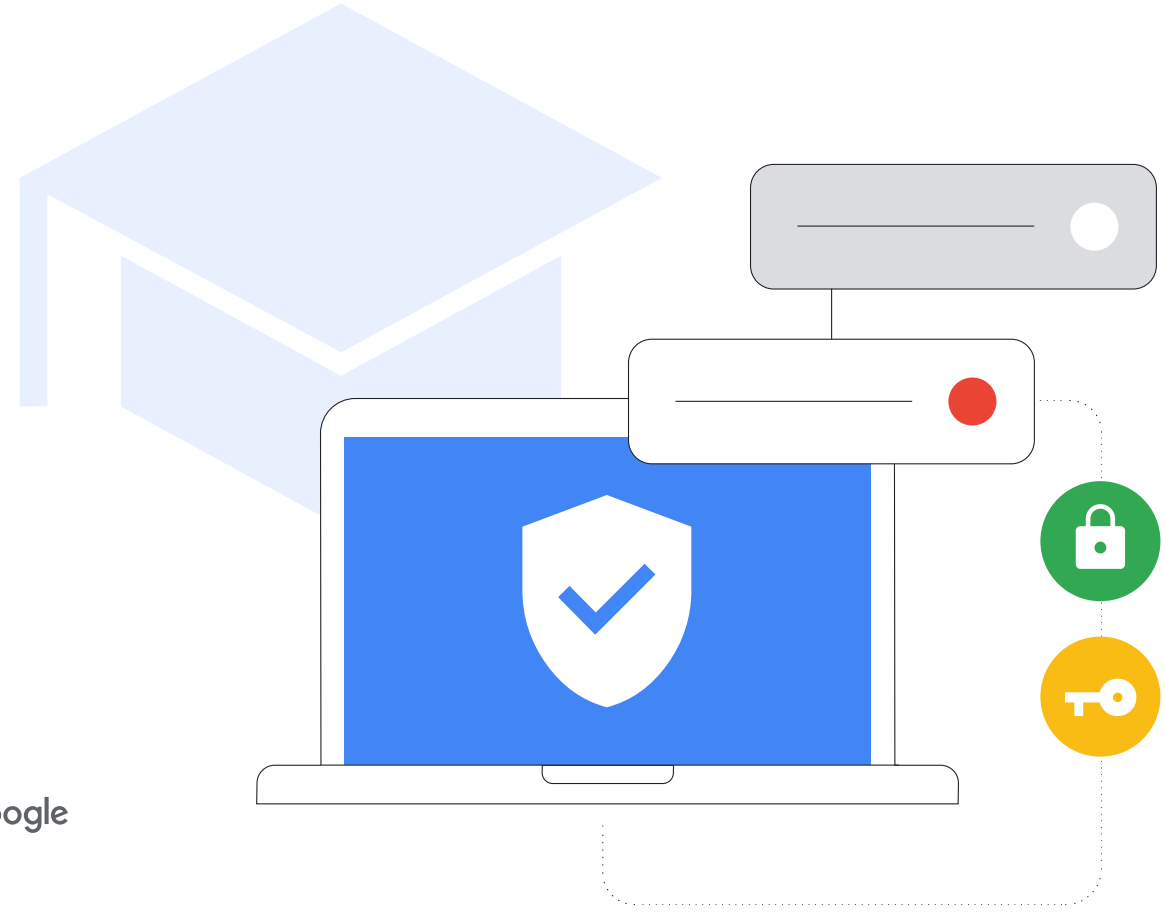
Google for Education

Guide sur la cybersécurité dans l'enseignement primaire et secondaire

Mise à jour août 2023



Safer with Google

Synthèse

Comme le souligne le rapport *Protecting Our Future*[1] de la CISA (l'Agence de cybersécurité et de sécurité des infrastructures aux États-Unis), il est essentiel que les établissements d'enseignement primaire et secondaire investissent dans la cybersécurité pour protéger les élèves, leurs familles, les enseignants, le personnel et les communautés scolaires. Ce document fournit des conseils et des bonnes pratiques permettant aux administrateurs informatiques de ces établissements d'installer et de configurer le matériel et les logiciels de façon à renforcer la cybersécurité. Il inclut des bonnes pratiques générales, ainsi que des conseils spécifiques aux produits et services Google. La mission de Google, qui vise à organiser les informations à l'échelle mondiale pour les rendre accessibles et utiles à tous, constitue un aspect essentiel des efforts déployés par l'équipe Google for Education, à savoir créer des outils conçus pour l'enseignement et l'apprentissage. Ce guide dresse un bilan de ce travail.

Les bonnes pratiques de sécurité sont présentées par thème afin que vous puissiez explorer plus en détail les processus de configuration et d'installation ainsi que les stratégies d'atténuation des risques. Nous expliquons par ailleurs comment Google aborde la cybersécurité pour ses services, en particulier pour ses outils pédagogiques. Ce document fournit des conseils détaillés sans faire référence à des produits ni à des services. Toutefois, nous sommes convaincus que nos produits offrent une protection supérieure contre les attaques courantes dès la première utilisation

Les risques

Les établissements d'enseignement sont des cibles privilégiées des cyberattaques, car les acteurs mal intentionnés cherchent à exploiter les environnements scolaires riches en données pour leur propre compte. 46% des établissements scolaires qui n'ont pas encore été ciblés pensent qu'ils le seront un jour, car les attaques de rançongiciels sont de plus en plus sophistiquées et difficiles à arrêter. Selon 42 % d'entre eux, les rançongiciels sont tellement répandus qu'une attaque est tout simplement inévitable. La nécessité pour les établissements scolaires de passer rapidement à l'enseignement à distance en 2020 a fortement contribué à accroître les failles de cybersécurité, ce qui les a rendus vulnérables aux attaques.

Les moyens de défense

Il est possible de lutter contre ces attaques. Bien qu'aucune technologie n'élimine complètement les menaces, le secteur éducatif et les fournisseurs EdTech peuvent collaborer pour adopter et implémenter des bonnes pratiques visant à créer une approche sécurisée et complète qui réduit considérablement les risques. En mettant en place les dispositions et règles appropriées pour protéger les utilisateurs, sécuriser les appareils et assurer la confidentialité des données, les établissements d'enseignement peuvent mieux gérer les risques et limiter les attaques.

Principales recommandations

- **UTILISEZ L'AUTHENTIFICATION SÉCURISÉE** pour protéger les informations sensibles, les e-mails, les fichiers et d'autres contenus, ainsi que pour empêcher les utilisateurs non autorisés d'accéder aux systèmes éducatifs. Dans la mesure du possible, suivez les bonnes pratiques pour l'authentification des utilisateurs, à savoir les mots de passe sécurisés, la validation en deux étapes, les clés d'accès et les gestionnaires de mots de passe, en particulier pour les administrateurs informatiques et le personnel qui traite des informations sensibles.
- **APPLIQUEZ DES PARAMÈTRES DE SÉCURITÉ APPROPRIÉS** pour protéger vos utilisateurs, vos données et votre environnement. Même si les produits Google sont sécurisés par défaut, il est essentiel que les administrateurs utilisent et configurent correctement les réseaux et les systèmes pour assurer la sécurité. Pour protéger les établissements scolaires, il convient d'appliquer les principes de zéro confiance et de moindre privilège. En effet, les utilisateurs ne doivent avoir accès qu'aux logiciels, données, applications et systèmes dont ils ont besoin pour travailler efficacement.
- **METTEZ À JOUR ET À NIVEAU VOS SYSTÈMES** pour vous assurer que les utilisateurs sont protégés contre les dernières menaces. Utilisez des systèmes d'exploitation (OS) et des navigateurs récents. Veillez également à ce que les utilisateurs bénéficient des dernières versions logicielles sur tous les appareils (ou de versions stables à long terme et approuvées) et que les mises à jour s'effectuent automatiquement. Le passage à une solution plus sûre, telle que les Chromebooks, peut renforcer la sécurité. Aucun rançongiciel n'a jamais été détecté sur un appareil ChromeOS.
- **TILISEZ DES SYSTÈMES D'ALERTE ET DE SURVEILLANCE EN TEMPS RÉEL** pour renforcer votre stratégie de sécurité et limiter rapidement les problèmes potentiels. Vous pouvez exploiter ces fonctionnalités intégrées à votre logiciel principal de collaboration et de communication, tel que Google Workspace for Education, ou déployer des solutions distinctes pour la journalisation et la surveillance de la sécurité. Assurez un suivi complet des activités liées au réseau, aux appareils, aux applications, aux utilisateurs et aux données de votre établissement. Surveillez les connexions aux comptes, le partage de fichiers, le volume des e-mails (en particulier, les tentatives d'hameçonnage et d'attaque de logiciels malveillants), l'activité des appareils et les changements de configuration. Mettez à jour votre solution d'alerte et de surveillance afin de recevoir des notifications sur les menaces, les événements critiques et les modifications des systèmes.
- **APPRENEZ AUX ENSEIGNANTS, AU PERSONNEL ET AUX ÉLÈVES** à utiliser les appareils et les logiciels de façon sécurisée, à reconnaître et signaler les menaces potentielles ainsi qu'à partager les données de manière appropriée afin de lutter contre certaines des attaques les plus courantes. Les établissements ou les secteurs scolaires peuvent créer des documents de formation personnalisés et utiliser en parallèle des supports prêts à l'emploi en libre accès de façon à créer un kit d'outils complet.

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.

Recommandations destinées spécifiquement aux utilisateurs des produits Google: des produits Google comme Google Workspace for Education et les Chromebooks peuvent renforcer la cybersécurité de votre établissement et faciliter l'application de chacune de ces recommandations. Ensemble, ils forment une solution complète permettant de protéger la confidentialité des données des utilisateurs et offrant à votre établissement un niveau de sécurité optimal.

Ces stratégies, ainsi que les conseils supplémentaires fournis ci-après, constituent une excellente base pour assurer la sécurité des établissements d'enseignement primaire et secondaire.

Approche de Google concernant l'enseignement

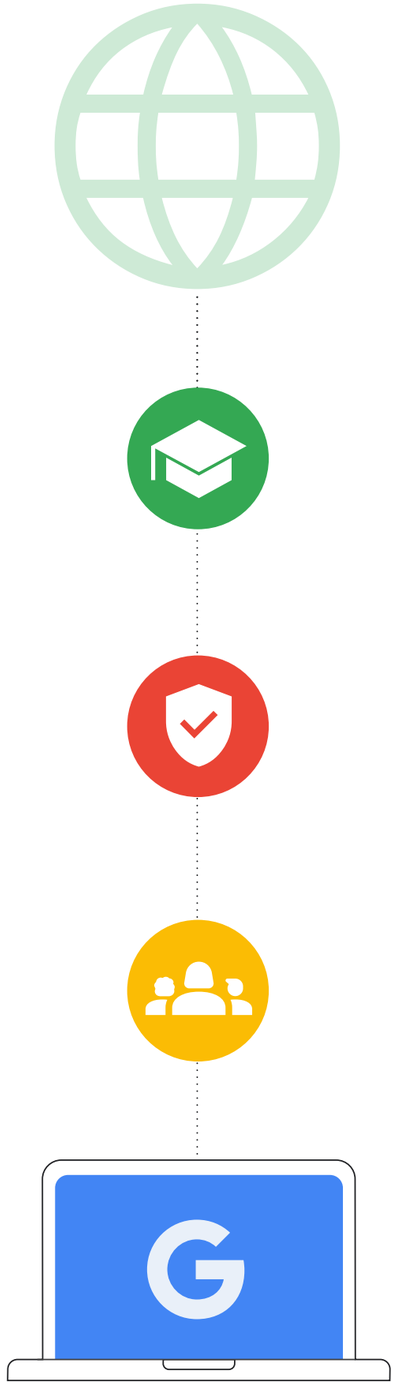
La mission de Google vise à organiser les informations à l'échelle mondiale pour les rendre accessibles et utiles à tous, et il en va de même dans le secteur éducatif. Pour ce faire, l'équipe Google for Education conçoit des produits tels que les Chromebooks et Google Classroom, qui permettent aux élèves et aux enseignants de créer, de partager et d'organiser leurs propres contenus, de même que d'accéder à des ressources pédagogiques ou des outils en ligne et de les exploiter, le tout de façon simple et sécurisée.

Les établissements scolaires méritent d'avoir accès à des technologies qui sont sécurisées par défaut, bénéficient d'une conception axée sur la confidentialité, permettent de garder le contrôle, et proposent des contenus et des informations fiables. Avec des produits tels que les Chromebooks et Google Workspace for Education, ils profitent de fonctionnalités de sécurité de pointe conformes aux normes éducatives mondiales les plus strictes. En outre, les administrateurs informatiques disposent d'une visibilité totale sur leurs données et leurs règles de sécurité tout en ayant la possibilité de les contrôler facilement. Les élèves peuvent participer pleinement à l'apprentissage dans un environnement numérique plus sûr qui propose des contenus adaptés à leur âge, et qui limite les spams et les cybermenaces.

Nous avons privilégié les fonctionnalités et contrôles de sécurité intégrés, les normes de confidentialité les plus strictes et les options permettant d'obtenir des outils de sécurité plus proactifs afin de sécuriser l'apprentissage pour tous. Les appareils ChromeOS contribuent à atténuer les menaces auxquelles font face les établissements scolaires. Ils constituent la meilleure défense contre les rançongiciels, qui représentent pour eux le plus grand danger. En effet, aucune attaque de rançongiciel visant les Chromebooks n'a jamais abouti.

Dans le même temps, Google Workspace for Education se positionne comme l'une des suites de communication et de collaboration basées dans le cloud les plus populaires et les plus sécurisées au monde. Pour en savoir plus sur la façon dont chaque produit protège la cybersécurité conformément aux recommandations présentées ici, veuillez consulter la dernière section.

Le présent document est divisé en deux sections : la première porte sur les conseils de sécurité pratiques et généraux destinés aux établissements d'enseignement primaire et secondaire, quels que soient les produits, tandis que la seconde concerne les conseils de configuration spécifiquement destinés aux établissements utilisant les produits Google for Education, tels que Google Workspace for Education et les Chromebooks. Ces deux sections fournissent des informations qui vous aideront à protéger votre établissement et vos élèves en ligne.



Introduction

Les établissements d'enseignement primaire et secondaire sont exposés à un risque élevé de cyberattaques, tant via leurs appareils que via leur réseau. Il est essentiel que ces établissements utilisent les meilleurs mécanismes de sécurité possibles pour protéger les élèves et empêcher les pertes de données, de services, de ressources, de temps ou d'argent qui peuvent résulter de ces attaques. (Source)

Ce guide est un outil destiné à promouvoir les bonnes pratiques de cybersécurité que les directeurs d'établissement et les systèmes scolaires peuvent appliquer afin de mieux sécuriser leur environnement. En adoptant ces bonnes pratiques, les établissements d'enseignement primaire et secondaire peuvent limiter, voire empêcher, les cyberattaques graves et coûteuses visant les systèmes éducatifs, de même que protéger les élèves, leurs familles, les enseignants et le personnel.

Les cyberattaques ciblant les établissements scolaires sont de plus en plus fréquentes et graves. Selon le K-12 Cybersecurity Resource Center, plus de 1 300 cyberincidents impliquant des établissements d'enseignement des 50 états aux États-Unis ont été rendus publics entre 2016 et 2021. Les responsables éducatifs doivent aujourd'hui protéger les données et les informations personnelles de leurs élèves, de leurs enseignants et de leurs équipes, ainsi que les systèmes et les informations de leur établissement. La tâche est d'autant plus complexe que l'enseignement a toujours eu plus de mal que d'autres secteurs à suivre le rythme d'évolution de la cybersécurité.

Les cyberattaques avérées (rançongiciels, hameçonnage, logiciels malveillants ou autres) peuvent engendrer des violations, à grande échelle, des informations permettant d'identifier personnellement les utilisateurs, des paiements coûteux (le montant moyen des rançons a été multiplié par cinq depuis 2020 pour atteindre 812 260 $) ainsi que des interruptions prolongées de l'enseignement et d'autres activités au sein des établissements. Récemment, une attaque de rançongiciel a arrêté tout un système scolaire. Les élèves n'ayant pas pu assister aux cours pendant plusieurs jours, l'événement a eu des répercussions sur l'ensemble de la communauté. Les établissements d'enseignement primaire et secondaire, qui disposent de ressources et de financements limités, demeureront des cibles de choix s'ils n'investissent pas pour renforcer la cybersécurité.

La communication, la collaboration et les partenariats restent les meilleurs moyens de renforcer la cybersécurité. Ce document a été élaboré à partir de sources de pratiques de cybersécurité largement reconnues, à savoir les conseils de sécurité de Google, le framework de cybersécurité du National Institute for Standards and Technology (NIST), ainsi que les outils et recommandations proposés par la CISA en 2023 concernant la cybersécurité dans l'enseignement primaire et secondaire. Il évoque les mesures générales que les administrateurs informatiques doivent prendre ou envisager, certaines des bonnes pratiques et directives de Google concernant ses produits, de même que des conseils et services de sécurité proposés par d'autres entreprises. Les administrateurs doivent examiner tous les conseils de sécurité fournis par les entreprises pertinentes et appliquer les directives les plus récentes. En effet, l'entreprise responsable est la mieux à même de décrire ses produits et les modifications qui ont pu être apportées.

Avant d'appliquer les recommandations présentées ci-après, tenez compte des facteurs suivant:

Remarques

1. **Protection de votre population scolaire.** Les besoins de chaque établissement varient, et des mesures supplémentaires peuvent être nécessaires pour assurer la sécurité et la confidentialité de certaines populations. De nombreux outils EdTech sont dotés de fonctionnalités qui facilitent l'accès basé sur l'âge, par exemple en limitant les contenus inappropriés ou en veillant à ce que les données de localisation et de contact restent confidentielles.
2. **Types de données que vous stockez.** Si vous stockez des données sensibles, vous pouvez les chiffrer ou les conserver dans un endroit distinct.
3. **Types d'appareils et de modèle de déploiement que vous utilisez.** Les appareils et les applications qu'ils exécutent doivent faire l'objet de mises à jour automatiques permettant de maximiser la sécurité, de chiffrer les données et d'isoler les comptes de sorte que les utilisateurs n'aient accès qu'à leurs propres informations.
4. **Règles appliquées par votre établissement scolaire, votre secteur ou votre région.** Votre établissement peut avoir établi des règles spécifiques concernant l'utilisation de la technologie. Vous devrez veiller à mettre en place toutes les mesures de protection conformément à ces règles.

Chaque jour
100 millions
de tentatives d'hameçonnage sont contrées par Gmail.

Chaque semaine
300,000
sites Web non sécurisés sont identifiés par Google.

Chaque jour
74 millions
de personnes utilisent le Gestionnaire de mots de passe Google.

Chaque année
700 millions
de personnes renforcent leur stratégie de sécurité grâce au Check-up Sécurité.

Conseils de sécurité généraux

Utiliser l'authentification sécurisée

L'authentification sécurisée doit être une priorité absolue pour les établissements scolaires et les autres organismes éducatifs. Au quatrième trimestre 2022, les comptes sans identifiant ou dotés d'un mot de passe peu sécurisé représentaient 48 % de tous les facteurs de compromission lors des piratages. L'application de certaines recommandations clés peut permettre de vérifier que les utilisateurs sont bien ceux qu'ils prétendent être et de limiter leur accès aux informations en fonction de leur rôle respectif.

Les administrateurs informatiques doivent imposer l'utilisation de la validation en deux étapes (également appelée "authentification à deux facteurs" ou "A2F"), et passer à l'authentification sans mot de passe (par exemple, via des clés d'accès) dans la mesure du possible, en particulier lorsque quelqu'un accède à distance aux systèmes d'un établissement d'enseignement. La validation en deux étapes ajoute un niveau de sécurité à vos comptes en ligne de sorte que les pirates informatiques aient plus de mal à y accéder.

Les établissements scolaires actuels utilisent de nombreux types d'appareils et modèles de déploiement. Par ailleurs, les aptitudes techniques sont inégales dans l'enseignement primaire et secondaire. Conformément aux bonnes pratiques définies, la sécurité des comptes et des appareils varie selon les rôles et les types d'utilisateurs : les administrateurs informatiques, les enseignants et le personnel, les élèves plus âgés qui utilisent des appareils attribués et les élèves plus jeunes qui utilisent des appareils partagés. Des recommandations propres à chaque groupe sont présentées ci-dessous.

Plusieurs types de méthodes d'authentification sont recommandés dans la plupart des cas:

- **Mots de passe sécurisés:**
  Invitez les utilisateurs à créer leur propre mot de passe lors de la première connexion, et définissez des exigences techniques minimales à respecter en termes de longueur et de complexité. Les phrases secrètes plus longues et utilisant des caractères complexes renforcent la sécurité. Les utilisateurs ne doivent pas être obligés de changer régulièrement de mot de passe, car cette pratique les encourage à utiliser des mots de passe plus simples ou à effectuer des modifications non pertinentes (comme le remplacement d'un seul caractère).
- **Validation en deux étapes:**
  Cette fonctionnalité protège les comptes au moyen d'une deuxième étape que l'utilisateur exécute généralement avec un élément en sa possession, comme une clé de sécurité ou une application de téléphone mobile qui crée un code de validation unique. Bien que toutes les formes de validation en deux étapes renforcent la sécurité des comptes, les administrateurs doivent éviter d'utiliser des codes de validation communiqués par message ou par téléphone, car ils peuvent être piratés.
- **Authentification sans mot de passe:**
  Les clés d'accès offrent une alternative aux mots de passe, à la fois plus sécurisée et plus simple. Les utilisateurs peuvent se connecter à des applications et des sites Web en saisissant un code, en dessinant un schéma, en se servant d'un capteur biométrique (empreintes digitales ou reconnaissance faciale, par exemple) ou en appuyant sur une clé de sécurité, ce qui leur évite d'avoir à mémoriser et à gérer des mots de passe. Même si ces méthodes ne conviennent pas à tous les contextes éducatifs, elles remplacent de plus en plus les modes d'authentification traditionnels, et permettent des connexions plus sûres et plus rapides. Les clés d'accès protègent les utilisateurs contre les attaques par hameçonnage, car elles ne fonctionnent que pour les applications et les sites Web enregistrés.
- **Authentification unique (SSO):**
  L'authentification unique permet aux utilisateurs d'accéder à plusieurs applications et sites Web à l'aide d'un même ensemble d'identifiants. Étant donné qu'ils n'ont à mémoriser qu'une seule série d'identifiants, ils ont moins tendance à noter ces informations. En outre, les établissements scolaires n'ayant pas à gérer plusieurs ensembles d'identifiants utilisateur, ils peuvent réduire les frais liés à l'assistance informatique et au centre d'assistance. Google Workspace for Education est compatible avec l'authentification unique en mode natif. Ainsi, les utilisateurs peuvent se connecter à des applications tierces à l'aide des identifiants de leur compte Google. Ils peuvent également utiliser les identifiants d'un autre fournisseur pour se connecter à leur compte Google.
- **Gestionnaires de mots de passe:**
  Les gestionnaires de mots de passe peuvent aider les utilisateurs à créer des mots de passe sécurisés et uniques pour tous les comptes et services dont ils se servent en classe et au travail (lorsque l'authentification unique n'est pas utilisée). Ils ne permettent pas de se connecter au système d'exploitation d'un appareil, mais peuvent gérer les mots de passe une fois que l'utilisateur est connecté. Les utilisateurs Google peuvent se servir du Gestionnaire de mots de passe dans Chrome sur n'importe quelle plate-forme, y compris ChromeOS et Android.

Les différents groupes ayant des besoins spécifiques, ils bénéficieront de combinaisons ou de sous-ensembles personnalisés de ces approches d'authentification, en fonction de leur rôle dans les établissements d'enseignement, du type de systèmes et de données auxquels ils ont accès, et de leur âge.

Administrateurs des établissements scolaires

Les administrateurs contrôlent les systèmes et une grande partie des données des établissements d'enseignement primaire et secondaire. La protection de leurs comptes est essentielle pour la sécurité de l'ensemble du système, de l'infrastructure aux données des comptes en passant par les appareils gérés par les établissements. Par conséquent, ils doivent adopter les normes d'authentification les plus élevées en utilisant, par exemple, des mots de passe sécurisés, un gestionnaire de mots de passe fiable et la validation en deux étapes. Chacun de ces procédés ajoute une couche de protection. Lorsqu'ils sont utilisés ensemble, ils offrent un niveau de sécurité maximal pour les comptes administrateur et les services d'entreprise.

- Les administrateurs doivent utiliser une clé de sécurité physique ou une méthode de validation en deux étapes cryptographiques sécurisée qui requiert un appareil vérifié et des invites. Il peut s'agir d'un service tel que Google Authenticator ou d'une autre application qui crée des codes de validation uniques. Les Chromebooks commercialisés après 2019 avec une puce TPM contiennent un bouton Marche/Arrêt qui peut être utilisé pour l'authentification à deux facteurs.
- Les administrateurs doivent utiliser un gestionnaire de mots de passe de confiance compatible avec la validation en deux étapes pour stocker leurs mots de passe d'accès à différents services.

Enseignants et personnel utilisant des appareils attribués

Comme les administrateurs, les enseignants et le personnel ont accès à des données sensibles. Toutefois, ils ne contrôlent pas l'infrastructure numérique et disposent de compétences techniques plus inégales.

- Lorsque la loi l'autorise, les enseignants et le personnel utilisant des Chromebooks doivent pouvoir s'identifier à l'aide d'une méthode de validation biométrique, comme les empreintes digitales.
- Les administrateurs doivent imposer l'utilisation de la validation en deux étapes et passer à l'authentification sans mot de passe dans la mesure du possible et chaque fois qu'un membre du personnel accède à distance aux systèmes d'un établissement d'enseignement.

Élèves plus âgés utilisant des appareils attribués (classe de CM1 et au-delà, en général)

Les élèves plus âgés sont mieux informés sur la manière de se protéger et sont généralement capables d'utiliser des mécanismes d'authentification plus sûrs, ce qui est en accord avec les types de services qu'ils sont susceptibles d'employer. Ils ne doivent avoir accès qu'à leur propre compte et aux informations qui leur ont été communiquées.

- Afin d'accélérer la procédure de connexion sur les appareils, les élèves utilisant des Chromebooks doivent pouvoir créer un code propre à chaque appareil. Les options biométriques peuvent ne pas être appropriées ou utilisables dans de nombreux environnements scolaires.
- Il convient d'aider chaque élève à créer un mot de passe unique ne contenant pas d'informations personnelles (telles que le nom, la classe ou la date d'anniversaire). Il faut également leur expliquer que l'utilisation de phrases secrètes peut complexifier les mots de passe tout en les rendant plus faciles à mémoriser.

Jeunes élèves utilisant des appareils partagés (classes de la maternelle au CE2, en général)

Étant donné que les élèves les plus jeunes ne maîtrisent pas encore les technologies éducatives, une méthode d'authentification simple et adaptée à des données et services limités leur sera utile.

- ÉLes établissements scolaires qui utilisent des alternatives aux mots de passe proposées par des fournisseurs tiers (comme les codes QR ou les connexions par image) pour leurs plus jeunes élèves et ceux qui ne peuvent pas se connecter avec des mots de passe doivent prendre des mesures de sécurité, car ces méthodes sont moins sûres. En cas de perte ou de divulgation d'un code, les administrateurs doivent modifier le mot de passe de l'élève concerné et mettre à jour le code.
- Les établissements scolaires doivent faire comprendre aux élèves et aux parents qu'il est important de garder les mots de passe secrets et de stocker de façon sécurisée les identifiants alternatifs tels que les codes QR.
- Pour les appareils attribués tels que les tablettes, une autre méthode d'authentification sécurisée peut consister à utiliser un code propre à chaque appareil.

Appliquer des paramètres de sécurité appropriés

ALes appareils et les réseaux des établissements scolaires constituent une cible à haute visibilité et de grande valeur pour les pirates informatiques du monde entier. Il est donc essentiel de mettre en place les meilleurs mécanismes de sécurité possibles pour éviter toute perte de services, de ressources, de temps et d'argent. Les administrateurs système doivent implémenter les fonctionnalités de sécurité efficaces et appropriées que proposent les produits utilisés par leur établissement tout en veillant à ce que ces systèmes restent simples d'utilisation pour les enseignants, le personnel et les élèves. Les paramètres de sécurité et de confidentialité importants doivent être configurés de sorte que des utilisateurs individuels ne puissent pas les désactiver ni les modifier. Les autres paramètres doivent assurer une protection efficace en étant définis sur des valeurs par défaut par l'administrateur. Il est essentiel de mettre en place les meilleurs mécanismes de sécurité possibles pour éviter toute perte de services, de ressources, de temps et d'argent. Si vous utilisez des Chromebooks, vous pouvez consulter la dernière section qui fournit des suggestions pour définir des règles relatives aux appareils.

Enfin, intégrez la "minimisation des données" à vos pratiques en limitant les objectifs et les moyens de collecte, d'utilisation et de divulgation des informations personnelles des individus à ce qui est raisonnablement nécessaire et proportionné pour fournir un service ou à ce qui est compatible avec le contexte de la relation.

Applications et mises à jour

Limitez les applications que vos utilisateurs peuvent installer, car chaque application présente sur un appareil représente un vecteur d'attaque potentiel à exploiter. Si possible, utilisez des applications provenant de sources de confiance. Par exemple, invitez les utilisateurs à vérifier la présence du badge de validation sur le Google Play Store afin de s'assurer qu'ils téléchargent les applications officielles qui ont fait l'objet d'un examen de sécurité. Toute modification du système d'exploitation ou du matériel ("jailbreaking" ou "rooting") engendre des failles de sécurité importantes et doit être évitée.

Accès et visibilité

Les administrateurs doivent veiller à ce que les utilisateurs n'aient accès qu'aux données, logiciels, services et systèmes dont ils ont besoin pour accomplir leurs tâches ou apprendre efficacement. Cela permet de limiter les accès indésirables et de savoir qui a accès à telle ou telle ressource. Accordez une attention particulière aux données très sensibles (comme les informations permettant d'identifier personnellement les utilisateurs) et aux systèmes (RH, paie, notation, sécurité et configuration, par exemple) en vérifiant quels utilisateurs peuvent accéder aux données et dans quelles circonstances, en limitant l'accès aux appareils appartenant aux établissements scolaires et en veillant à ce que seuls certains membres du personnel disposent de droits d'accès.

Examinez les règles de partage des données définies dans les outils de collaboration afin d'empêcher tout partage inapproprié ou excessif, et tout accès non autorisé. Limitez ou bloquez le partage en dehors de votre environnement (en particulier pour les élèves) et mettez en place des règles permettant de surveiller le partage des contenus sensibles.

Perte ou vol d'appareils

La perte d'un appareil n'entraîne pas nécessairement une perte de données. Les administrateurs doivent établir un plan standard pour assurer l'accès aux informations et aux documents en cas de perte ou de vol d'un appareil, par exemple en conservant les documents dans un environnement cloud. Téléchargez et imprimez des codes de secours pour vos processus de validation en deux étapes afin d'éviter toute interruption des accès aux comptes.

Lorsqu'un appareil est déclaré comme perdu ou volé, veillez à le verrouiller à distance si possible. Assurez-vous également que les comptes associés sont verrouillés ou signalés afin qu'ils ne soient pas utilisés pour obtenir un accès non autorisé. En cas de perte d'un Chromebook, vous pouvez effacer ses données. Par ailleurs, vous pouvez surveiller les comptes Google Workspace for Education à la recherche d'activités suspectes ou les suspendre (verrouiller) si nécessaire.

Protection avancée pour les utilisateurs à haut risque

Google propose le Programme Protection Avancée (PPA) aux utilisateurs qui possèdent des informations hautement visibles et sensibles (y compris aux administrateurs Google Workspace for Education). Ce programme offre aux utilisateurs une protection supplémentaire contre les attaques ciblées, telles que les tentatives d'hameçonnage, les téléchargements dangereux et les piratages de mots de passe. Spécialement conçu pour contrecarrer les attaques en ligne ciblant des comptes Google, il utilise automatiquement une authentification forte et des clés de sécurité. Par ailleurs, il restreint l'accès des tiers aux données des comptes. D'autres fournisseurs de comptes en ligne proposent également des protections efficaces pour les comptes des utilisateurs à haut risque. Les administrateurs et le personnel doivent les utiliser systématiquement s'ils ont accès à des informations personnelles ou à des systèmes technologiques.

Mettre à jour et à niveau vos systèmes

Pour se protéger, l'une des mesures les plus importantes qu'il convient de prendre consiste à maintenir à jour le système d'exploitation et les applications des appareils. C'est encore plus essentiel pour les établissements d'enseignement primaire et secondaire, car ils jouent un rôle primordial dans l'éducation et la vie quotidienne des enfants. La plupart des attaques de logiciels malveillants survenant dans les environnements éducatifs et dans d'autres contextes à haut risque sont basées sur Windows. C'est le cas, entre autres, de la faille SolarWinds, des attaques de rançongiciels ciblant les districts scolaires Los Angeles Unified School District et Albuquerque School District, du piratage du Little Rock School District, de la violation de données visant Microsoft Exchange Server ainsi que de la brèche de sécurité des systèmes Microsoft ayant récemment affecté des agences fédérales. Là aussi, l'utilisation de produits et services cloud devrait faciliter la tâche des administrateurs en leur permettant de réduire la surface d'attaque, ainsi que de mettre à jour automatiquement leurs systèmes et leurs applications.

Passer à un système d'exploitation récent et le maintenir à jour

La version la plus récente d'un système d'exploitation (OS) comporte généralement de nouvelles fonctionnalités de sécurité permettant de lutter contre les vecteurs d'attaque connus. Vous devez activer la fonctionnalité de mise à jour automatique dans le système d'exploitation de l'appareil. Si les mises à jour automatiques sont impossibles, il convient de télécharger et d'installer les correctifs et les mises à jour d'un fournisseur de confiance au moins une fois par mois.

Les Chromebooks fonctionnent sous ChromeOS. Par conséquent, ils bénéficient de mises à jour fréquentes et automatiques incluant les derniers correctifs de sécurité, ce qui permet d'adopter rapidement les innovations les plus récentes. Par ailleurs, ils vérifient l'intégrité du système d'exploitation en lecture seule avant le démarrage. Ils chiffrent toutes les données stockées sur l'appareil afin de les protéger contre tout accès non autorisé, et exécutent chaque page Web et chaque application dans un bac à sable séparé. Ainsi, si une application ou un site Web sont infectés par un logiciel malveillant, les autres parties de l'appareil ne seront pas affectées.

Si votre établissement n'est pas prêt à passer aux Chromebooks, sachez que ChromeOS Flex est une version de ChromeOS conçue pour moderniser vos appareils. Ce système d'exploitation offre à chacun une expérience d'enseignement et d'apprentissage unifiée et moderne, avec des mécanismes de sécurité proactifs intégrés et des fonctionnalités de gestion basées dans le cloud. ChomeOS Flex permet d'automatiser la protection ainsi que de bloquer les applications et les fichiers exécutables malveillants sans remplacer le matériel existant.

Passer à un navigateur récent et le maintenir à jour

Il est important de s'assurer que les navigateurs sont également mis à jour et sécurisés. Les navigateurs récents offrent des fonctionnalités de sécurité avancées. Ils peuvent inviter les utilisateurs à les activer facilement ou être configurés par les administrateurs afin d'activer par défaut ces fonctionnalités sur les ordinateurs des établissements scolaires. Cela contribue à protéger la confidentialité des informations sensibles qui circulent sur Internet. Les navigateurs doivent être maintenus à jour. Que ce soit pour le travail, l'apprentissage ou d'autres activités en ligne, un navigateur récent et à jour offre les avantages suivants:

- **Il utilise des mécanismes de sécurité fiables**,, tels que l'isolation de sites et la navigation sécurisée, pour empêcher les utilisateurs d'accéder accidentellement à des sites Web dangereux.
- **Vous pouvez activer les mises à jour automatiques** afin de vous assurer que le navigateur intègre les mises à jour de sécurité dès qu'elles sont disponibles.
- **La connexion est sécurisée**, car les navigateurs récents doivent utiliser le protocole Transport Layer Security. Les utilisateurs peuvent cliquer à côté d'une URL pour vérifier que la connexion est marquée comme sécurisée.

Chrome intègre la sécurité dès sa conception et offre des fonctionnalités telles que la navigation sécurisée, qui est activée par défaut. Un gestionnaire de mots de passe intégré est également disponible. Vous pouvez saisir automatiquement les mots de passe lorsque vous naviguez sur le Web, ce qui vous permet d'utiliser facilement des mots de passe sécurisés.

Utiliser des systèmes d'alerte et de surveillance en temps réel

Les systèmes d'alerte et de surveillance en temps réel peuvent aider les établissements scolaires à identifier les menaces et y répondre rapidement, avant qu'elles ne causent des dommages. Il est important de s'assurer que les outils de sécurité s'exécutent en arrière-plan afin de collecter et d'enregistrer les événements liés à la sécurité sur l'ensemble de vos systèmes. Les outils d'IA sont particulièrement efficaces pour parcourir de grandes quantités de données collectées et pour identifier des anomalies ou des modèles. Cela permet de détecter plus rapidement et plus facilement les menaces, puis de traiter et de corriger les failles. Les activités devant être examinées par l'administrateur ou le personnel informatique peuvent ainsi être priorisées.

Les établissements scolaires peuvent utiliser les fonctionnalités d'alerte et de surveillance intégrées à leur logiciel principal de collaboration et de communication, tel que Google Workspace for Education, ou déployer des solutions SIEM (Security Information and Event Management) distinctes.

Les systèmes d'alerte et de surveillance en temps réel peuvent suivre diverses activités liées au réseau, aux appareils, aux applications, aux utilisateurs et aux données d'un établissement scolaire. Il peut s'agir, par exemple, des connexions des utilisateurs, des accès aux fichiers, des intrusions potentielles, des vols (ou tentatives de vols) de données ou des activités des administrateurs.

Si le système détecte une activité suspecte, il peut envoyer une alerte au personnel informatique de l'établissement. Cela permet aux administrateurs d'examiner le problème et de prendre des mesures pour atténuer la menace.

En outre, les outils d'alerte et de surveillance permettent de mieux cerner les menaces auxquelles les établissements scolaires sont confrontés. En analysant les données de ces systèmes en temps réel, les établissements peuvent identifier des tendances et des modèles afin de mieux se protéger.

.

Voici quelques bonnes pratiques à suivre pour utiliser des systèmes d'alerte et de surveillance (y compris des solutions SIEM):

1. **Définir vos objectifs de sécurité**
   Identifiez les informations et les systèmes les plus importants pour l'établissement scolaire, ainsi que les types de menaces qui lui font courir le plus grand risque. Ensuite, déterminez les données que vous devez recueillir pour surveiller ces menaces.

2. **Collecter les données adéquates et effectuer une configuration appropriée**
   Il est important de collecter les données adéquates et de configurer les applications afin d'atteindre les objectifs de sécurité les plus pertinents. Il peut s'agir de données provenant de pare-feu, de filtres de contenu, de systèmes de détection des intrusions, de serveurs Web et d'autres dispositifs de sécurité, ainsi que de logiciels de communication et de collaboration, de systèmes d'information sur la scolarité et de systèmes de gestion de l'apprentissage.

3. **Examiner et gérer les alertes**
   Lorsque votre système de surveillance génère une alerte, il est important d'examiner le problème et de prendre les mesures appropriées. Vous pouvez, par exemple, réunir plusieurs équipes pour enquêter sur la source de l'alerte, déterminer s'il s'agit d'un faux positif ou prendre des mesures pour atténuer la menace (comme suspendre les comptes, réinitialiser les mots de passe des utilisateurs, placer en quarantaine ou supprimer les e-mails, modifier les autorisations de fichiers ou effacer les données des appareils).

Former les enseignants, le personnel et les élèves

Les établissements d'enseignement primaire et secondaire doivent attirer l'attention des communautés scolaires sur la sécurité et améliorer leurs pratiques dans ce domaine à l'aide de campagnes et de partenariats qui contribuent à responsabiliser les utilisateurs. Il est essentiel de sensibiliser les enseignants, le personnel et les élèves à l'importance de la sécurité pour les aider à se protéger en ligne et à éviter les menaces de cybersécurité les plus graves. Apprenez-leur à utiliser les produits et services dont dispose votre établissement, à repérer et signaler les menaces telles que les e-mails d'hameçonnage et, surtout, à prendre des mesures pour empêcher ces attaques. Les établissements et les secteurs scolaires doivent attirer l'attention des communautés scolaires sur la sécurité et améliorer leurs pratiques dans ce domaine à l'aide de campagnes et de partenariats qui contribuent à responsabiliser les utilisateurs.

Apprendre à utiliser les appareils et les logiciels de façon sécurisée

Les administrateurs peuvent collaborer avec des enseignants et des experts pour élaborer des programmes de cybersécurité adaptés à l'âge qui aident les élèves à utiliser les appareils, les logiciels et les systèmes de façon sécurisée. La création de documents de formation propres à votre établissement ou à votre secteur vous aide à contextualiser les recommandations pour vos enseignants et vos élèves. Mais vous pouvez également exploiter les contenus prêts à l'emploi disponibles, entre autres, dans Les Super-héros du Net, sur la page safety.google ou sur la plate-forme Khan Academy, et les adapter à vos besoins. Ces programmes peuvent aider vos utilisateurs à se protéger, qu'ils se trouvent en classe ou dans leur communauté.

Identifier les menaces

Former les enseignants, le personnel et les élèves à reconnaître les menaces est essentiel pour assurer leur sécurité. Il est important d'apprendre aux enfants à identifier les menaces, car ils ne savent peut-être pas déterminer si une activité est légitime. Ils doivent pouvoir reconnaître certains types de menaces et savoir comment les signaler. De leur côté, les administrateurs doivent se concentrer sur les sujets qui, selon eux, génèrent le meilleur retour sur investissement. Autre point important : la formation doit apprendre aux utilisateurs non seulement à identifier les menaces, mais également à intervenir. Les menaces courantes que les utilisateurs doivent reconnaître incluent les rançongiciels, l'hameçonnage, l'ingénierie sociale, les logiciels malveillants et les escroqueries. Toutefois, si certaines menaces sont plus répandues dans un établissement donné, il convient de s'assurer que la communauté scolaire en est informée.

Sécuriser le partage de données et de fichiers

Les enseignants et le personnel doivent apprendre à partager correctement les fichiers et les données de même qu'à identifier les demandes inappropriées reçues par e-mail. Ils doivent impérativement veiller à ce que les informations personnelles sensibles ne soient partagées ou traitées que si cela est nécessaire et avec des niveaux de protection supplémentaires. Ainsi, il convient de ne jamais partager de telles données par e-mail ou avec des tiers. Des fonctionnalités de protection contre la perte de données (incluses dans ChromeOS et Workspace for Education) doivent être utilisées pour avertir les utilisateurs finaux et les empêcher de partager des fichiers contenant des données sensibles (comme les numéros de sécurité sociale), ou de copier et coller des contenus sensibles en dehors du domaine.

L’approche de Google en action : appareils et services pour l’enseignement

Pour un secteur scolaire, l’acquisition de logiciels est l’un des meilleurs moyens de se protéger. Les logiciels doivent bénéficier d’une architecture et d’une conception robustes afin de limiter les risques de failles et d’intégrer la sécurité à tous les niveaux. En exigeant que les établissements scolaires achètent des logiciels sécurisés ou des logiciels d’entreprises ayant fait leurs preuves dans le domaine de la sécurité, il est possible de réduire considérablement les risques liés à la cybersécurité au sens large. Ainsi, Google a renforcé ChromeOS tout en continuant à déployer des solutions plus proactives et intelligentes qui exploitent son expertise dans le domaine du machine learning, du cloud et de l’identité.

Google s’engage à créer des produits capables de protéger la confidentialité des élèves et des enseignants, et offrant une sécurité optimale pour votre établissement. Vous pouvez vous fier aux produits et services Google for Education pour assurer la protection des utilisateurs, des appareils et des données contre des menaces toujours plus complexes. Cette section présente aux administrateurs informatiques des établissements scolaires les recommandations sur la sécurité qu’ils doivent suivre lorsqu’ils utilisent les produits Google for Education.

Google Workspace for Education

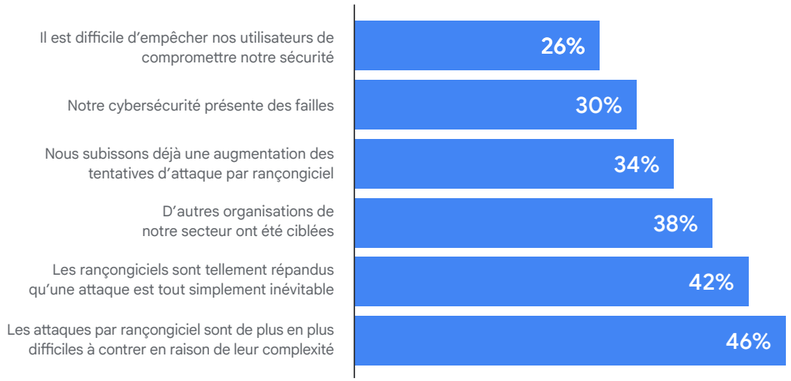
Google Workspace for Education est un ensemble d’outils et de services Google conçus spécialement pour les établissements scolaires. Il permet de collaborer, de simplifier l’enseignement et d’assurer la sécurité de l’environnement d’apprentissage. Les produits et services Google for Education assurent la protection des utilisateurs, des appareils et des données contre des menaces toujours plus complexes. En outre, ils fournissent des outils tels que les centres d’alerte et de sécurité, Vault pour l’eDiscovery, Identity and Access Management et la fonctionnalité Protection contre la perte de données.

Nous avons regroupé des documents utiles pour ceux qui font leurs premiers pas avec Google Workspace for Education. Nombre d’entre eux peuvent vous aider à vous organiser conformément aux recommandations de cette section. Si vous avez besoin d’aide pour commencer à utiliser Google Workspace for Education, consultez ce guide de démarrage rapide pour la configuration informatique.

Checklists de sécurité

Examinez les checklists de sécurité pour savoir comment renforcer la sécurité et la confidentialité des données de votre établissement. Les établissements scolaires disposant des éditions Google Workspace for Education Standard et Plus peuvent également utiliser la page État de sécurité pour surveiller la configuration des paramètres de la console d’administration. Par exemple, vous pouvez vérifier l’état de paramètres tels que le transfert automatique des e-mails, le chiffrement des appareils, les paramètres de partage de Drive, entre autres. Vous pouvez, si nécessaire, configurer les paramètres de votre domaine en fonction des consignes générales de sécurité et des bonnes pratiques en vigueur, tout en tenant compte des besoins de votre organisation et de sa stratégie de gestion des risques.

Pourquoi le secteur éducatif s’attend à être ciblé par des attaques



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

Vous trouverez ci-dessous d’autres conseils vous permettant d’exploiter au mieux les protections intégrées à Google Workspace for Education.

Configure unidades organizacionais (UOs)

Il est indiscutable que tous les membres de votre compte Google Workspace for Education doivent disposer des mêmes paramètres. Les unités organisationnelles sont des groupes d’utilisateurs qui vous permettent d’attribuer des autorisations, services et paramètres distincts à différents utilisateurs. Vous pouvez, par exemple, utiliser la validation en deux étapes pour les enseignants et le personnel, et l’authentification adaptée à l’âge pour les jeunes élèves. Configurez des unités organisationnelles distinctes pour le personnel, les enseignants et les élèves afin d’appliquer des règles distinctes à chaque groupe d’utilisateurs. Une structure bien conçue est essentielle pour que vous puissiez gérer votre compte Google Workspace for Education de manière efficace et flexible.

Configurer des règles de mots de passe et des protections de comptes administrateur

Comme nous l’avons expliqué, l’authentification des utilisateurs est essentielle à la sécurité de votre établissement. C’est pourquoi nous avons mis en place des méthodes flexibles de gestion de l’authentification pour les administrateurs. Vous pouvez ainsi vous assurer que les utilisateurs disposent de protections de compte appropriées et sûres. Définissez des règles de mots de passe pour veiller à ce que les utilisateurs créent des mots de passe sécurisés. Le cas échéant, exigez l’utilisation de la validation en deux étapes en fonction des groupes recommandés dans la section “Utiliser l’authentification sécurisée”. Vous pouvez imposer la validation en deux étapes à un sous-ensemble d’utilisateurs (en leur laissant le temps de la configurer) et déployer cette fonctionnalité en suivant différentes méthodes. Il peut s’agir, par exemple, de clés de sécurité (technique la plus sûre), d’une invite Google (applications Google sur Android et iOS), de générateurs de codes de validation (comme Google Authenticator), ou bien de messages ou d’appels téléphoniques (technique la moins sûre).

Si votre organisation utilise un fournisseur d’identité (IdP) autre que Google, vous pouvez configurer l’authentification unique (SSO) via un fournisseur d’identité tiers. Si vous préférez, vous pouvez également utiliser la validation en deux étapes avec l’authentification unique pour les comptes autres que super-administrateur.

Activer ou désactiver des services

Dans la console d’administration Google, les administrateurs peuvent déterminer les services Google auxquels les utilisateurs ont accès avec leur compte Google Workspace for Education. Vous pouvez contrôler l’accès aux services Google, comme Agenda, Drive et Meet, en les activant ou les désactivant par unité organisationnelle (UO). Il est également possible d’activer les services lorsque vous utilisez des groupes. Vous pouvez aussi examiner les différences entre les services Workspace principaux et supplémentaires avant d’activer des services supplémentaires comme YouTube, Google Maps et Blogger. Nous invitons les administrateurs à définir l’accès aux services Google en fonction de l’âge. Ils doivent garder à l’esprit que des restrictions d’accès à certains services Google s’appliquent automatiquement aux utilisateurs désignés comme ayant moins de 18 ans lorsqu’ils sont connectés à leur compte Google Workspace for Education.

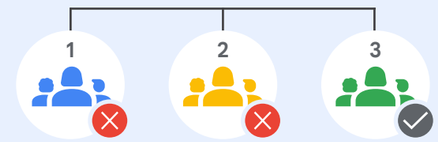
Par ailleurs, l’accès contextuel (disponible dans les éditions Workspace for Education Standard et Plus) vous permet d’autoriser ou de bloquer l’accès aux applications Google telles que Gmail, Drive et Agenda en fonction de l’adresse IP, de l’origine géographique, des règles de sécurité ou du système d’exploitation d’un appareil. Vous pouvez, par exemple, autoriser Drive pour ordinateur uniquement sur les appareils appartenant à l’entreprise dans des pays/régions spécifiques.

Méthodes pour accorder aux utilisateurs l’accès aux services

Dans la console d’administration Google, vous pouvez désactiver l’accès d’une unité organisationnelle à un service Google tel que Google Drive. Si certains utilisateurs de cette unité organisationnelle ont besoin d’utiliser Drive, vous avez deux possibilités:

1. Déplacer ces utilisateurs vers une unité organisationnelle pour laquelle Drive est activé.
2. Ajouter ces utilisateurs à un groupe d’accès et activer Drive pour le groupe. Tous les membres pourront accéder au service, même s’il n’est pas activé dans leur unité organisationnelle.

Unités organisationnelles



Google Drive est désactivé pour les unités organisationnelles 1 et 2.

Dans un groupe d’accès

Mais un **groupe d’utilisateurs** au sein des unités organisationnelles 1 et 2 peut utiliser Google Drive.

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

Définir des règles de partage des données et de conservation

En tant qu'administrateur, vous pouvez décider si les utilisateurs peuvent partager des fichiers et des dossiers Google Drive avec des personnes extérieures à votre organisation. Cela peut aider à éviter le partage involontaire ou bien trop large de données et de fichiers, et à empêcher les fuites de données. Il est essentiel de séparer les fichiers et les Drive, de créer des unités organisationnelles et d'appliquer le principe du moindre privilège pour empêcher les pirates informatiques de passer d'un réseau à l'autre s'ils s'introduisent dans un compte. Plus l'accès d'un pirate potentiel aux données et au réseau est restreint, moins il peut causer de dommages.

Désactivez le partage de fichiers externe pour les élèves (ou limitez-le exclusivement aux domaines autorisés) et définissez la fonctionnalité Vérificateur d'accès sur "Destinataires uniquement". Si vous autorisez tous les utilisateurs ou certains d'entre eux à partager des fichiers en dehors de votre domaine, activez l'affichage d'un avertissement lorsque cela se produit. En outre, désactivez la publication de fichiers sur le Web et exigez que les collaborateurs externes se connectent à l'aide d'un compte Google.

Par ailleurs, les clients Google Workspace for Education Standard et Plus peuvent utiliser les audiences cibles et les règles de confiance pour définir des recommandations et des restrictions de partage plus précises. Par exemple, les audiences cibles vous permettent de définir l'audience par défaut des enseignants de sorte qu'ils puissent partager des liens exclusivement avec les autres enseignants et le personnel, et non avec tous les membres de votre établissement. Avec les règles de confiance, vous pouvez empêcher les élèves du primaire de partager des fichiers avec des élèves plus âgés.

Pour vous assurer que seuls les utilisateurs appropriés peuvent créer des Drive partagés et empêcher les utilisateurs externes d'y accéder, examinez les règles applicables à ces Drive. Il est préférable de n'autoriser que les administrateurs (ou le personnel et les enseignants) à créer des Drive partagés et de gérer l'accès aux Drive partagés de façon stricte.

Si possible, restreignez la visibilité dans l'annuaire et le partage des contacts. Vous pouvez désactiver le partage des contacts pour tous les utilisateurs ou certains d'entre eux, ou bien créer des annuaires personnalisés pour limiter les utilisateurs visibles par telle ou telle personne.

Configurez des règles de protection contre la perte de données dans Drive et Gmail afin de détecter et de bloquer les informations sensibles. Les règles prédéfinies permettent de protéger les informations sensibles courantes (comme les numéros de cartes bancaires ou de crédit). Vous pouvez également créer des règles personnalisées basées sur des mots clés, des listes de mots et des expressions régulières.

Gérer les paramètres Gmail

Gmail est l'un des principaux services Google Workspace for Education. Il offre aux administrateurs de nombreux paramètres pour protéger leur établissement et leurs utilisateurs.

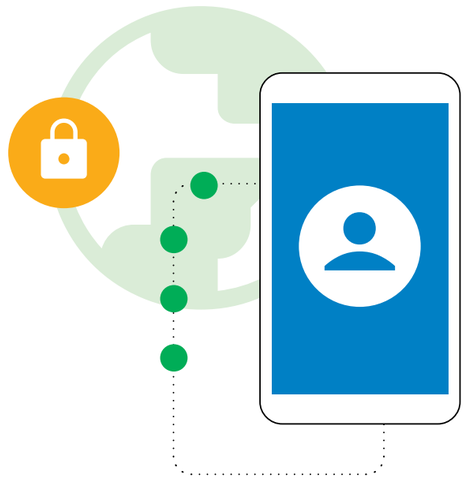
Grâce à l'authentification Gmail, empêchez le spam, le spoofing et l'hameçonnage. Personnalisez les paramètres de filtre antispam. Vous pouvez, par exemple, exiger l'authentification de l'expéditeur pour tous les expéditeurs approuvés et désactiver le contournement de ces filtres pour les expéditeurs internes

Désactivez les accès POP/IMAP dans la mesure du possible et activez l'analyse améliorée des messages avant distribution ainsi que la protection avancée contre l'hameçonnage et les logiciels malveillants. Si vous autorisez l'envoi d'e-mails externes à tous les utilisateurs ou à certains d'entre eux, vous pouvez activer les avertissements de destinataire externe.

Les clients Google Workspace for Education Standard et Plus peuvent également se protéger contre les logiciels malveillants et les rançongiciels en configurant des règles de détection des pièces jointes dangereuses à l'aide du bac à sable de sécurité.

Applications tierces

Utilisez les workflows intégrés pour approuver les applications tierces qui accèdent aux données des comptes via des API. Cela aide à empêcher le partage non autorisé de données avec des applications tierces non approuvées pour un usage scolaire.



Rapports et suivi

En tant qu'administrateur, vous pouvez afficher des rapports et des événements de journaux dans la console d'administration Google pour examiner l'activité de votre organisation (comme les risques de sécurité potentiels), savoir qui se connecte et quand, et comprendre comment les utilisateurs créent et partagent des contenus. Vous pouvez afficher des données au niveau du domaine, ainsi que des informations plus précises à l'aide de graphiques et de tableaux. Consultez les rapports et les journaux d'audit (y compris dans le Centre d'alerte) pour identifier les risques de sécurité, analyser l'utilisation des services, diagnostiquer les problèmes de configuration, suivre l'activité des utilisateurs et plus encore.

Les administrateurs Google Workspace for Education Standard et Plus peuvent utiliser le tableau de bord de sécurité pour afficher un aperçu des différents rapports de sécurité, identifier les tendances et comparer les données actuelles à celles de l'historique (par exemple, concernant le partage de fichiers dans Drive, le spam, l'hameçonnage et les logiciels malveillants dans Gmail, les connexions suspectes à des comptes utilisateur et les activités douteuses sur les appareils). La plupart des journaux d'utilisation, d'activité et d'audit (y compris les événements des journaux d'administration, Drive, Meet et Chat) ainsi que les rapports de sécurité sont disponibles pendant six mois.

Utiliser le centre de sécurité

Les administrateurs Google Workspace for Education Plus et Standard peuvent utiliser le Centre de sécurité, qui fournit des informations et des données analytiques avancées concernant la sécurité, ainsi qu'une visibilité et un contrôle accrus sur les problèmes de sécurité affectant votre domaine.

Le centre de sécurité inclut l'outil d'investigation de sécurité, qui peut aider les administrateurs à identifier les problèmes de sécurité et de confidentialité, à les trier et à prendre les mesures adéquates. Il peut s'agir d'attaques par hameçonnage, de partages de fichiers inappropriés, d'activités suspectes des utilisateurs et des appareils, et plus encore.

Google Workspace est la suite cloud native de collaboration et de communication la plus sécurisée au monde

0

faille logicielle activement exploitée sur Workspace depuis novembre 2021*

50%

d'économies potentielles sur les primes d'assurance liées à la cybersécurité grâce à l'utilisation de Workspace

2x moins

d'incidents de sécurité dans les organisations qui utilisent Workspace plutôt que Microsoft 365

2.5x moins

d'incidents de sécurité dans les organisations qui utilisent Workspace plutôt que Microsoft Exchange

* D'après la CISA, ce chiffre est bien inférieur à celui des autres fournisseurs d'outils de productivité dans ce domaine.

Google Chromebooks for Education

Destinés aux élèves et aux enseignants, les Chromebooks sont des ordinateurs hautement sécurisés, évolutifs et faciles à utiliser grâce à leurs fonctionnalités de sécurité intégrées et prêtes à l'emploi. Aucune attaque de rançongiciel n'a jamais été signalée sur un appareil ChromeOS appartenant à une entreprise, un établissement scolaire ou un particulier. Grâce à leurs fonctionnalités mises à jour, les Chromebooks protègent les établissements scolaires contre les menaces en constante évolution. Les mises à jour s'exécutent automatiquement en arrière-plan pour que les utilisateurs puissent reprendre leur travail en quelques secondes.

Mises à jour automatiques (système d'exploitation et applications) et protection intégrée contre les logiciels malveillants

Les pirates informatiques tentent constamment d'exploiter les bugs et les failles des systèmes d'exploitation, des navigateurs et des applications populaires pour installer des logiciels malveillants et voler les données des utilisateurs. Pour protéger votre établissement et vos utilisateurs, les Chromebooks mettent à jour votre système d'exploitation et vos applications, car ils sont sécurisés par défaut avec des mises à jour de sécurité. Contrairement aux applications locales, les applications cloud n'ont jamais besoin de mises à jour logicielles. Conçue par Google, la puce de sécurité des Chromebooks aide à sécuriser les appareils, à protéger l'identité des utilisateurs et à assurer l'intégrité du système.

Les Chromebooks de votre parc exécuteront automatiquement les dernières mises à jour de protection contre les logiciels malveillants. Grâce aux fonctionnalités de sécurité intégrées telles que le chiffrement des données, le démarrage validé, le système de bac à sable et les mises à jour automatiques, les élèves et les enseignants sont protégés contre les cybermenaces.

Données utilisateur sécurisées

Lorsque vous vous connectez à un Chromebook avec votre compte Google, toutes vos données sont stockées dans des fichiers chiffrés de sorte qu'aucun autre utilisateur de l'appareil ne puisse les consulter ni se connecter à des applications à l'aide de votre compte. Les élèves d'une classe peuvent ainsi partager des appareils tandis que les établissements scolaires réduisent le coût total de l'infrastructure informatique, le tout de façon très simple et sécurisée. Chrome Education Upgrade, la licence de gestion des appareils, offre des fonctionnalités de sécurité plus avancées et une meilleure visibilité.

Règles de sécurité applicables à distance aux appareils gérés par les utilisateurs

Les directeurs d'établissement peuvent configurer les règles ChromeOS et installer/mettre à jour les applications à distance à l'aide de la console d'administration Google. D'un simple clic, un seul administrateur informatique peut mettre à jour instantanément les règles et les configurations de centaines de milliers de Chromebooks. Vous vous assurez ainsi que:

Isso garante que:

- Les élèves ne peuvent accéder qu'aux applications et contenus approuvés par leur établissement ;
- Toutes les applications et extensions sont mises à jour avec les derniers correctifs de sécurité ;
- Les utilisateurs ne peuvent pas copier, transférer ni partager de données scolaires hors de l'appareil ;
- Vous prenez des décisions basées sur les données en suivant les recommandations de sécurité personnalisées de Google pour gérer les menaces de sécurité ;
- Les règles de sécurité et de gestion de l'authentification et des accès sont gérées de façon centralisée pour tous les utilisateurs, directement dans la console d'administration.

Voici quelques règles notables que les administrateurs peuvent choisir de configurer:

Règles relatives aux appareils

- **Mode Invité**
  Il est recommandé de désactiver le mode Invité de vos appareils de sorte que les élèves et les enseignants soient obligés de se connecter à l'aide de leurs propres identifiants au lieu d'utiliser les appareils de manière anonyme.
- **Restrictions de connexion**
  Vous ne souhaitez peut-être pas que vos élèves et vos enseignants se connectent aux Chromebooks de votre établissement à l'aide de leurs comptes Gmail personnels. Appliquez les restrictions de connexion uniquement à votre domaine Workspace pour les appareils utilisés exclusivement par les élèves.
- **Création de rapports sur les utilisateurs et les appareils**
  Nous recommandons aux administrateurs d'activer la création de rapports sur les utilisateurs et les appareils afin de recueillir des métriques sur la fréquence d'utilisation des Chromebooks, leurs utilisateurs et l'état du matériel.
- **Réenregistrement forcé**
  Il est essentiel que les Chromebooks restent dans l'établissement scolaire auquel ils appartiennent à moins qu'un administrateur ne les déprovisionne. Nous conseillons aux administrateurs d'activer le réenregistrement forcé des Chromebooks afin que les appareils soient systématiquement réenregistrés si leurs données sont effacées ou si quelqu'un tente de les voler.

Règles relatives aux utilisateurs

- **Mode navigation privée**
  Les Chromebooks d'un établissement scolaire doivent être configurés pour garantir la réussite des élèves. Par exemple, les élèves ne doivent avoir accès qu'à leur navigateur authentifié afin que les filtres de contenus Web les tiennent à l'écart des sites Web inappropriés. Les administrateurs doivent désactiver le mode navigation privée de sorte que les élèves ne puissent pas contourner les filtres Web.
- **Mode proxy**
  Certains établissements scolaires utilisent des proxys pour le filtrage Web. Il est toutefois important de désactiver la fonctionnalité permettant à vos utilisateurs de modifier eux-mêmes les paramètres proxy.
- **Accès à la connexion multicompte**
  Si les utilisateurs sont autorisés à se connecter à un compte secondaire lorsqu'ils se servent des Chromebooks et des comptes Workspace de leur établissement scolaire, ils peuvent facilement exfiltrer des données/informations sensibles des élèves ou de l'établissement vers ce compte. Nous recommandons aux administrateurs de bloquer l'accès à la connexion multicompte.
- **Historique du navigateur**
  Il peut être judicieux de désactiver la fonctionnalité permettant aux élèves d'effacer l'historique de leur navigateur. En cas d'incident de sécurité Internet, ces journaux d'historique Internet peuvent s'avérer utiles lors des investigations.

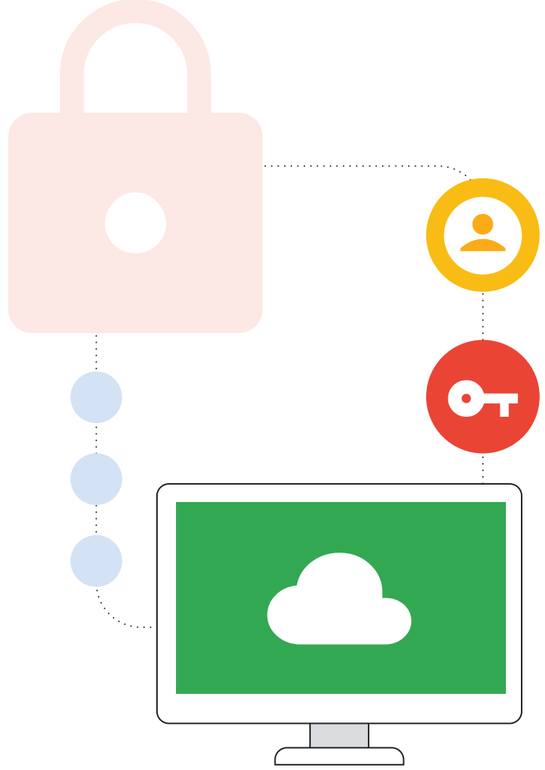
Cette liste est un bon point de départ pour vous assurer que vos réseaux sont protégés contre les types d'erreurs les plus courants qui engendrent des cyberincidents majeurs. Vous trouverez d'autres règles de sécurité recommandées dans notre checklist de sécurité.

Gestion des points de terminaison pour une utilisation sécurisée à tout moment et en tout lieu

Le système de gestion à distance des règles de ChromeOS permet aux administrateurs des établissements scolaires d'appliquer des paramètres de sécurité et d'exécuter des outils de sécurité (tels que des systèmes de filtrage de contenus) sur les appareils plutôt que sur les serveurs de réseau des établissements. Ainsi, les élèves bénéficient des mêmes avantages en termes de sécurité lorsqu'ils utilisent les Chromebooks de l'établissement à la maison et en classe. Ce point est d'autant plus important que les établissements scolaires migrent vers des manuels numériques et des outils d'apprentissage en ligne, et que les élèves doivent emporter les ordinateurs chez eux pour faire leurs devoirs.

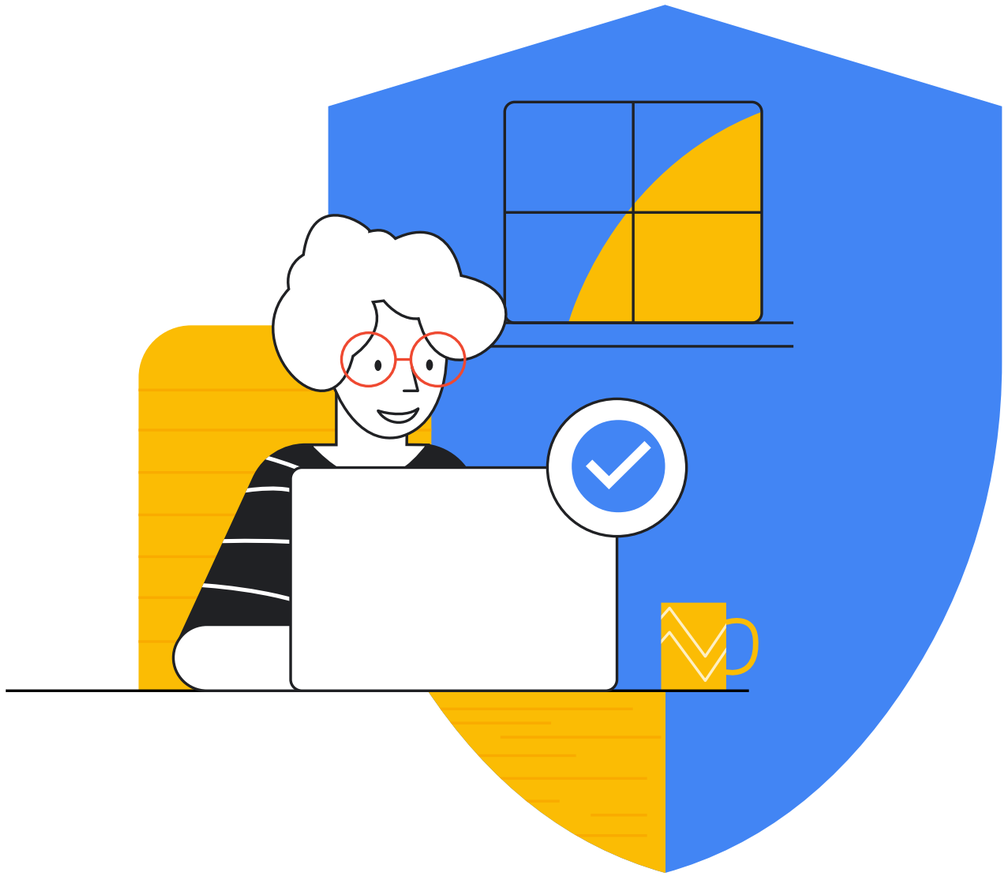
Conclusão

Protéger les établissements d'enseignement primaire et secondaire contre les cyberincidents est un défi complexe. Pourtant, l'investissement à consentir pour assurer votre sécurité ainsi que celle des élèves, des enseignants, du personnel et de l'écosystème en ligne dans son ensemble est réellement payant. Les points abordés dans ce document représentent un bon point de départ. Toutefois, chaque établissement devra adapter les recommandations à ses besoins spécifiques, et continuer à suivre l'évolution des menaces et des technologies émergentes. Cette ressource constitue une base solide pour tout programme de sécurité des établissements d'enseignement primaire et secondaire. Elle fournit des informations sur les éventuelles mesures à prendre et les tâches à accomplir. Google dispose également d'un certain nombre de ressources, de formations et de professionnels qualifiés dans le domaine de la cybersécurité pour aider les établissements scolaires et les organisations à suivre ce guide et à se familiariser avec les technologies émergentes telles que l'IA. Conçus pour l'enseignement, les produits Google apportent des solutions prêtes à l'emploi à de nombreux problèmes de cybersécurité décrits dans le présent document. Nous sommes impatients de vous aider à concevoir et implémenter vos programmes de sécurité.



Liste de ressources

- Google. “Outils et conseils pour assurer votre sécurité en ligne”. Centre de sécurité Google, https://safety.google/security/security-tips/. Date de consultation : 6 octobre 2022.
- NIST. “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1”. NIST Technical Series Publications, 16 avril 2018, https://doi.org/10.6028/NIST.CSWP.04162018. Date de consultation : 6 octobre 2022.
- Microsoft. “Programme Microsoft AccountGuard”. Programme Microsoft AccountGuard, https://www.microsoftaccountguard.com/fr-fr/. Date de consultation : 6 octobre 2022.
- Google. “Programme Protection Avancée”. Programme Protection Avancée de Google, https://landing.google.com/advancedprotection. Date de consultation : 6 octobre 2022.
- Google. “Centre de sécurité Google”. Centre de sécurité Google – Se protéger en ligne, https://safety.google. Date de consultation : 6 octobre 2022.
- Meta. “Notions de base : protéger votre compte”. Protéger votre compte, https://www.facebook.com/gpa/resources/basics/security. Date de consultation : 6 octobre 2022.
- Meta. “Facebook Protect”. Facebook, https://www.facebook.com/gpa/facebook-protect. Date de consultation : 6 octobre 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. Date de consultation : 6 octobre 2022.
- Clés d’accès : https://developers.google.com/identity/passkeys
- Rapport de la CISA “Protecting Our Future : Cybersecurity for K-12” https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- Rapport du GAO https://www.gao.gov/products/gao-20-644
- Pour savoir comment Google for Education peut vous aider à protéger votre établissement scolaire, consultez le Centre de confidentialité et de sécurité Google for Education.
- Rapport de Zcaler sur l'hameçonnage



Google for Education