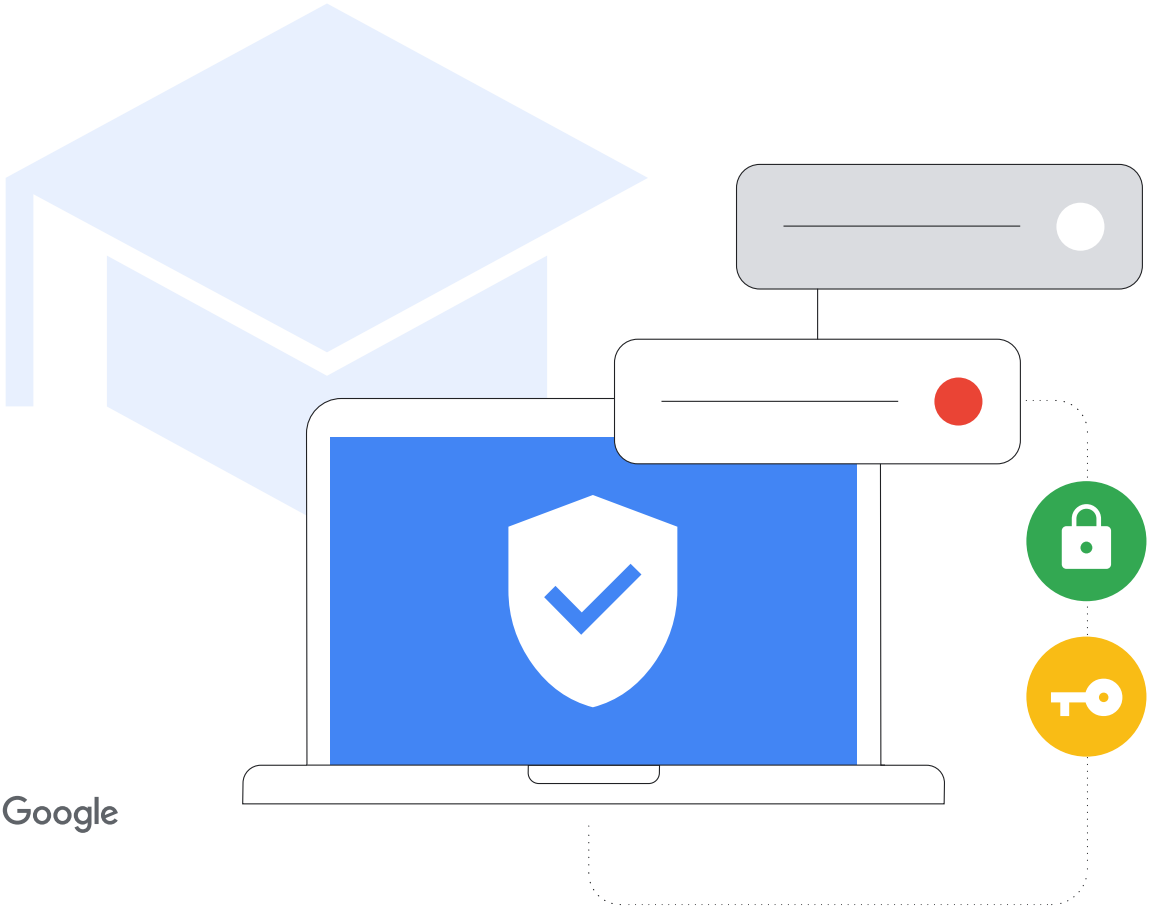
Google for Education

Посібник із кібербезпеки для закладів освіти K-12

Оновлено: серпень 2023



Безпечніше з Google

Короткий зміст

Як зазначено у звіті CISA «На захисті нашого майбутнього», для закладів освіти K-12 критично важливо інвестувати в кібербезпеку, щоб захистити своїх учнів, їхні сім'ї, вчителів, персонал та громади. Цей документ містить рекомендації та передові практики для IT-адміністраторів шкіл щодо налаштування та конфігурації апаратного та програмного забезпечення в закладах освіти K-12 для посилення кібербезпеки. Він включає як загальні передові методи, так і конкретні рекомендації щодо продуктів і сервісів Google. Місія Google щодо організації світової інформації та забезпечення її загально доступною та корисною є ключовим фактором нашої роботи в команді Google for Education: розробки інструментів, призначених для навчання та викладання. У цьому посібнику ми поділимося досвідом цієї роботи.

Ми наводимо найкращі практики безпеки за темами, які дають змогу глибше ознайомитися зі стратегіями конфігурації, налаштування та зменшення ризиків. Ми також пояснюємо, як Google підходить до забезпечення кібербезпеки наших сервісів, особливо інструментів для освіти. Хоча ми надаємо докладні рекомендації в цьому документі незалежно від продукту чи послуги, ми вважаємо, що наші продукти пропонують найкращий захист від поширених атак у нестандартний спосіб.

Ризик

Заклади освіти є головними цілями кібератак, оскільки зловмисники намагаються використати багате на дані середовище шкіл для отримання власної вигоди. 46% шкіл, які ще не зазнали атак, вважають, що зрештою вони будуть атаковані, оскільки програми-вимагачі стають складнішими, і їх все важче зупинити. А 42% з цих шкіл вважають, що програми-вимагачі настільки поширені, що атака просто неминуча. Необхідність швидкого переходу шкіл на дистанційне навчання у 2020 році стала суттєвим чинником для прогалин у кібербезпеці, адже вона зробила школи вразливими до атак.

Захист

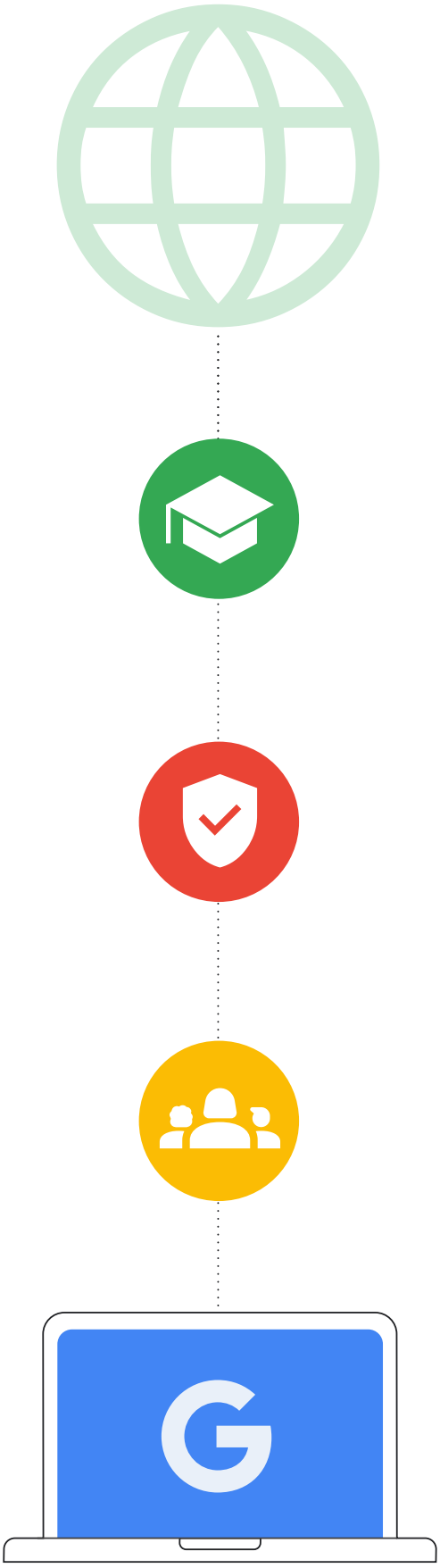
Такі атаки можна пом'якшити. І хоча жодна технологія не усуває ризиків повністю, заклади освіти та постачальники освітніх технологій можуть співпрацювати, щоб приймати та впроваджувати передові методи задля створення безпечного, надійного та комплексного підходу для значного зниження ризиків. Завдяки належним заходам та політикам для захисту користувачів, безпеки пристроїв та забезпечення конфіденційності даних навчальні заклади можуть краще керувати ризиками та пом'якшувати атаки.

Ключові рекомендації:

- **Використовуйте безпечну автентифікацію** для захисту конфіденційної інформації, електронної пошти, файлів та інших матеріалів, а також для запобігання доступу до освітніх систем для неавторизованих користувачів. Застосовуйте передові методи автентифікації користувачів, зокрема надійні паролі та двоетапну автентифікацію (2SV), ключі безпеки та менеджери паролів, де це можливо. Це особливо актуально для IT-адміністраторів та співробітників, які працюють із конфіденційною інформацією.
- **Застосовуйте належні налаштування безпеки** для захисту користувачів, даних та середовища. Хоча продукти Google є захищеними за замовчуванням, для забезпечення безпеки адміністраторам також критично важливо правильно використовувати та налаштовувати мережі та системи. Щоб забезпечити безпеку шкіл, застосовуйте принцип нульової довіри та мінімальних привілеїв: користувачі повинні мати доступ лише до того програмного забезпечення, даних, додатків і систем, що є необхідними для ефективного виконання їхньої роботи.
- **Оновлюйте та модернізуйте ваші системи,** щоб забезпечити захист користувачів від найновіших загроз. Використовуйте сучасні операційні системи (ОС) та вебпереглядачі, а також переконайтеся, що користувачі використовують останні версії програмного забезпечення на всіх пристроях (або схвалені довгострокові стабільні версії), а їхнє оновлення відбувається автоматично. Перехід на безпечніше рішення, як-от Chromebook, може підвищити рівень захисту. На жодному пристрої з ChromeOS ніколи не було виявлено програм-вимагачів.
- **Використовуйте системи сповіщення та моніторингу в режимі реального часу**, щоб підвищити рівень безпеки та швидко усувати потенційні проблеми. Ви можете використовувати ці функції, вбудовані у ваше основне програмне забезпечення для спільної роботи та комунікації, наприклад Google Workspace for Education, або впроваджувати окремі рішення для ведення журналів безпеки та моніторингу. Забезпечте комплексне відстеження активності в мережі вашої школи, на пристроях, у додатках, серед користувачів та даних. Відстежуйте входи до облікових записів, обмін файлами, обсяг електронної пошти (особливо спроби фішингу та атаки шкідливого програмного забезпечення), активність пристроїв та зміни конфігурації. Підтримуйте актуальність вашого рішення для сповіщення та моніторингу, щоб отримувати повідомлення про загрози, критичні події та зміни системи.
- **Навчайте вчителів, персонал та учнів**, як безпечно користуватися пристроями та програмним забезпеченням, розпізнавати потенційні загрози та повідомляти про них, а також обмінюватися даними в належний спосіб, щоб допомогти захиститися від деяких найпоширеніших атак. Школи або райони можуть створювати власні навчальні матеріали, а також використовувати готові матеріали у вільному доступі, що забезпечує комплексний інструментарій для шкіл.

Рекомендації для користувачів продуктів Google
Продукти Google, як-от Google Workspace for Education та пристрої Chromebook, можуть підвищити рівень кібербезпеки вашої школи та полегшити впровадження кожної з цих рекомендацій. Разом вони надають комплексне рішення, що допомагає захистити конфіденційність користувачів і забезпечує найкращий захист для вашого закладу освіти.

Ці стратегії разом із додатковими рекомендаціями, наведеними в цьому документі, формують чудову основу для безпеки закладів освіти K-12.



Підхід Google до освіти

Місія Google полягає в тому, щоб організувати світову інформацію та зробити її загальнодоступною й корисною – це стосується й сектору освіти. У команді Google for Education ми робимо це, створюючи інструменти, такі як пристрої Chromebook та Google Клас, які дозволяють учням і вчителям легко та безпечно створювати, ділитися та організовувати власний контент, а також використовувати та отримувати доступ до освітніх ресурсів й онлайн-інструментів.

Школи заслуговують на технології, які є безпечними за замовчуванням, приватними за своєю суттю, надають змогу контролювати, а також пропонують надійний контент та інформацію. Завдяки таким продуктам, як пристрої Chromebook та Google Workspace for Education, школи отримують найкращий рівень безпеки що відповідає найвищим глобальним освітнім стандартам.
IT-адміністратори отримують повну видимість і легке керування даними та політиками безпеки, а учні можуть повністю зануритися в навчання в безпечному цифровому середовищі, яке пропонує контент відповідно до віку та мінімізує спам і кіберзагрози.

Ми надали пріоритет вбудованим функціям і засобам керування безпекою, найвищим стандартам конфіденційності та можливостям більш проактивних інструментів захисту, щоб забезпечити безпечне навчання для всіх. Пристрої ChromeOS допомагають зменшити загрози для шкіл та є найкращим захистом від найбільшої загрози для шкіл — програм-вимагачів. Адже на пристрої Chromebook ніколи не було здійснено успішної атаки програм-вимагачів.

Тим часом Google Workspace for Education є одним із найпопулярніших і найбезпечніших у світі хмарних пакетів для комунікації та співпраці. Детальнішу інформацію про те, як кожен із цих продуктів забезпечує кібербезпеку відповідно до наведених тут рекомендацій, можна знайти в останньому розділі.

Цей документ складається з двох розділів. Перший розділ містить практичні та загальні рекомендації щодо безпеки для закладів освіти K-12 незалежно від продуктів. Другий розділ пропонує детальні інструкції з налаштування для шкіл, які використовують продукти Google for Education, як-от Google Workspace for Education та пристрої Chromebook. Обидва розділи надають інформацію, аби допомогти вам та вашим учням залишатися в безпеці онлайн.

Вступ

Заклади освіти K-12, їхні пристрої та мережі, мають високий ризик кібератаки. Вкрай важливо, щоб заклади освіти K-12 використовували найкращі засоби безпеки для захисту учнів та запобігання втраті даних, послуг, ресурсів, часу та грошей від цих атак. (Джерело: https://www.gao.gov/products/gao20-644)

Цей посібник є інструментом для просування найкращих практик кібербезпеки для шкільних адміністрацій та систем, які вони можуть впроваджувати для кращого захисту їхнього середовища. Завдяки впровадженню цих практик заклади освіти K-12 можуть зменшити або запобігти серйозним та дороговартісним кібератакам на освітні системи та захистити учнів, їхні сім'ї, вчителів та персонал.

Кібератаки на школи збільшуються за частотою та тяжкістю. За даними Ресурсного центру кібербезпеки K-12 у період із 2016 по 2021 рік відбулося понад 1300 публічно відомих кіберінцидентів у всіх 50 штатах США. Сучасні освітні лідери мають захистити дані та персональну інформацію учнів, вчителів та персоналу, а також системи та інформацію їхніх закладів освіти. Це складне завдання, особливо якщо зважати на те, що освіта традиційно є повільнішою в розвитку кібербезпеки порівняно з іншими секторами.

Успішні кібератаки, включаючи програми-вимагачі, фішинг, шкідливе програмне забезпечення та інші, можуть призвести до масштабних витоків персональних даних (PII), значних виплат (середня сума викупу зросла у 5 разів з 2020 року до $812 260 доларів), а також спричинити тривалі перебої в навчанні та інших шкільних процесах. Нещодавно успішна атака програми-вимагача зупинила роботу цілої шкільної системи, спричинивши хвильові ефекти в усій громаді, оскільки учні не могли відвідувати школу кілька днів поспіль. Зважаючи на обмежені ресурси та фінансування, заклади освіти K-12 надалі залишатимуться першочерговими об'єктами атак, якщо не інвестувати в посилення кібербезпеки.

Кібербезпека завжди забезпечується найкраще через комунікацію, співпрацю та партнерство. Цей документ був створений на основі порад Google щодо безпеки та захисту, Рамки кібербезпеки Національного інституту стандартів і технологій (NIST), а також Інструментарію та рекомендацій з кібербезпеки CISA K-12 2023 року - загальновизнаних джерел із питань кібербезпеки. Цей документ визначає загальні кроки, які IT-адміністратори мають зробити або розглянути, деякі з найкращих практик Google та рекомендації для наших продуктів, а також посилання на поради та послуги з безпеки, пропоновані іншими компаніями. Адміністратори повинні переглянути всі рекомендації з безпеки, надані релевантними компаніями, та впроваджувати їхні найновіші рекомендації, оскільки відповідальна компанія найкраще може описати свої продукти та будь-які зміни, що могли статися.

Перед тим, як діяти за вказаними нижче рекомендаціями, врахуйте такі фактори:

Чинники до врахування

1. **Захист ваших учнів.**
   Потреби кожної школи відрізняються, а деякі групи учнів можуть потребувати додаткових заходів для захисту безпеки та конфіденційності. Багато технологічних інструментів для освіти мають функції, що допомагають налаштувати доступ залежно від віку, як-от обмежити неприйнятний контент або впевнитися, що місцезнаходження та контактні дані є конфіденційними.
2. **Види даних, які ви зберігаєте.**
   Якщо ви зберігаєте конфіденційні дані, ви можете зашифрувати їх або зберігати в окремому місці.
3. **Які типи пристроїв та модель розгортання ви використовуєте.**
   Пристрої та їхні додатки повинні отримувати автоматичні оновлення, щоб максимізувати безпеку, шифрувати дані та ізолювати облікові записи, аби забезпечити доступ користувачів лише до власної інформації.
4. **Політики вашої школи, району або регіону.**
   У вашому закладі освіти можуть діяти особливі правила щодо використання технологій. Ви маєте переконатися, що всі засоби захисту налаштовані відповідно до цих правил.

Щодня
Gmail блокує
100 мільйонів
спроб фішингу.

Щотижня
Google ідентифікує
300,000
небезпечних вебсайтів.

Щодня
74 мільйони
користувачів отримують допомогу від Менеджера паролів Google.

Щороку
700 мільйонів
людей посилюють їхню безпеку з Перевіркою безпеки.

Використовуйте безпечну автентифікацію

Безпечна автентифікація має бути головним пріоритетом для шкіл та інших закладів освіти. У четвертому кварталі 2022 року слабкі або неавторизовані облікові записи становили 48% усіх компрометуючих факторів у порушеннях. Впровадження деяких ключових рекомендацій може допомогти верифікувати, що користувачі є тими, за кого вони себе видають, а також обмежити доступ до інформації відповідно до ролі кожного користувача.

IT-адміністратори мають забезпечити використання двоетапної верифікації (2SV, також відомої як двофакторної або багатофакторної автентифікації) та перехід до безпарольної автентифікації (за допомогою ключів безпеки), де це можливо та особливо у випадках віддаленого доступу до систем закладу освіти. 2SV створює додаткових шар безпеки до ваших облікових записів онлайн, значно ускладнюючи доступ для нападників.

2SV є основою власної політики безпеки Google, і ми продовжуємо працювати над розробкою більш безпечних методів автентифікації.

Сьогодні в школах використовується багато типів пристроїв і моделей розгортання, а в середовищі K-12 є різні технічні можливості. Безпека облікових записів та пристроїв різниться залежно від ролей та типів користувачів. Водночас існують визначені найкращі практики: IT-адміністратори, вчителі та персонал, а також старші учні використовують закріплені за ними пристрої, тоді як молодші учні користуються спільними пристроями. Нижче ми розглянемо конкретні рекомендації для кожної групи.

Існує кілька типів методів автентифікації, які найкраще підходять у більшості випадків

- **Надійні паролі**
  Під час першого входу в систему запропонуйте користувачам створити власний пароль та встановіть мінімальні вимоги до довжини та складності. Довші паролі забезпечують додатковий елемент безпеки завдяки своїй довжині та складному використанню символів. Не слід вимагати від користувачів регулярної зміни паролів, оскільки це спонукає їх використовувати простіші паролі або вносити несуттєві зміни (наприклад, змінювати один символ).

- **Двофакторна верифікація**
  2SV захищає облікові записи завдяки другому крокові - часто чомусь, що користувач має з собою, як-от ключ безпеки або додаток на мобільному телефоні, що створює одноразовий код верифікації. Хоча будь-яка форма 2SV додає обліковому запису безпеки, адміністраторам варто уникати використання верифікаційних кодів, надісланих текстовими повідомленнями або дзвінками, які можуть бути вразливими до атак на основі номеру телефона.

- **Безпарольна автентифікація**
  Ключі доступу є безпечнішою та простішою альтернативою паролям. Користувачі можуть входити до додатків та вебсайтів за допомогою PIN-коду, графічного ключа, біометричного датчика (як-от відбитка пальця або розпізнавання обличчя) або натискання клавіші безпеки, що звільняє їх від потреби запам'ятовувати та керувати паролями. Тоді як зазначені методи можуть не підходити для кожного освітнього контексту, вони все частіше замінюють традиційні форми автентифікації та забезпечують більш безпечний і швидкий процес входу. Ключі безпеки захищають користувачів від фішингових атак, адже вони працюють лише на їхніх зареєстрованих вебсайтах та додатках.

- **Єдиний вхід (SSO)**
  SSO дозволяє користувачам отримувати доступ до кількох додатків та вебсайтів за допомогою одного набору облікових даних. Коли користувачі мають пам'ятати лише один набір облікових даних, вони з меншою ймовірністю записуватимуть їх. Окрім того, коли школи не мають керувати кількома наборами облікових даних, вони можуть заощадити кошти на IT-підтримку та послуги служби підтримки. Google Workspace for Education підтримує SSO, тому користувачі можуть використовувати їхні облікові дані Google для входу у сторонні додатки або використовувати облікові дані іншого постачальника для входу у свої облікові записи Google.

- **Менеджери паролів**
  Менеджери паролів можуть допомогти користувачам створювати надійні, унікальні паролі для облікових записів і служб, які вони використовують протягом навчального та робочого дня (за винятком випадків використання єдиного входу (SSO). Вони не допомагають увійти в операційну систему пристрою, але можуть керувати паролями після того, як користувач увійшов. Користувачі Google можуть використовувати Менеджер паролів у Chrome на будь-якій платформі, ChromeOS і Android.

Різні групи зі своїми унікальними потребами отримають перевагу від спеціалізованих підгруп або комбінацій цих підходів до автентифікації відповідно до їхньої ролі в закладі освіти, типу систем і даних, до яких вони мають доступ, а також їхнього віку.

Шкільні адміністратори

Адміністратори контролюють системи та більшу частину даних будь-якого закладу освіти типу K-12. Захист їхніх облікових записів є ключовим для безпеки всієї системи: від інфраструктури до даних облікових записів і пристроїв, якими керує заклад освіти. Вони повинні використовувати золотий стандарт серед методів автентифікації, зокрема застосовувати надійні паролі, потужний менеджер паролів та 2SV. Кожна з цих складових створює шар захисту, що разом забезпечують найбільш надійний захист для облікового запису адміністратора та корпоративних послуг.

- Адміністратори мають використовувати фізичний ключ безпеки або криптографічно безпечний метод 2SV, який вимагає довіреного пристрою та підказок. Це може бути такий сервіс, як Google Authenticator, або інший додаток, який створює одноразові коди перевірки. Пристрої Chromebook, випущені після 2019 року з чипом TPM, містять кнопку ввімкнення, яку можна використовувати для двофакторної автентифікації.
- Адміністратори повинні використовувати надійний менеджер паролів, що підтримує 2SV, для зберігання своїх паролів до різних сервісів.

Вчителі та персонал, які використовують призначені пристрої

Як і адміністратори, вчителі та співробітники мають доступ до конфіденційних даних, однак вони не контролюють цифрову інфраструктуру і мають різні рівні технічної підготовки.

- Вчителям та співробітникам, які використовують пристрої Chromebook, слід надати можливість входу в систему за допомогою біометричної автентифікації, якщо це дозволено законодавством, наприклад, за допомогою відбитка пальця.
- Адміністратори мають запровадити використання двофакторної автентифікації (2SV) та перейти на безпарольний метод автентифікації, коли це можливо і коли співробітник має віддалений доступ до систем навчального закладу освіти.

Старші учні, які користуються призначеними пристроями

(як правило, 4+ класи)

Старші учні краще обізнані в тому, як захистити себе, і зазвичай здатні використовувати більш надійні механізми автентифікації, які відповідають типам послуг, якими вони, ймовірно, користуватимуться. Вони повинні мати доступ тільки до власного облікового запису та інформації, що була з ними поширена.

- Учням, які використовують пристрої Chromebook, варто надати можливість створити PIN-код для конкретного пристрою, щоб пришвидшити вхід на ньому. Варіанти біометричної автентифікації можуть бути недоцільними або нездійсненними в багатьох шкільних умовах.
- Кожному учневі слід допомогти створити унікальний пароль, який не містить особистої інформації (наприклад, ім'я, клас або день народження). Учнів потрібно навчити, як використання фраз-паролів може забезпечити складність пароля та водночас зробити його легким для запам'ятовування.

Молодші учні, які користуються спільними пристроями (як правило, класи K-3)

Наймолодші учні тільки навчаються користуватися освітніми технологіями. Для них буде корисною проста автентифікація, яка підходить для використання з обмеженими послугами та даними.

- Школи, які використовують альтернативи паролям від сторонніх виробників, як-от QR-коди або вхід за зображеннями, для наймолодших учнів та тих, хто не може використовувати паролі, повинні вживати заходів безпеки, оскільки ці методи є менш захищеними. Адміністратори повинні змінювати пароль учня та оновлювати код щоразу, коли він губиться або стає доступним для інших.
- Школи мають навчати учнів та батьків про важливість збереження паролів у таємниці та безпечного зберігання альтернативних облікових даних, як-от QR-кодів.
- Для призначених пристроїв, як-от планшетів, можна використовувати PIN-код, прив'язаний до конкретного пристрою, як альтернативний безпечний метод автентифікації.

Застосовуйте належні налаштування безпеки

Шкільні пристрої та мережі є дуже привабливою ціллю для зловмисників в усьому світі, тому критично важливо використовувати найкращі можливі засоби безпеки, щоб запобігти втраті мережі, ресурсів, часу та коштів. Системні адміністратори повинні застосовувати ефективні та належні функції безпеки, доступні в продуктах, які використовують їхні заклади освіти. Водночас необхідно переконатись, що ці системи залишаються зручними у використанні для викладачів, співробітників та учнів.
Важливі налаштування безпеки та конфіденційності слід налаштовувати в такий спосіб, щоб окремі користувачі не могли їх вимкнути або змінити, а решта налаштувань повинні за замовчуванням мати захист, встановлений адміністратором. Критично важливо впроваджувати найкращі засоби безпеки, аби не втратити мережу, ресурси, час та кошти.
Якщо ви використовуєте Chromebook, ви можете переглянути наші рекомендації щодо налаштування безпеки пристроїв в останньому розділі.
Також застосовуйте принцип мінімізації даних у своїй практиці, обмежуючи цілі та засоби збору даних, використання та розкриття особистої інформації осіб тим мінімумом, який є розумно необхідним та пропорційним для надання послуги або відповідає контексту ситуації.

Додатки та оновлення

Обмежте та мінімізуйте кількість програм, які можуть встановлювати користувачі. Кожна встановлена програма є потенційною ціллю, яку можна використати для атаки. За можливості встановлюйте додатки з перевірених джерел. Наприклад, рекомендуйте користувачам звертати увагу на значок верифікації в Google Play (Play Маркет). Це допоможе їм завантажувати офіційні програми, які пройшли перевірку безпеки.
Будь-які модифікації операційної системи або апаратного забезпечення (джейлбрейк або рутинг) створюють серйозні проблеми безпеки, тому їх слід уникати.

Доступ та видимість

Адміністратори мають переконатись, що користувачі мають доступ лише до тих даних, програмного забезпечення, сервісів та систем, які їм необхідні для виконання своїх обов'язків або для ефективного навчання. Це допомагає обмежити зайвий доступ і відстежувати, хто має доступ та до яких ресурсів.

Особливу увагу слід приділити конфіденційним даним, таким як ідентифікаційна інформація користувача (PII), та системам (наприклад, відділ кадрів, заробітна плата, оцінювання, безпека та конфігурація). Для цього необхідно проводити аудит того, які користувачі можуть отримати доступ до даних і за яких обставин. Налаштуйте доступ виключно для пристроїв, що належать школі, та переконайтеся, що лише певні співробітники мають потрібні допуски.

Перегляньте політику обміну даними у спільних інструментах, щоб запобігти неналежному або надмірному обміну та несанкціонованому доступу. Обмежте або заблокуйте обмін інформацією за межами вашого середовища (особливо для студентів) та увімкніть політики, які контролюють обмін конфіденційною інформацією.

Якщо ваш пристрій втрачено або викрадено

Втрата пристрою не обов'язково означає втрату даних. Адміністратори повинні розробити та стандартизувати план дій для забезпечення доступу до інформації та документів у випадку втрати або крадіжки пристрою. Наприклад, зберігати документи в хмарному середовищі. Завантажте та роздрукуйте резервні коди для двоетапної перевірки, щоб запобігти перебоям у роботі облікового запису.

Якщо пристрій був втрачений або вкрадений, переконайтеся, що він буде заблокованим віддалено, якщо це можливо. Також потрібно заблокувати або позначити прапорцем пов'язані з цим пристроєм облікові записи, щоб запобігти несанкціонованому доступу. Дані з Chromebook можна віддалено стерти, якщо пристрій було втрачено, а облікові записи Google Workspace for Education можна відстежувати на предмет підозрілої активності або за потреби призупинити чи заблокувати.

Додатковий захист для користувачів із високим рівнем ризику

Для користувачів, які перебувають у категорії підвищеного ризику та працюють із конфіденційною інформацією (включно з адміністраторами Google Workspace for Education), Google пропонує Програму додаткового захисту (Advanced Protection Program, APP). Програма надає користувачам додатковий захист від цілеспрямованих атак, таких як фішингові розсилки, шкідливі завантаження та злам паролів. APP спеціально розроблено для протидії цілеспрямованим онлайн-атакам на облікові записи Google. Вона автоматично використовує надійну автентифікацію, ключі безпеки та обмежує стороннім особам доступ до даних облікового запису.

Інші постачальники онлайн-сервісів також пропонують надійний захист облікових записів для користувачів із високим рівнем ризику. Адміністратори та співробітники завжди повинні використовувати запропоновані засоби захисту, якщо вони мають доступ до особистої інформації або технологічних систем.

Оновлюйте та модернізуйте ваші системи

Оновлення операційної системи та програм на ваших пристроях — одна з найважливіших дій для захисту. Це особливо актуально для дитячого садку та школи, адже вони відіграють важливу роль в освіті та повсякденному житті дітей. Більшість атак шкідливого програмного забезпечення, як в освітньому середовищі, так і в інших сферах високого ризику, були спрямовані на системи Windows. Це стосується атаки SolarWinds; атаки програм-вимагачів на шкільні райони Лос-Анджелеса, Little Rock, Альбукерке; витоку даних Microsoft Exchange Server та нещодавнього зламу федеральних агентств Microsoft.

Саме тут використання хмарних продуктів та сервісів може полегшити завдання адміністраторів. Вони зменшують можливу поверхню для атаки та автоматично оновлюють системи та програми.

Оновлюйте операційну систему до найновішої

Найновіші версії операційних систем (ОС) зазвичай містять нові функції безпеки, які допомагають захиститись від відомих методів атак. Увімкніть функцію автоматичного оновлення в налаштуваннях операційної системи вашого пристрою. Якщо автоматичне оновлення неможливе, завантажуйте та встановлюйте оновлення та патчі щонайменше раз на місяць з офіційного джерела довіреного провайдера.

Пристрої Chromebook працюють на ChromeOS, яка автоматично оновлюється з найновішими патчами безпеки і застосовує останні розробки у сфері безпеки, також ChromeOS перевіряє цілісність операційної системи лише для читання перед завантаженням. Також Chromebook шифрує всі дані, що зберігаються на пристрої, захищаючи їх від несанкціонованого доступу. Кожна вебсторінка та програма запускається в окремій пісочниці. Тож якщо вебсайт або програма заражені шкідливим програмним забезпеченням, воно не зможе поширитися на інші частини пристрою.

Якщо ваша школа ще не готова перейти на Chromebook, ChromeOS Flex – це версія ChromeOS, призначена для модернізації шкільних пристроїв. ChromeOS Flex забезпечує всіх учасників навчального процесу єдиним сучасним досвідом навчання та викладання. Вона має вбудовані функції безпеки та можливості керування на основі хмари. Flex може автоматично блокувати шкідливі файли та програми, не замінюючи наявне обладнання.

Переходьте на сучасний браузер та оновлюйте його

Важливо також оновити та захистити ваш браузер. Сучасні браузери пропонують більш досконалі функції безпеки і спонукають користувачів їх увімкнути або ж адміністратори можуть налаштувати їх автоматичне ввімкнення на службових комп'ютерах. Це дозволяє захистити конфіденційність чутливої інформації під час її передачі через Інтернет. Браузер слід постійно оновлювати. Оновлений сучасний браузер, незалежно від того, чи використовується він для роботи, навчання чи інших онлайн дій, забезпечить:

- **Безпеку**, включаючи ізоляцію сайтів та захист безпечного перегляду, щоб запобігти випадковому відвідуванню небезпечних вебсайтів.
- **Автоматичне оновлення:** щоб ваш браузер швидко отримував останні оновлення безпеки
- **Безпечне з'єднання:** сучасні браузери використовують шифрування транспортного рівня (TLS). Користувачі можуть перевірити, чи з'єднання є безпечним, клацнувши поруч із URL-адресою.

Chrome було розроблено з урахуванням безпеки, такі функції безпеки, як безпечний перегляд, увімкнено за замовчуванням. Також є інтегрований менеджер паролів, який може автоматично заповнювати паролі під час перегляду вебсторінок, дозволяючи легко використовувати складні паролі.

Використовуйте системи сповіщення та моніторингу в реальному часі

Системи сповіщення та моніторингу в реальному часі можуть допомогти школам швидко виявляти та реагувати на загрози ще до того, як вони завдадуть шкоди. Важливо, щоб засоби безпеки працювали фоново, збираючи та реєструючи події безпеки з усіх ваших систем. Інструменти штучного інтелекту (AI) особливо ефективні для аналізу великих обсягів зібраних даних та пошуку аномалій і закономірностей, які можна використовувати для швидкого та легкого виявлення загроз, а також для обробки та усунення вразливих точок. Це дозволяє визначити пріоритетність того, які дії потребують перегляду IT-адміністратором або співробітниками.

Школи можуть використовувати функції сповіщення та моніторингу, вбудовані в основне програмне забезпечення для спільної роботи та зв'язку, наприклад, Google Workspace for Education, або розгортати окремі рішення, як-от Security Information and Event Monitoring (SIEM).

Системи сповіщення та моніторингу в реальному часі можуть відстежувати різноманітну активність у мережі школи, на пристроях, у програмах, облікових записах користувачів та даних, наприклад, входи користувачів, доступ до файлів, потенційні вторгнення, успішне або невдале викрадення даних та дії адміністраторів. Якщо система виявляє підозрілу активність, вона може надіслати сповіщення IT-персоналу школи. Це дозволяє адміністраторам дослідити проблему та вжити заходів для нейтралізації загрози.

Окрім того, інструменти сповіщення та моніторингу можна використовувати для глибшого розуміння загроз, із якими стикаються школи. Аналізуючи дані з цих систем реального часу, школи можуть виявляти тенденції та закономірності, які допоможуть їм краще захистити себе.

Найкращі практики використання систем сповіщення та моніторингу (включаючи SIEM)

1. **Визначте свої цілі безпеки**
   Визначте, яка інформація та системи є найбільш критичними для школи, а також, які типи загроз становлять для вас найбільший ризик. Після цього слід визначити дані, які потрібно збирати для моніторингу цих загроз.

2. **Збирайте потрібні дані та налаштовуйте їх належним чином**
   Важливо збирати потрібні дані та налаштовувати програми для досягнення ваших найважливіших цілей безпеки. Це можуть бути дані з брандмауерів, фільтрів вмісту, систем виявлення вторгнень, вебсерверів та інших пристроїв безпеки, а також із програм для спілкування та співпраці, шкільних інформаційних систем та систем управління навчанням.

3. **Розслідуйте та реагуйте на сповіщення**
   Коли ваша система моніторингу надсилає сповіщення, важливо дослідити проблему та вжити належних заходів. Це може потребувати залучення кількох команд для розслідування джерела оповіщення, визначення того, чи це хибна тривога. Можливо, необхідно зробити певні дії для нейтралізації загроз, наприклад, призупинити облікові записи, оновити паролі користувачів, ізолювати або видалити електронні листи, змінити дозволи доступу до файлів, очистити пристрої.

Навчайте вчителів, співробітників та учнів

Заклади освіти повинні підвищувати рівень обізнаності та формувати безпечні звички у шкільних спільнотах. Для цього можна використовувати інформаційні кампанії та співпрацювати з партнерами. Обов'язково навчайте вчителів, співробітників та учнів важливості безпеки в Інтернеті, щоб допомогти їм захистити себе та уникнути серйозних кіберзагроз. Розкажіть їм, як користуватися продуктами та сервісами, що використовуються в закладі освіти, як виявляти та повідомляти про загрози, такі як фішингові електронні листи, а найголовніше – як вживати заходів для запобігання цим атакам.

Як безпечно користуватися пристроями та програмним забезпеченням

Адміністратори шкіл можуть співпрацювати з вчителями та експертами з кібербезпеки для розробки навчальних програм з урахуванням віку учнів. Такі програми допоможуть їм зрозуміти, як безпечно користуватися пристроями, програмним забезпеченням та системами. Створення навчальних матеріалів під власним брендом школи або району допоможе адаптувати рекомендації для ваших вчителів та учнів. Однак ви також можете скористатися вже готовими матеріалами, такими, як програма «Безпека дітей в Інтернеті», яка доступна на сайті Safety.Google та Khan Academy, та адаптувати їх до ваших потреб. Ці програми можуть допомогти користувачам залишатися в безпеці незалежно від того, де вони перебувають – у школі чи поза її межами.

Як розпізнати загрози

Навчання вчителів, співробітників та учнів розпізнавати загрози є важливим елементом їхньої безпеки. Вміння дітей визначати, чи щось є загрозою, чи ні, є критичним, оскільки вони можуть не знати, як перевірити правдивість інформації. Існує кілька типів загроз, які вони повинні вміти розпізнавати та повідомляти про них. Адміністраторам слід зосередитися на тих темах, які, на їхню думку, принесуть найбільшу користь. Важливо, щоб навчання не просто допомагало користувачам розпізнавати загрозу, а й спонукало їх до дій. Поширені загрози, які користувачі повинні розпізнавати, включають програми-вимагачі, фішинг, соціальну інженерію, шкідливе програмне забезпечення та шахрайство. Однак, якщо в закладі освіти поширені певні типи загроз, варто подбати про те, щоб шкільна спільнота була поінформована саме про них.

Безпечне зберігання та передача даних і файлів

Вчителів і співробітників слід навчати належному обміну файлами та даними, а також тому, як розпізнавати підозрілі запити на електронній пошті. Вкрай важливо, щоб вони передавали або обробляли конфіденційну особисту інформацію лише за необхідності та із застосуванням додаткових засобів захисту даних. Наприклад, ніколи не слід передавати таку інформацію електронною поштою або стороннім організаціям. Для запобігання витоку даних вчителі та персонал повинні використовувати функції захисту від втрати даних (вони доступні в ChromeOS і Workspace for Education). Ці функції можуть попереджувати та блокувати кінцевих користувачів від передачі файлів з конфіденційними даними (наприклад, номерами соціального страхування) або від копіювання та перенесення конфіденційного вмісту за межі домену.

Підхід Google у дії: Пристрої та сервіси для освіти

Закупівля програмного забезпечення — один із найпотужніших інструментів, яким користується шкільний район для захисту. Програмне забезпечення повинно бути надійно побудованим та спроєктованим у такий спосіб, щоб мінімізувати ризики вразливостей, із безпекою, вбудованою на кожному рівні. За умови закупівля школами надійного програмного забезпечення або програмного забезпечення від компаній із перевіреною безпечністю загальний кіберризик може бути значно зменшений. Наприклад, у Google ми посилили безпеку ChromeOS, продовжуючи впроваджувати більш прогнозовані інтелектуальні рішення, які використовують потужність нашого машинного навчання, хмари та експертизи в ідентифікації.

Google Workspace for Education

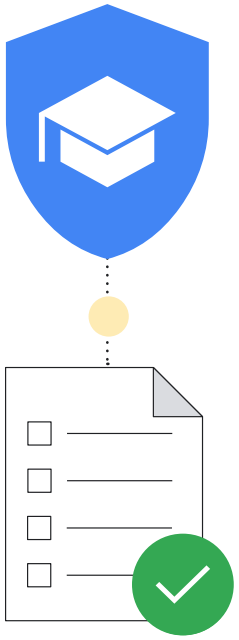
Google Workspace for Education - це набір інструментів та сервісів Google, які адаптовані для шкіл з метою співпраці, оптимізації інструкцій та безпеки навчання. Продукти та сервіси Google for Education постійно захищають користувачів, пристрої та дані від все складніших загроз і надають інструменти, такі як центри попереджень та безпеки, сховище для електронного виявлення, ідентифікації та управління доступом, а також запобігання втрати даних. Ми підготували корисні матеріали на випадок, якщо ви тільки починаєте використовувати Google Workspace for Education, багато з яких можуть допомогти вам налаштувати все відповідно до рекомендацій. Для початку роботи з Google Workspace for Education, перегляньте посібник зі швидкого IT-налаштування.

Google прагне створювати продукти, які допомагають захищати приватність учнів та вчителів і забезпечують найвищий рівень безпеки для вашого закладу освіти. Ви можете бути певні, що продукти та сервіси Google for Education постійно захищають користувачів, пристрої та дані від усе більш складних загроз. Цей розділ надає рекомендації з безпеки для адміністраторів IT-систем шкіл під час використання продуктів Google for Education.

Перелік пунктів перевірки безпеки

Ознайомтеся з переліками перевірки безпеки, наведеними у розділі джерел, щоб дізнатися більше про те, як підвищити безпеку та конфіденційність вашого закладу освіти. Школи, які використовують Google Workspace for Education Standard і Plus, також можуть використовувати сторінку Security Health для моніторингу конфігурації налаштувань вашої консолі адміністратора. Наприклад, ви можете перевірити статус таких налаштувань, як автоматичне пересилання електронної пошти, шифрування пристроїв, налаштування обміну даними у Google Drive та багато іншого. У разі потреби ви можете вносити зміни до налаштувань вашого домену на основі загальних рекомендацій із безпеки та найкращих практик, збалансувавши ці рекомендації з потребами вашої організації та політикою управління ризиками.

Чому освітній сектор очікує бути враженим?



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

Ось кілька інших корисних порад, щоб переконатися, що ви максимізуєте захист, вбудований у Google Workspace for Education:

Створення організаційних підрозділів

Ніхто не стане сперечатися, що всі у вашому обліковому записі Google Workspace for Education повинні мати однакові налаштування. Організаційні підрозділи – це групи користувачів, які дозволяють надавати різні послуги, налаштування та дозволи різним користувачам, наприклад, використовувати 2SV* для вчителів і персоналу та автентифікацію відповідно до віку для молодших учнів. Створіть окремі організаційні підрозділи для персоналу, викладачів і студентів, щоб застосовувати політики окремо для кожної групи користувачів. Добре продумана структура має вирішальне значення для ефективного й гнучкого керування обліковим записом Google Workspace for Education.

*2SV – (англ. 2-Step Verification) – двофакторна верифікація;

Налаштування політики паролів і захисту облікових записів адміністратора

Як ми й обговорювали, автентифікація користувачів є важливою складовою безпеки вашої установи. Ось чому ми налаштували гнучкі способи керування автентифікацією для адміністраторів, які дозволять вам переконатися, що користувачі мають належний і безпечний захист облікових записів.

Установіть політику паролів, щоб гарантувати, що користувачі створюватимуть надійні паролі, і розгляньте можливість використання 2SV, де це доречно, на основі рекомендованих груп у розділі «Безпечний вхід». Ви можете примусово використовувати 2SV для підмножини користувачів (даючи їм час на налаштування) і розгортати 2SV за допомогою різноманітних методів, зокрема ключів безпеки (найбільш безпечний), сповіщення Google (за допомогою програм Google на Android та iOS) , генераторів додатків перевірки (наприклад, Google Authenticator), текстових повідомлень чи телефонних дзвінків (хоча це найменш безпечний метод).

Якщо ваша організація використовує постачальника ідентифікаційної інформації (IdP), відмінного від Google, ви можете налаштувати систему єдиного входу (SSO*) через стороннього постачальника ідентифікаційної інформації. За бажанням ви все ще можете використовувати 2SV з SSO* для облікових записів, які не є суперадміністраторами.

*SSO – (англ. Single Sign On) – єдиний вхід.

Увімкніть або вимкніть служби

Адміністратори можуть контролювати, до яких служб Google користувачі мають доступ за допомогою свого облікового запису Google Workspace for Education, із консолі адміністратора Google. Ви можете керувати доступом до таких служб Google, як Календар, Диск і Meet, увімкнувши або вимкнувши служби за організаційними підрозділами (ви також можете ввімкнути служби під час використання груп). Ви також можете переглянути відмінності між Workspace Core і Додатковими службами, перш ніж увімкнути додаткові служби, як-от YouTube, Карти Google і Blogger.

Адміністраторам варто встановлювати доступ до сервісів Google на основі віку та мати на увазі, що користувачі, які мають статус осіб, що не досягли 18 років, автоматично мають обмеження у деяких сервісах Google під час входу у свій обліковий запис Google Workspace for Education.

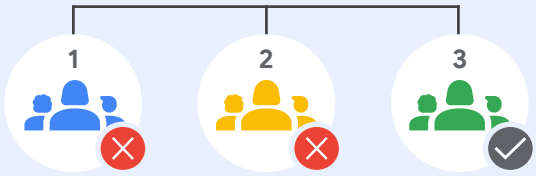
Ви також можете використовувати функцію Контекстно-залежного доступу (доступна у Workspace for Education Standard та Plus), щоб дозволяти або блокувати доступ до додатків Google, таких як Gmail, Диск та Календар, на основі IP-адреси пристрою, географічного походження, політик безпеки або операційної системи. Наприклад, ви можете дозволити доступ до Диску лише на пристроях, що належать компанії та перебувають у певних країнах/регіонах.

Способи надання користувачам доступу до сервісів

У консолі адміністратора Google можна вимкнути організаційний доступ пристрою до служби Google, наприклад Google Диск. Якщо деяким користувачам у цьому організаційному підрозділі потрібно використовувати Диск, у вас є 2 варіанти:

1. Перемістіть користувачів до організаційного підрозділу, у якому ввімкнено Диск.
2. Додайте користувачів у групу доступу та ввімкніть Диск для групи. Кожен учасник може отримати доступ до служби, навіть якщо в її організаційному підрозділі служба вимкнена.

Організаційні підрозділи



Google Диск вимкнено для організаційних підрозділів 1 і 2

З групою доступу

Але **група користувачів** усередині організаційних підрозділів 1 і 2 можуть використовувати Google Диск

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

Встановіть політику обміну даними та правила зберігання

Як адміністратор ви можете контролювати, чи можуть користувачі ділитися файлами та папками Google Диска з людьми за межами вашої організації. Це може допомогти запобігти ненавмисному або надто широкому обміну даними та файлами, запобігаючи витоку даних. Розділення файлів і дисків, створення організаційних одиниць та діяльність за принципом найменших привілеїв є важливими для запобігання переміщенню зловмисників мережами, якщо вони проникнуть в один обліковий запис. Чим менше доступу до даних і мережі має потенційний зловмисник, тим менше шкоди може бути завдано.

Вимкніть зовнішній обмін файлами для учнів (або обмежте зовнішнє спільне використання лише дозволеними доменами) і встановіть для параметра «Перевірка доступу» значення «Лише для одержувачів». Якщо ви дозволяєте деяким або всім користувачам ділитися файлами за межами вашого домену, увімкніть попередження, коли користувач це робить. Окрім того, вимкніть публікацію файлів в Інтернеті та вимагайте від зовнішніх співавторів входу за допомогою облікового запису Google.

Окрім того, клієнти Workspace for Education Standard і Plus можуть використовувати Цільові аудиторії та Правила довіри, щоб встановлювати рекомендації та обмеження спільного доступу на більш детальному рівні. Наприклад, за допомогою «Цільової аудиторії» ви встановлюєте аудиторію для вчителів за замовчуванням для обміну посиланнями на «Викладачі та персонал», а не на всіх у вашому закладі освіти. За допомогою «Правил довіри» ви можете заборонити учням початкових класів ділитися файлами зі старшими.

- Перегляньте політику спільного диска, щоб переконатися, що лише відповідні користувачі можуть створювати спільні диски та забороняти зовнішнім користувачам доступ до спільних дисків. Рекомендовано дозволяти створювати спільні диски лише адміністраторам (або персоналу та викладачам) і ретельно керувати доступом до спільного диску.
- Подумайте про обмеження видимості каталогу та спільного доступу до контактів, коли це можливо, шляхом вимкнення спільного доступу до контактів для деяких чи всіх користувачів або шляхом створення користувацьких каталогів, щоб обмежити, які користувачі кому доступні.
- Налаштуйте політики запобігання втраті даних (DLP - data loss prevention) на Диску та в Gmail, щоб виявляти та блокувати конфіденційну інформацію. Існують попередньо створені політики, які можна використовувати для захисту загальної конфіденційної інформації (наприклад, номерів банків або кредитних карток). Ви також можете створювати власні політики на основі ключових слів, списків слів і регулярних виразів (Regex).

Керуйте налаштуваннями Gmail

Gmail є одним із основних сервісів Google Workspace for Education, і є багато налаштувань, перевагами яких адміністратори можуть скористатися, щоб захистити свою установу та своїх користувачів.

Запобігайте спаму, спуфінгу та фішингу за допомогою автентифікації Gmail. Налаштуйте параметри спам-фільтра, включно з вимогою автентифікації відправника для всіх схвалених відправників і вимкнення обходу спам-фільтрів для внутрішніх відправників.

Вимкніть доступ POP/IMAP, коли це можливо, і ввімкніть покращене сканування повідомлень перед відправкою та розширений захист від фішингу і зловмисного програмного забезпечення. Якщо ви дозволяєте зовнішні електронні листи для деяких або всіх користувачів, ви можете ввімкнути попередження зовнішніх одержувачів.

Клієнти Google Workspace for Education Standard і Plus також можуть допомогти захистити дані від зловмисного програмного забезпечення та програм-вимагачів, налаштувавши правила для виявлення шкідливих вкладень за допомогою Пісочниці безпеки.

Сторонні програми

Використовуйте вбудовані робочі процеси для схвалення сторонніх програм, які отримують доступ до даних облікового запису через API. Це допомагає запобігти передачі несанкціонованих даних додаткам сторонніх розробників, не схвалених для використання в школі.

Скористайтеся центром безпеки

Адміністратори Google Workspace for Education Plus і Standard можуть використовувати центр безпеки, який надає розширену інформацію про безпеку та аналітику, а також додає видимість і контроль проблем безпеки, що стосуються вашого домену.

Центр безпеки містить Інструмент дослідження безпеки, який може допомогти адміністраторам ідентифікувати, сортувати та вживати заходів щодо проблем безпеки та конфіденційності, таких як фішингові атаки, неприйнятне поширення файлів, підозрілі дії користувачів і пристроїв і багато іншого.

Звіти та моніторинг

Як адміністратор ви можете переглядати звіти та реєструвати події на консолі адміністратора Google, щоб перевіряти діяльність у своїй організації, як-от потенційні загрози безпеки, бачити, хто та коли входить, а також розуміти, як користувачі створюють і діляться вмістом. Ви можете переглядати дані на рівні домену разом із детальною інформацією на рівні користувача за допомогою графіків і таблиць. Використовуйте звіти та журнали аудиту (включно з центром сповіщень), щоб визначати ризики безпеки, аналізувати використання служб, діагностувати проблеми конфігурації, відстежувати дії користувачів і багато іншого.
Адміністратори Google Workspace for Education Standard і Plus можуть використовувати інформаційну панель безпеки, щоб переглядати різні звіти про безпеку, визначати тенденції та порівнювати поточні та історичні дані, як-от спільний доступ до файлів на Диску, спам, фішинг і зловмисне програмне забезпечення в Gmail, підозрілі входи в облікові записи користувачів і підозрілі дії на пристроях. Більшість журналів використання, активності та аудиту, включаючи події адміністратора, Диска, Meet і Chat, а також звіти про безпеку доступні протягом шести місяців.

Google Workspace – найбезпечніший у світі хмарний набір для спілкування та співпраці

0
активно використаних вразливостей програмного забезпечення у Workspace із листопада 2021 року*

2x менше
інцидентів безпеки для організацій, які використовують Workspace порівняно з Microsoft 365

2.5x менше
інцидентів безпеки для організацій, які використовують Workspace порівняно з Microsoft Exchange

50%
потенційної економії на страхуванні з кібербезпеки за допомогою Workspace

*Згідно з CISA це значно менше, ніж в інших продуктових постачальників у цьому просторі.

Chromebook

Пристрої Chromebook — це надзвичайно безпечні, універсальні та прості у використанні комп'ютери для студентів і викладачів завдяки вбудованим функціям безпеки. Жодного випадку атак програм-вимагачів на будь-які корпоративні, навчальні чи персональні пристрої ChromeOS офіційно не було зафіксовано. Пристрої Chromebook допомагають захистити заклади освіти від нових загроз завдяки постійним оновленням, які відбуваються автоматично у фоновому режимі, тож користувачі можуть повертатись до роботи за лічені секунди.

Автоматичне оновлення ОС і програм із вбудованим захистом від зловмисного програмного забезпечення

Зловмисники постійно намагаються скористатися помилками та лазівками в операційних системах, браузерах і популярних програмах, щоб встановити шкідливе програмне забезпечення та вкрасти дані користувачів. Аби захистити вас і ваших користувачів, Chromebook оновлює вашу ОС та застосунки автоматично, адже безпека вбудована за замовчуванням. До того ж, хмарним додаткам не потрібні такі оновлення програмного забезпечення, як це буває з локальними програмами.

Спеціальний захисний чіп від Google на Chromebook допомагає захистити пристрій, дані користувачів та гарантує цілісність системи.

Всі пристрої Chromebook у вашому користуванні автоматично отримуватимуть найновіші оновлення захисту від шкідливого програмного забезпечення. Вбудовані функції безпеки, такі як шифрування даних, перевірене завантаження, ізольоване програмне середовище та автоматичне оновлення, забезпечують захист учнів та освітян від кіберзагроз.

Безпека даних користувачів

Під час входу на пристрій Chromebook за допомогою вашого облікового запису Google усі ваші дані зберігаються в зашифрованих файлах. Це гарантує, що ніхто інший на пристрої не зможе переглянути ваші дані або ввійти в програми, використовуючи ваш обліковий запис. Завдяки цьому учні можуть легко й безпечно користуватися спільними пристроями в межах класу, а заклади освіти скоротити загальні витрати на обчислювальну техніку.

Для отримання додаткових функцій безпеки Chrome Education Upgrade (ліцензія на керування пристроями) пропонує розширений моніторинг.

Безпека пристроїв із віддаленим керуванням користувачами

Шкільні адміністратори можуть налаштовувати політики ChromeOS, а також дистанційно встановлювати та оновлювати програми за допомогою консолі Google Admin. Лише одним кліком IT-адміністратор може миттєво оновити політики та налаштування сотень тисяч пристроїв Chromebook.

Ці політики можуть гарантувати, що:

- Учні матимуть доступ лише до схваленого школою контенту та додатків
- Всі програми та розширення оновлені з останніми виправленнями безпеки
- Користувачі не можуть копіювати, передавати або поширювати шкільні дані за межами пристрою
- Адміністратори можуть приймати обґрунтовані рішення на основі персоналізованих рекомендацій Google щодо безпеки для протидії кіберзагрозам
- Адміністратори можуть централізовано керувати безпекою, посвідченнями користувачів та політиками керування доступом безпосередньо в консолі адміністратора.

Деякі важливі політики для налаштування адміністраторами:

Політики пристроїв

- **Гостьовий режим**
  Рекомендовано вимкнути гостьовий режим на пристроях, щоб учні та вчителі входили у систему за допомогою власних облікових даних, а не анонімно користувалися пристроєм.
- **Обмеження входу в систему**
  Можливо, ви не захочете, щоб учні та вчителі входили на Chromebook вашої школи за допомогою особистих облікових записів Gmail. Встановіть обмеження входу в систему, щоб облікові записи обмежувалися лише вашим доменом Workspace для пристроїв, які використовуються виключно учнями.
- **Звіти про користувачів і пристрої**
  Адміністраторам слід подумати про ввімкнення звітування про користувачів і пристрої, щоб збирати дані про те, як часто використовуються пристрої Chromebook, хто їх використовує та який стан їхнього апаратного забезпечення.
- **Примусова повторна реєстрація**
  Вкрай важливо, щоб Chromebook, що належить школі, залишався в школі, якщо адміністратор його не виведе з експлуатації. Адміністраторам слід подумати про ввімкнення примусового повторного зарахування пристроїв Chromebook, щоб вони завжди повторно реєструвались, якщо їх скинули до заводських налаштувань або спробували вкрасти.

Політики користувача

- **Режим інкогніто**
  Учнів слід налаштувати на успішну роботу зі шкільними пристроями Chromebook. Це включає в себе обмеження доступу до їхнього автентифікованого браузера, щоб фільтри вебконтенту могли утримувати їх від відвідування неприйнятних вебсайтів. Адміністратори повинні вимкнути режим інкогніто, щоб учні не могли обійти вебфільтри.
- **Режим проксі-сервера**
  Хоча деякі школи можуть використовувати проксі-сервери для вебфільтрації, важливо не надавати користувачам можливості самостійно змінювати налаштування проксі-сервера.
- **Багаторазовий доступ до входу**
  Якщо користувачам дозволено входити в додатковий обліковий запис під час використання шкільних облікових записів Chromebooks і Workspace, це може дозволити користувачеві легко викрасти конфіденційні дані/інформацію про учнів або школу в цьому додатковому обліковому записі. Адміністраторам варто розглянути можливість блокування доступу з декількома входами.
- **Історія браузера**
  Для учнів може бути корисним відключити можливість очищення історії браузера. Якщо станеться інцидент з інтернет-безпекою, ці журнали можуть бути корисними під час розслідування.

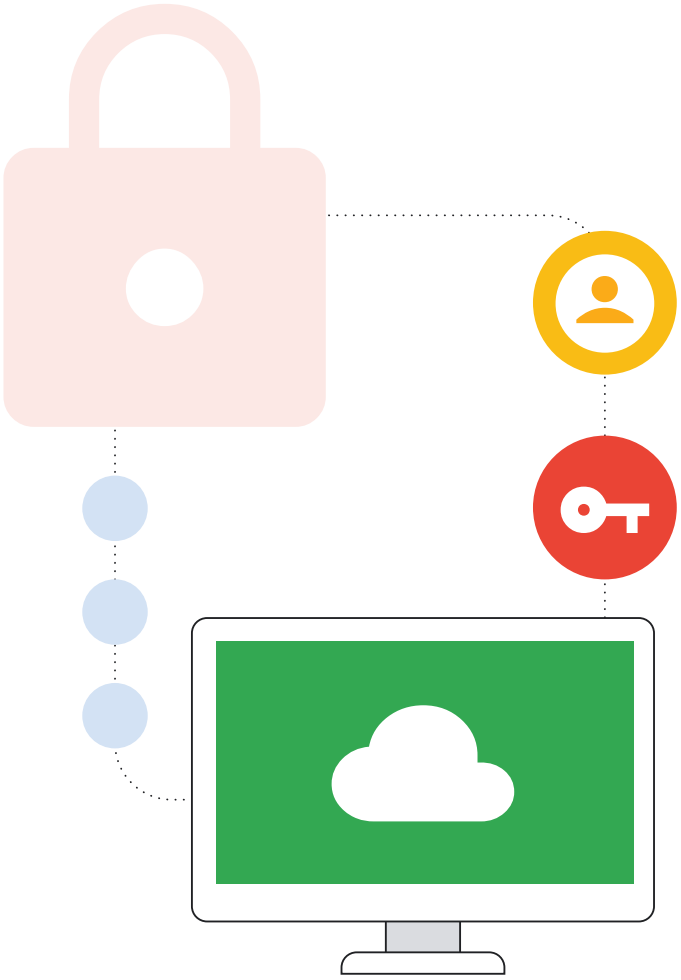
Цей список є хорошою відправною точкою для забезпечення захисту ваших мереж від найпоширеніших типів помилок, які призводять до серйозних кіберінцидентів. Інші додаткові рекомендовані політики безпеки можна знайти в нашому Контрольному списку безпеки.

Керування кінцевими точками для безпечного використання будь-де та будь-коли

Система віддаленого керування політиками ChromeOS дає змогу шкільним адміністраторам застосовувати налаштування безпеки та запускати інструменти захисту, як-от системи фільтрації контенту, на пристрої, а не на мережевих серверах школи. Це гарантує, що учні отримують ті ж переваги безпеки на шкільних пристроях Chromebook вдома, що й у класі. Це стає дедалі важливішим, оскільки школи переходять на цифрові підручники та онлайн-інструменти навчання, а також виникає потреба надавати учням комп'ютери додому для виконання домашніх завдань.

Висновок

Захист закладів освіти K-12 від кіберінцидентів є складним завданням, але інвестиції в нього повністю виправдані, оскільки захищають вас, учнів, вчителів, персонал та усю онлайн-екосистему. Пункти, викладені в цьому документі, є гарним початком, проте кожній школі потрібно буде адаптувати рекомендації до своїх потреб та постійно йти в ногу зі змінами загроз та новітніми технологіями. Цей ресурс є надійною основою будь-якої програми безпеки закладів освіти K-12, пропонуючи потенційні наступні кроки та можливі до виконання дії. Google також має різноманітні ресурси, навчання та кваліфікованих фахівців з кібербезпеки, які можуть допомогти школам та організаціям, що використовують цей посібник, а також у сфері новітніх технологій, таких як штучний інтелект. Продукти Google, розроблені спеціально для освіти, пропонують готові рішення для багатьох пасток кібербезпеки, описаних у цьому документі. Ми прагнемо співпрацювати з вами під час розробки та реалізації ваших програм безпеки.



Список ресурсів

Стан кібербезпеки в технологіях для навчання учнів K-12 та пов'язані ризики

Звіти уряду США

- Звіт CISA «На захисті нашого майбутнього» (січень 2023 р.) досліджує кіберзагрози, з якими стикаються початкові та середні школи, та надає рекомендації, що включають вказівки щодо кібербезпеки, покликані допомогти школам протистояти цим ризикам
- Попередження CISA "Кіберактори атакують дистанційне навчання K-12, щоб спричинити збої та викрасти дані" (грудень 2020 р.) зазначає, що заклади освіти є пріоритетними цілями для кібератак
- Звіт GAO "Безпека даних: останні витоки даних K-12 показують, що учні вразливі до шкоди" (15 жовтня 2020 р.)
- CISA, ФБР та MS-ISAC випустили спільне попередження під назвою #StopRansomware (Зупинимо програми-вимагачі)

  Згідно з повідомленням Vice Society (вересень 2022 р.) деякі зловмисники непропорційно часто атакують сектор освіти програмами-вимагачами. Перехід на більш безпечне рішення, наприклад Chromebook, може підвищити рівень захисту. На жодному пристрої ChromeOS ніколи не було виявлено програм-вимагачів.

Обговорення кіберзагроз в освіті та інших сферах

- Звіт Sophos «Стан програм-вимагачів в освіті 2023», опублікований у липні 2023 року, виявив, що 80% опитаних закладів освіти K-12 постраждали від програм-вимагачів
- Дослідження Zscaler, оприлюднене у квітні 2023 року, показує майже 50% зростання фішингових атак, насамперед серед сфер освіти, фінансів та уряду
- Стаття про приклад атаки-вимагача на шкільний округ, опублікована у вересні 2022 року, під назвою «Все, що ми знаємо наразі про атаку програми-вимагача на школи Лос-Анджелеса»
- Ще одна програма-вимагач, яка призвела до закриття шкіл, описана у статті «Кібератака в Альбукерке змушує школи скасувати заняття», опублікованій у січні 2022 року
- Інформація про нещодавній злам електронної пошти, опублікована Microsoft у липні 2023 року, повідомляє про те, що китайські хакери зламали електронну пошту, включаючи установи уряду США

Початок роботи з Google for Education

Загальна інформація для початку роботи з продуктами Google for Education

- Посібник зі швидкого IT-налаштування для Google Workspace for Education містить вісім кроків налаштування вашого закладу
- Більше про Chromebook в освіті
- Сторінка «Про керування пристроями Chromebook» містить посібник, який надасть початкову допомогу адміністраторам, які керують ChromeOS у школі

- Контрольний список безпеки для середнього та великого бізнесу містить поради щодо налаштування Google Workspace for Education та пристроїв Chromebook, які застосовуються в освітньому контексті
- Перегляньте додаткову інформацію про пакети Google Workspace for Education Fundamentals, Standard, та Plus тут
- Дізнайтеся, як підключати, реєструвати, керувати та оновлювати Chromebook та Chrome-пристрої
- Перегляньте більше інформації про те, як Google for Education може допомогти вам захистити ваш заклад у Центрі конфіденційності та безпеки Google for Education

Використовуйте безпечну автентифікацію

- Як використовувати ключ безпеки для двофакторної верифікації
- Інформація про те, як використовувати безпарольний вхід із ключами доступу
- Як встановити в Google Workspace for Education
  - Вимоги до пароля для користувачів
  - Стороннього постачальника ідентифікації SSO
  - Як двофакторна верифікація працює з цими сторонніми постачальниками
- Як змусити користувачів здійснювати вхід за допомогою двофакторної або багатофакторної автентифікації на пристроях Chromebook або в ОС Chrome
- Захист облікових записів для користувачів із високим ризиком
  - Як захистити користувачів із Програмою додаткового захисту Google

Застосовуйте відповідні налаштування безпеки та конфіденційності

- Як контролювати доступ сторонніх та внутрішніх програм до даних Google Workspace
- Як керувати доступом користувачів до 18 років до сторонніх не налаштованих додатків
- Як керувати налаштуваннями Gmail
  - Запобігайте спаму, фішингу та викраденню особистих даних за допомогою автентифікації Gmail
  - Додавайте власні фільтри спаму до Gmail
  - Вмикайте або вимикайте POP та IMAP для користувачів, щоб запобігти використанню сторонніх поштових програм
  - Запобігайте фішингу за допомогою сканування повідомлень перед доставкою
  - Захистіть користувачів від вхідних листів із фішингом та шкідливими програмами
  - Контролюйте, чи показуватиме Gmail попередження для зовнішніх отримувачів
  - Встановіть правила для виявлення шкідливих вкладень за допомогою Пісочниці безпеки
- Додати організаційний підрозділ

- Увімкнення та вимкнення сервісів Google Workspace for Education
  - Пояснення основних та додаткових сервісів Google Workspace for Education
  - Інструкції щодо вмикання та вимикання сервісів для користувачів Google Workspace
  - Способи керування доступом до сервісів Google залежно від віку користувачів
  - Захист вашої організації за допомогою детального контролю доступу до програм на основі таких атрибутів, як особисті дані користувача, розташування, стан безпеки пристрою та IP-адреси
- Встановлення політик обміну даними та правил зберігання
  - Керування зовнішнім обміном даних для вашої організації
  - Обмеження доступу, який користувачі можуть надавати до файлів
  - Налаштування цільових аудиторій для обміну, наприклад, відділів або команд
  - Створення та керування правилами обміну Диском
  - Дозвіл користувачам створювати спільні диски та встановлювати налаштування спільного доступу за замовчуванням
  - Керування учасників спільних дисків та їх рівнів доступу в організації
  - Увімкнення або вимкнення каталогу для контролю доступу до організаційних та зовнішніх контактів
  - Налаштування каталогу для команди або групи в межах організації
  - Захист конфіденційної інформації за допомогою політик запобігання втраті даних

Оновлення та модернізація ваших систем

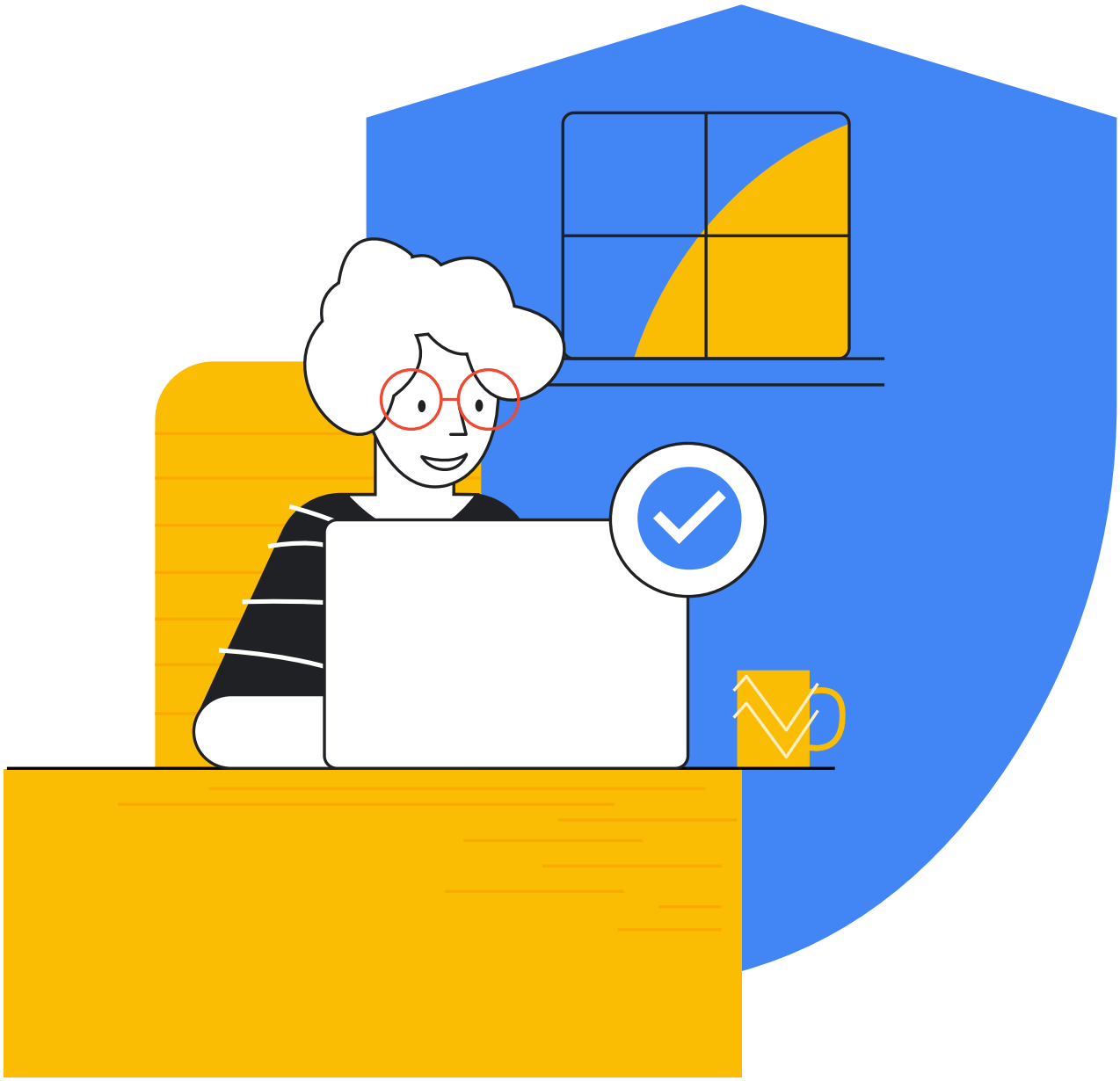
- Як керувати оновленнями пристроїв ChromeOS
- Chrome – сучасний браузер, простий в управлінні та оснащений засобами безпеки та керування корпоративного рівня
- Chrome OS Flex – це хмарна швидка, легка в управлінні та безпечна операційна система для ПК та Mac, яка може модернізувати пристрої, що вже є у вас

Використовуйте системи оповіщення та моніторингу в реальному часі

- Найкращі практики для моніторингу ваших пристроїв з ChromeOS, із використанням консолі Google Admin
- Сповіщення та моніторинг Google Workspace
  - Інформація про те, як контролювати використання та звіти безпеки для виявлення ризиків безпеки та відстеження активності користувачів
  - Інформація про те, як користуватися центром сповіщень та чим центр сповіщень відрізняється від сповіщень адміністратора електронною поштою
  - Інформація про те, як користуватися інформаційною панеллю безпеки, включно з відповідями на поширені запитання
  - Інформація про те, як центр безпеки Google Workspace може забезпечити розширену аналітику та підвищити видимість проблем безпеки
  - Інформація про те, як можна використовувати інструмент розслідування безпеки для виявлення та вирішення проблем безпеки та конфіденційності за допомогою звітів на інформаційній панелі, інструменту розслідування та сторінки стану безпеки

Навчайте вчителів, співробітників та учнів

- Поради від Google щодо безпеки та захисту в Інтернеті в Центрі безпеки Google
- Допомагаємо дітям бути безпечними та впевненими дослідниками онлайн-світу
- Khan Academy пропонує безкоштовні онлайн-курси, зокрема з безпеки в Інтернеті



Google for Education