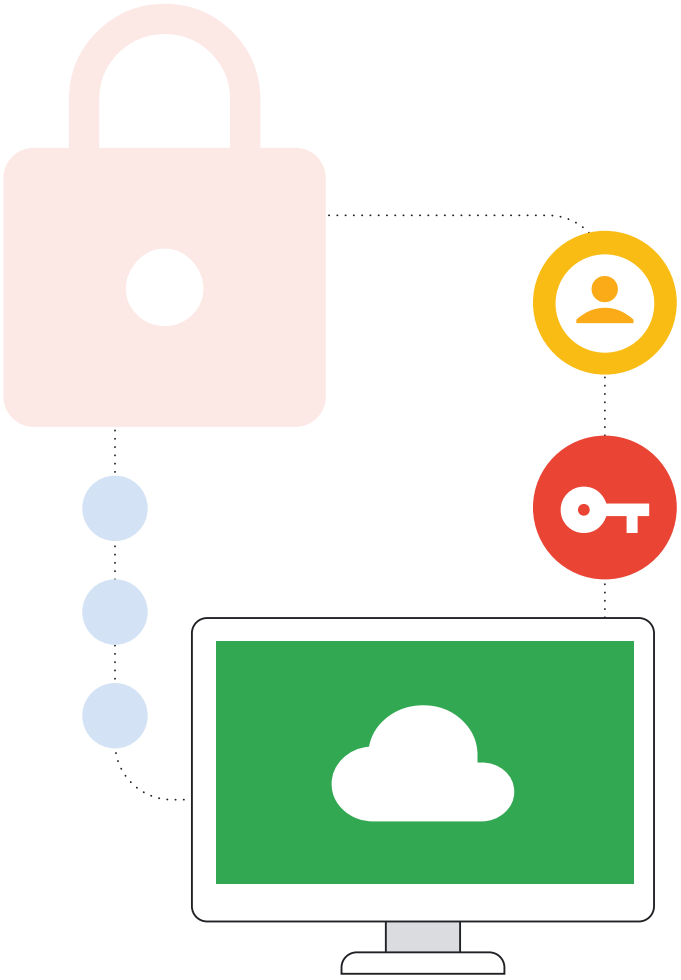
Questo elenco è un buon punto di partenza per garantire che le reti siano protette dagli errori più comuni che potrebbero portare a gravi incidenti informatici. Altri criteri consigliati per la sicurezza sono disponibili nel nostro elenco di controllo per la sicurezza.

Gestione degli endpoint per l'uso sicuro sempre e ovunque

La gestione remota dei criteri di ChromeOS consente agli amministratori IT delle scuole di applicare impostazioni di sicurezza ed eseguire strumenti per la protezione come i sistemi di filtro dei contenuti sul dispositivo, invece che sui server della rete della scuola. In questo modo, gli studenti che usano i Chromebook hanno gli stessi vantaggi in termini di sicurezza sia a casa che in classe. Questo aspetto è sempre più importante man mano che le scuole passano ai libri di testo digitali e agli strumenti didattici online, con la conseguente necessità da parte degli studenti di portare a casa i computer per fare i compiti.

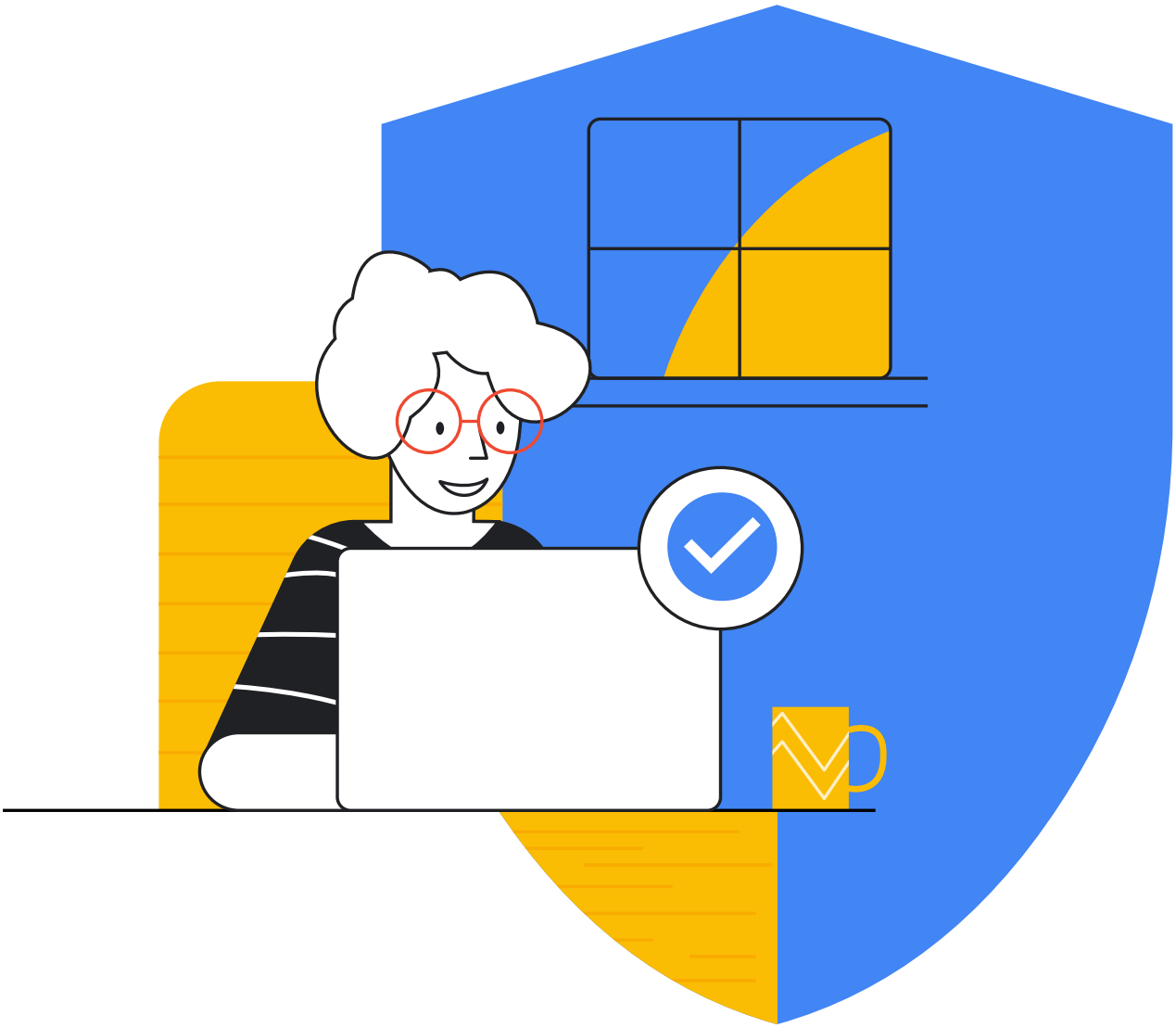
Conclusione

I problemi legati alla protezione degli istituti di istruzione primaria e secondaria da incidenti informatici sono complessi, ma vale la pena investire per salvaguardare l'istituto, gli studenti, gli insegnanti, il personale non docente e, più in generale, l'intero ecosistema online. Gli argomenti trattati in questo documento sono un buon punto di partenza, ma ogni scuola deve adeguare i consigli alle proprie esigenze specifiche e stare al passo con le tecnologie emergenti, controllando al contempo il panorama delle minacce in continua evoluzione. Questo è un documento di base molto efficace per qualsiasi programma di sicurezza per l'istruzione primaria e secondaria, nonché una risorsa utile per eventuali ulteriori interventi da attuare. Google dispone inoltre di una serie di risorse, corsi di formazione e professionisti esperti nel campo della cybersicurezza per aiutare le scuole e le organizzazioni a seguire i consigli di questa guida e ad approfondire la conoscenza di tecnologie emergenti come l'IA. I prodotti di Google sono realizzati su misura per il settore dell'istruzione e forniscono soluzioni di uso immediato per molte delle insidie legate alla cybersicurezza e descritte in questo documento. Siamo felici di collaborare con gli istituti per aiutarli a progettare e implementare i programmi relativi alla sicurezza.



Elenco delle risorse

- Google. “Strumenti e suggerimenti per la sicurezza online.” Centro per la sicurezza online di Google, https://safety.google/security/security-tips/. Consultato il 6 ottobre 2022.
- NIST. “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.” NIST Technical Series Publications, 16 aprile 2018, https://doi.org/10.6028/NIST.CSWP.04162018. Consultato il 6 ottobre 2022.
- Microsoft. “Microsoft AccountGuard Program.” Microsoft AccountGuard Program, https://www.microsoftaccountguard.com/en-us/. Consultato il 6 ottobre 2022.
- Google. “Programma di protezione avanzata.” Programma di protezione avanzata Google, https://landing.google.com/advancedprotection. Consultato il 6 ottobre 2022.
- Google. “Centro per la sicurezza online di Google.” Centro per la sicurezza online di Google - Maggiore sicurezza online, https://safety.google. Consultato il 6 ottobre 2022.
- Meta. “Nozioni di base di Meta: protezione dell’account.” Protezione dell’account, https://www.facebook.com/gpa/resources/basics/security. Consultato il 6 ottobre 2022.
- Meta. “Protezione di Facebook.” Facebook, https://www.facebook.com/gpa/facebook-protect. Consultato il 6 ottobre 2022.
- 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. Consultato il 6 ottobre 2022.
- Passkey: https://developers.google.com/identity/passkeys
- Report CISA “Protecting Our Future” sulla cybersicurezza per l’istruzione primaria e secondaria https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- Report GAO https://www.gao.gov/products/gao-20-644
- Per ulteriori informazioni su come Google for Education consente di proteggere gli istituti, consulta il Centro sicurezza e privacy di Google for Education.
- Report Zcaler sul phishing



Google for Education