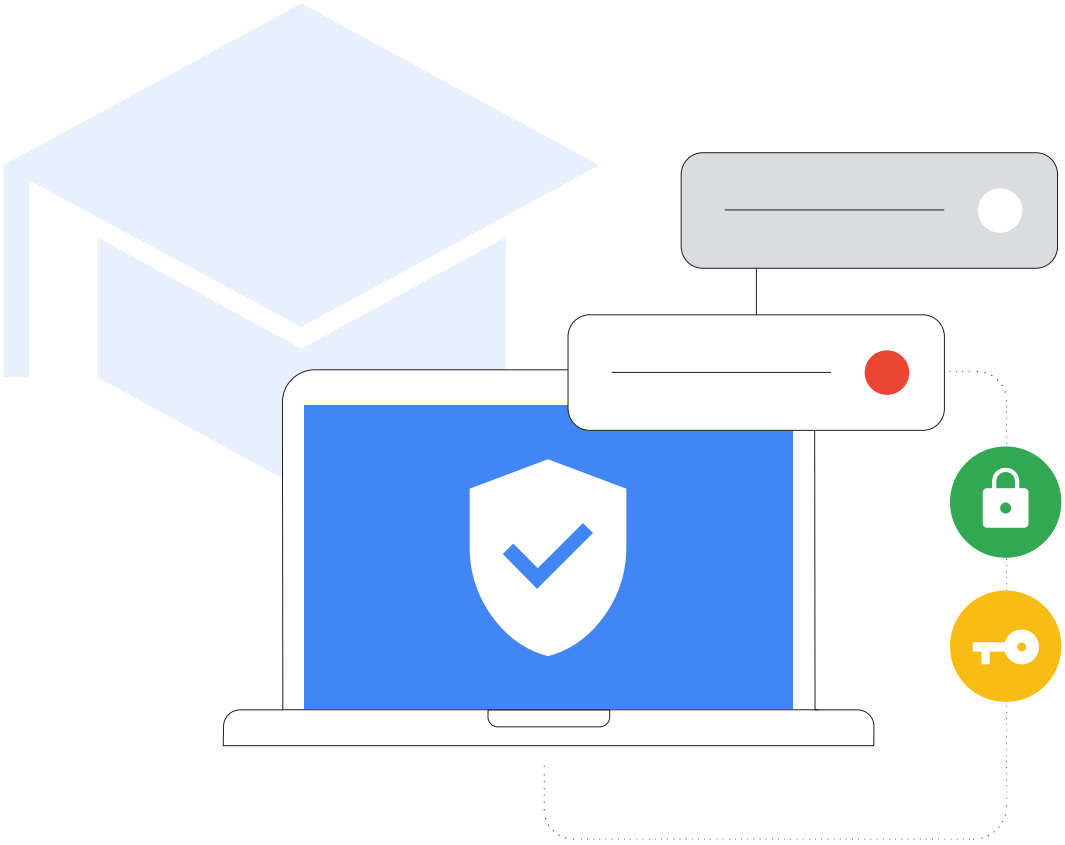
Google for Education

K-12 사이버 보안 가이드북

2023년 8월에 업데이트된



Safer with Google

위험 요소

요약

CISA의 우리의 미래를 보호하는 방법(Protecting Our Future) 보고서에서 강조했듯이 K-12 교육 기관에서 학생, 가족, 교사, 교직원, 지역사회를 보호하기 위해 사이버 보안에 투자하는 것은 매우 중요합니다. 이 가이드에서는 K-12 교육 기관의 사이버 보안을 강화하기 위해 학교 IT 관리자에게 하드웨어와 소프트웨어를 설정하고 구성하는 방법에 대한 안내와 권장사항을 제공합니다. 이 가이드에는 일반적인 권장사항과 Google 제품 및 서비스에 대한 구체적인 안내가 모두 포함되어 있습니다. 전 세계의 정보를 체계화하여 누구나 쉽게 액세스하고 유용하게 사용할 수 있도록 한다는 Google의 사명은 Google for Education팀에서 수행하는 작업인 교육 및 학습용 도구의 설계 및 구축을 위한 중요한 원동력입니다. 이 가이드를 통해 해당 작업에서 얻은 교훈을 공유하고자 합니다.

이 가이드에서는 구성, 설정, 위험 감소 전략을 더욱 심층적으로 살펴볼 수 있는 주제별 보안 권장사항을 제공합니다. 또한 Google이 Google 서비스, 특히 교육용 도구를 위한 사이버 보안에 어떻게 접근하는지에 대해서도 설명합니다. 이 가이드에서는 제품이나 서비스에 관계없이 자세한 안내를 제공하지만, Google 제품은 기본적으로 일반적인 공격에 대해 별도의 구성이나 기능을 추가하지 않아도 그 차제로 탁월한 보호기능을 제공 하고 있습니다.

위험 요소

교육 기관은 사이버 공격의 주요 표적으로, 악의적인 공격 자는 자신의 이익을 위해 학교의 풍부한 데이터 환경을 악용하려고 합니다. 아직 사이버 공격을 받은 적이 없는 학교의 46%가 공격이 점점 더 교묘해지고 방어하기 어려워지고 있기 때문에 결국 표적이 될 것이라고 예상합니다. 그리고 이러한 학교의 42%는 랜섬웨어가 너무 광범위하게 퍼져 있어 공격을 *제어할* 수 없다고 생각합니다. 2020년에 학교가 원격 교육으로 빠르게 전환해야 하는 상황으로 인해 사이버 보안 공백이 불가피하게 발생하면서 학교는 공격에 취약하게 되었습니다.

방어

이러한 공격에 따른 영향은 줄일 수 있습니다. 위험을 완전히 제거하는 기술은 존재하지 않지만 교육 부문과 에듀테크 공급업체가 협력하여 권장사항을 채택하고 구현함으로써 위험을 크게 줄일 수 있는 안전하고 포괄적인 접근 방식을 고안할 수 있습니다. 교육 기관은 사용자와 기기를 보호하고, 데이터 개인 정보 보호를 보장하는 적절한 예방 조치와 정책을 마련하여 위험을 보다 효과적으로 관리하고 공격에 따른 영향을 줄일 수 있습니다.

주요 권장사항:

- **보안 인증 사용:** 민감한 정보를 안전하게 보관하고, 이메일, 파일을 비롯한 콘텐츠를 보호하며, 권한이 없는 사용자가 교육 시스템에 액세스하는 것을 방지합니다. 가능하다면 안전한 비밀번호와 2단계 인증(2SV), 패스키, 비밀번호 관리자 등 사용자 인증 권장사항을 사용하세요. 이는 특히 민감한 정보를 다루는 IT 관리자와 교직원의 경우 매우 중요합니다.
- **적절한 보안 설정 적용:** 사용자, 데이터 및 환경을 안전하게 보호합니다. Google 제품은 기본적으로 안전하게 구축되어 있지만, 관리자가 네트워크와 시스템을 적절히 활용하고 구성하여 보안을 유지하는 것도 중요합니다. 학교의 보안을 유지하려면 제로 트러스트와 최소 권한 원칙을 적용하세요. 즉, 사용자는 업무를 효과적으로 수행하는 데 필요한 소프트웨어, 데이터, 애플리케이션, 시스템에만 액세스 해야 합니다.
- **시스템 업데이트 및 업그레이드:** 최신 위협으로부터 사용자를 보호합니다. 최신 운영체제(OS)와 브라우저를 사용하고, 사용자가 모든 기기에서 최신 소프트웨어 버전(또는 승인된 장기 안정화 버전)을 실행하고 있으며 자동으로 업데이트하는지 확인합니다. Chromebook과 같은 더욱 안전한 솔루션으로 업그레이드하면 보안을 강화할 수 있습니다. 지금까지 어떤 ChromeOS 기기에서도 랜섬웨어가 발견된 적이 없습니다.
- **실시간 알림 및 모니터링 시스템 사용:** 보안 상태를 강화하고 잠재적인 문제를 신속하게 완화합니다. Google Workspace for Education 과 같은 기본 공동작업 및 커뮤니케이션 소프트웨어에 내장된 이러한 기능을 사용하거나 별도의 보안 로깅 및 모니터링 솔루션을 배포할 수 있습니다. 학교 네트워크, 기기, 애플리케이션, 사용자, 데이터 전반의 활동을 포괄적으로 추적하고, 계정 로그인, 파일 공유, 이메일 크기(특히 피싱 및 멀웨어 시도), 기기 활동 및 구성 변경사항을 모니터링하고, 알림 및 모니터링 솔루션을 최신 상태로 유지하여 위협, 중요 이벤트 및 시스템 변경사항에 대한 알림을 받으세요.
- **교사, 교직원, 학생을 위한 보안 교육 실시:** 기기와 소프트웨어를 안전하게 사용하고, 잠재적인 위협을 인식 및 보고하며, 데이터를 적절히 공유하여 가장 일반적인 공격으로부터 보호하는 방법에 대해 교육합니다. 학교나 교육구는 무료로 제공되는 기존의 자료를 사용해 자체적으로 교육 자료를 만들어 학교를 위한 종합적인 툴킷으로 제작할 수 있습니다.

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

Google 제품 사용자를 위한 권장사항:

Google Workspace for Education 및 Chromebook과 같은 Google 제품을 사용하면 학교의 사이버 보안을 강화하고 이러한 각 권장사항을 쉽게 구현할 수 있습니다. 이 러한 제품들은 사용자 개인 정보를 보호하고 교육 기관에 동급 최고의 보안을 제공하는 포괄적인 솔루션을 제공할 수 있습니다.

이러한 전략은 다음 자료에서 제공하는 추가 안내와 함께 K-12 교육 기관의 보안을 위한 훌륭한 기반이 됩니다.

교육에 대한 Google의 접근 방식

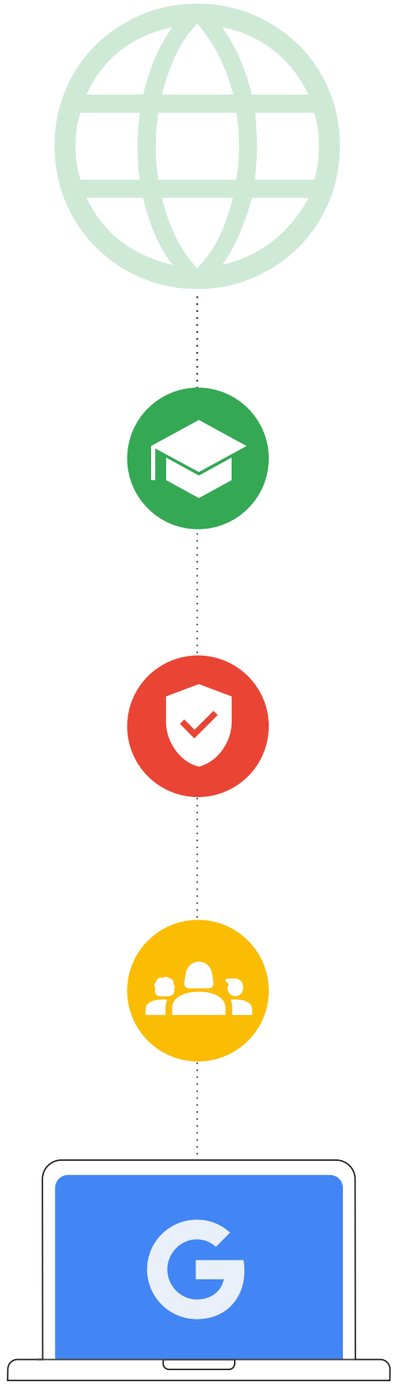
Google의 목표는 전 세계 정보를 체계화하여 모두가 편리하게 이용할 수 있도록 하는 것으로, 이는 교육 분야에서도 마찬가지입니다. Google for Education팀에서는 이를 실현하기 위해, 학생과 교사가 간편하고 안전하게 자신의 콘텐츠를 제작하여 공유하고 정리하며 교육 리소스 및 온라인 도구에 액세스하고 사용할 수 있도록 지원하는 Chromebook 및 Google 클래스룸과 같은 도구를 구축하고 있습니다.

학교는 기본적으로 보안이 유지되고, 설계상 개인 정보가 보호되며, 사용자가 제어할 수 있고, 신뢰할 수 있는 콘텐츠와 정보를 제공하는 기술이 필요합니다. Chromebook 및 Google Workspace for Education과 같은 제품을 통해, 학교는 최고의 글로벌 교육 표준을 준수하는 동급 최강의 보안을 확보하고, IT 관리자는 데이터와 보안 정책을 완벽하게 파악하고 손쉽게 제어할 수 있으며, 학생은 연령 기반 콘텐츠를 제공하고 스팸과 사이버 위협을 완화하는 안전한 디지털 환경에서 학습에 몰입할 수 있습니다.

우리는 모든 사람의 안전한 학습을 보장하기 위해 기본 보안 기능 및 제어, 최고 수준의 개인 정보 보호 표준, 더욱 능동적인 보안 도구 옵션에 우선순위를 두었습니다. ChromeOS 기기는 학교가 직면한 위협을 줄이 는 데 도움이 되며 학교의 가장 큰 위협인 랜섬웨어에 대한 최고의 방어 수단으로서, 지금까지 Chromebook을 공격하는 데 성공한 랜섬웨어는 없었습니다.

한편 Google Workspace for Education은 세계에서 가장 많이 사용되고 안전한 클라우드 기반의 커뮤니케이션 및 공동작업 제품군 중 하나입니다. 여기에 설명된 권장사항과 관련하여 각각이 사이버 보안을 보호하는 방법에 대한 자세한 내용은 마지막 섹션을 참고하세요.

이 자료는 제품에 관계없이 K-12 교육 기관을 위한 실용적이고 일반적인 보안 지침을 설명하는 첫 번째 섹션과 Google Workspace for Education 및 Chromebook과 같은 Google for Education 제품을 사용하는 교육 기관을 위한 구체적인 구성 안내를 설명하는 두 번째 섹션으로 나누어져 있습니다. 두 섹션 모두 온라인에서 여러분과 학생을 안전하게 보호하는 데 도움이 되는 정보를 제공합니다.



도입

K-12 교육 기관은 기기와 네트워크 모두 사이버 공격에 노출될 위험이 높습니다. K-12 교육 기관은 학생을 보호하고 이러한 공격으로 인해 발생할 수 있는 데이터, 서비스, 리소스, 시간, 비용의 손실을 방지하기 위해 가능한 최고의 보안을 적용해야 합니다. (Source)

이 가이드는 학교 관리자와 학교 시스템이 환경에 대한 보안을 강화하기 위해 구현할 수 있는 사이버 보안 권장사항을 홍보하기 위한 도구입니다. K-12 교육 기관은 이러한 권장사항을 구현함으로써 교육 시스템에 대한 심각하고 많은 비용이 발생하는 사이버 공격을 완화하거나 예방하고 학생, 가족, 교사, 교직원을 보호할 수 있습니다.

학교를 대상으로 한 사이버 공격의 빈도와 심각성이 증가하고 있습니다. K-12 사이버 보안 리소스 센터(K-12 Cybersecurity Resource Center)에 따르면 2016년부터 2021년까지 미국 50개 주의 교육 기관에서 발생했다고 보고된 사이버 사고가 1,300건 이상이었습니다. 오늘날의 교육 지도자는 학생, 교사, 교직원의 데이터와 개인 정보는 물론 교육 기관의 시스템과 정보를 보호해야 합니다. 이것은 힘든 과제이며, 특히 교육 분야가 전통적으로 다른 분야에 비해 최신 사이버 보안 기술을 따라가는 데 어려움을 겪었다는 점을 고려하면 더욱 그렇습니다.

랜섬웨어, 피싱, 멀웨어 등 사이버 공격이 성공하면 개인 식별 정보(PII)의 대규모 유출, 막대한 요구액(2020년 이후 평균 요구액이 5배 증가하여 812,260달러에 달함)으로 이어질 수 있으며 교육 및 기타 학교 운영에 장기간 차질이 발생할 수 있습니다. 최근 랜섬웨어 공격으로 학교 시스템 전체가 중단되어 학생이 며칠 동안 학교에 갈 수 없게 되면서 지역사회 전체에 큰 여파가 있었습니다. K-12는 제한된 리소스와 예산으로 인해 사이버 보안 강화를 위한 투자가 이루어지지 않는 한 계속해서 주요 공격 대상이 될 것입니다.

사이버 보안은 항상 커뮤니케이션, 협업, 파트너십을 통해 가장 잘 이루어집니다. 이 가이드는 Google의 안전 및 보안 팁, 미국 국립표준기술연구소(NIST)의 사이버 보안 프레임워크, 2023년 CISA K-12 사이버 보안 툴킷 및 권장사항 등 널리 활용되고 있는 사이버 보안 지침을 바탕으로 작성되었습니다. 이 가이드에서는 IT 관리자가 취하거나 고려해야 하는 일반적인 단계, Google 제품의 권장사항 및 지침에 대해 설명하며다른 회사에서 제공하는 보안 팁 및 서비스도 참조합니다. 관리자는 관련 회사에서 제공하는 모든 보안 지침을 검토하고 최신 지침을 실행해야 합니다. 담당 회사가 자사 제품 및 변경사항을 가장 잘 설명할 수 있기 때문입니다.

아래 나열된 권장사항에 따라 조치를 취하기 전에 다음 요소도 고려해야 합니다.

고려사항:

1. **학생 보호.**
   학교마다 요구사항이 다르며 일부 학생의 경우 보안 및 개인 정보 보호를 위해 추가 조치가 필요할 수 있습니다. 많은 에듀테크 도구가 부적절한 콘텐츠를 제한하거나 위치 및 연락처 데이터를 비공개로 설정하는 등 연령별 액세스 지원 기능을 제공합니다.
2. **저장하는 데이터 유형:**
   민감한 정보를 저장하는 경우 그러한 데이터를 암호화하거나 별도의 위치에 저장해야 합니다.
3. **사용하는 기기의 유형 및 배포 모델:**
   기기와 애플리케이션은 자동 업데이트를 통해 보안을 극대화하고, 데이터를 암호화하고, 계정을 격리하여 사용자가 자신의 정보에만 액세스할 수 있도록 해야 합니다.
4. **학교, 교육구 또는 지역 정책:**
   학교에 따라 기술 사용에 관한 특별한 정책을 두고 있을 수 있습니다. 이러한 정책에 따라 모든 보호 수단이 설정되어 있는지 확인해야 합니다.

Gmail 에서 매일
1억
건의 피싱 시도 차단

Google 에서 매주
30만
개의 안전하지 않은 웹사이트 식별

7,400만
Google 비밀번호 관리자에서 도움을 받는 일일 사용자 수 7,400만 명

7억
명의 사용자가 매년 보안 진단으로 보안 강화

일반 보안 지침

보안 인증 사용

보안 인증은 학교 및 기타 기관의 최우선 순위가 되어야 합니다. 2022년 4분기에는 사용자 인증 정보가 취약하거나 아예 없는 계정에서 전체 침해 사고의 48%가 발생했습니다. 몇 가지 주요 권장사항을 구현하면 사용자가 본인이 맞는지 확인하고 각 사용자의 역할에 적합한 정보로 액세스를 제한하는 데 도움이 될 수 있습니다.

IT 관리자는 2단계 인증(2SV 또는 2FA라고도 함)을 사용하고, 가능하면 패스워드리스 인증(즉, 패스키)으로 전환하도록 해야 하며, 특히 교육 기관의 시스템에 원격으로 액세스할 때는 이러한 보안 인증이 더욱 필요합니다. 2단계 인증은 온라인 계정에 보안 레이어를 추가하여 공격자가 액세스하기 훨씬 더 어렵게 만듭니다.

오늘날 학교에서 사용하는 기기 유형과 배포 모델은 매우 다양하며 K-12 환경의 기술 숙련도도 다양합니다. 계정 및 기기의 보안은 IT 관리자, 교사 및 교직원, 할당된 기기를 사용하는 고학년 학생, 공유 기기를 사용하는 저학년 학생과 같은 사용자 역할과 유형에 따라 다르며, 이에 따라 정의된 권장사항도 다릅니다. 각 그룹에 대한 구체적인 권장사항은 아래에서 설명합니다.

대부분의 설정에서 권장사항으로 사용되는 여러 종류의 인증 방법이 있습니다.

- **안전한 비밀번호:**
  처음으로 로그인할 때 사용자에게 직접 비밀번호를 생성하도록 메시지를 표시하고, 길이와 복잡성에 있어 최소한의 기술 요구사항을 준수하도록 합니다. 암호가 길면 길이와 사용되는 복잡한 문자로 인해 보안 요소가 추가됩니다. 사용자에게 정기적으로 비밀번호를 변경하도록 요구하면 더 간단한 비밀번호를 사용하거나 한 글자만 업데이트하는 등 무의미하게 변경하도록 유도할 수 있기 때문에 바람직하지 않습니다.
- **2단계 인증(2SV):**
  단계 인증은 일회성 인증 코드를 생성하는 휴대전화의 앱이나 보안 키 등 사용자가 소지하고 있는 것을 통해 2단계로 계정을 보호합니다. 어떤 형태의 2단계 인증을 사용하든 계정 보안은 강화되지만, 관리자는 전화번호 기반 공격에 취약할 수 있는 문자나 전화로 전송되는 인증 코드는 사용하지 않아야 합니다.
- **패스워드리스 인증:**
  패스키는 비밀번호를 대체하는 더 안전하고 간편한 방법입니다. 사용자는 PIN, 패턴, 생체 인식 센서(지문 또는 얼굴 인식 등) 또는 보안 키 탭을 사용하여 앱과 웹사이트에 로그인할 수 있으므로 비밀번호를 기억하고 관리할 필요가 없습니다. 이 방법은 모든 교육 환경에 적합한 것은 아니지만, 점차적으로 기존의 인증 방식을 대체하고 있으며 더 안전하고 빠른 로그인을 가능하게 하고 있습니다. 패스키는 등록된 웹사이트와 앱에서만 작동하므로 피싱 공격으로부터 사용자를 보호합니다.
- **싱글 사인온(SSO):**
  SSO를 사용하면 사용자는 하나의 사용자 인증 정보로 여러 애플리케이션과 웹사이트에 액세스할 수 있습니다. 사용자가 하나의 사용자 인증 정보 세트만 기억하면 되기 때문에 각각의 인증 정보를 일일이 적어둘 필요가 없습니다. 또한 학교에서는 여러 사용자 인증 정보 세트를 관리할 필요가 없으므로 IT 지원 및 헬프 데스크 비용을 절감할 수 있습니다. Google Workspace for Education은 기본적으로 SSO를 지원하므로 사용자는 Google 계정 사용자 인증 정보를 사용하여 서드 파티 애플리케이션에 로그인하거나 다른 제공업체의 사용자 인증 정보를 사용하여 Google 계정에 로그인할 수 있습니다.
- **비밀번호 관리자:**
  비밀번호 관리자는 사용자가 학교와 회사에서 사용하는 계정과 서비스 전반에 걸쳐 안전하고 고유한 비밀번호를 생성하도록 도와줍니다(SSO를 사용하지 않는 경우). 기기의 운영체제에 로그인하는 데는 도움이 되지 않지만, 사용자가 로그온한 후에는 비밀번호를 관리할 수 있습니다. Google 사용자는 모든 플랫폼의 Chrome, ChromeOS, Android에서 비밀번호 관리자를 사용할 수 있습니다.

다양한 그룹의 고유한 요구사항은 교육 기관 내 각 사용자의 역할, 액세스 권한이 있는 시스템 및 데이터의 종류, 연령에 따라 이러한 인증 방식의 특수한 하위 집합 또는 여러 방식의 조합을 통해 대응할 수 있습니다.

학교 관리자

관리자는 모든 K-12 교육 기관의 시스템과 대부분의 데이터를 제어합니다. 계정 보호는 인프라부터 계정 데이터, 교육 기관에서 관리하는 기기에 이르기까지 전체 시스템 보안의 핵심입니다. 따라서 안전한 비밀번호, 강력한 비밀번호 관리자, 2단계 인증을 사용하는 등 가장 효과적인 인증 표준을 채택해야 합니다. 이들 각각은 함께 사용할 경우 보호 레이어를 추가해 관리자 계정과 엔터프라이즈 서비스에 가장 강력한 보안을 제공합니다.

- 관리자는 실물 보안 키를 사용하거나, 신뢰할 수 있는 기기와 프롬프트 및 암호화를 통해 보안이 유지되는 2단계 인증을 사용해야 합니다. 여기에는 Google OTP 또는 일회성 인증 코드를 생성하는 기타 앱과 같은 서비스가 포함됩니다. 2019년 이후에 출시된, TPM 칩 이 탑재된 Chromebook에는 2단계 인증에 사용할 수 있는 전원 버튼이 포함되어 있습니다.
- 관리자는 2단계 인증을 지원하는 신뢰할 수 있는 비밀번호 관리자를 사용하여 각기 다른 서비스에 사용하는 여러 비밀번호를 저장해야 합니다.

할당된 기기를 사용하는 교사 와 교직원

교사와 교직원도 관리자와 마찬가지로 민감한 데이터에 액세스할 수 있지만 디지털 인프라를 제어하지는 않으며 기술 숙련도에 있어서도 개인별 차이가 있습니다.

- Chromebook을 사용하는 교사와 교직원에게는 법적으로 허용 된 경우 디지털 지문과 같은 생체 인식 인증으로 로그인할 수 있는 옵션을 제공해야 합니다.
- 관리자는 가능한 경우, 그리고 교직원이 교육 기관의 시스템에 원격으로 액세스할 때는 반드시 2단계 인증을 사용하게 하고 패스워드리스 인증으로 전환해야 합니다.

할당된 기기를 사용하는 고학년 학생 (보통 4학년 이상)

고학년 학생일수록 자신을 보호하는 방법에 대해 더 잘 알고 있으며 일반적으로 사용하려는 서비스 유형에 적합한 더 안전한 인증 메커니즘을 사용할 수 있습니다. 그들은 자신의 계정 및 자신과 공유된 정보에만 액세스할 수 있어야 합니다.

- Chromebook을 사용하는 학생에게는 해당 기기에서 빠르게 로그인하도록 기기별 PIN을 생성할 수 있는 옵션이 제공되어야 합니다. 생체 인식 옵션은 많은 학교 환경에서 적절하지 않거나 실현 가능하지 않을 수 있습니다.
- 모든 학생은 개인 정보(예: 이름, 학급, 생일)가 포함되지 않은 고유한 비밀번호를 만들 수 있도록 도움 이 필요합니다. 학생들에게 암호를 사용하면 비밀번호를 복잡하면서도 기억하기 쉽게 만들 수 있다는 것을 알려주어야 합니다.

공유 기기를 사용하는 저학년 학생 (일반적으로 유치원~3학년)

어린 학생은 아직 교육용 기술을 사용하는 방법을 배우는 단계이므로 제한된 서비스와 데이터를 사용하는 데 적합한 간단한 인증을 사용 할 수 있습니다.

- 저학년 학생과 비밀번호로 로그인할 수 없는 학생을 위해 QR 코드나 사진 로그인과 같이 서드 파티의 비밀번호 대체 수단을 사용하는 학교는 보안이 취약하므로 보안을 위한 예방 조치를 마련해야 합니다. 관리자는 코드가 분실되거나 다른 사람에게 노출된 경우 학생의 비밀번호를 수정하고 코드를 업데이트해야 합니다.
- 학교는 비밀번호를 비공개로 유지하고 QR코드와 같은 대체 사용자 인증 정보를 안전하게 보관하는 것의 중요성에 대해 학생과 학부모 모두를 교육해야 합니다.
- 태블릿과 같이 할당된 기기의 경우 기기별 PIN을 대체 보안 인증 방법으로 사용할 수 있습니다.

적절한 보안 설정 적용

학교 기기와 네트워크는 전 세계 공격자의 눈에 잘 띄고 가치가 높은 표적이므로 서비스, 리소스, 시간, 비용의 손실을 방지하기 위해 가능한 한 최고의 보안을 적용하는 것이 중요합니다. 시스템 관리자는 교육 기관에서 사용하는 제품에서 사용 가능한 효과적이고 적절한 보안 기능을 구현해야 하지만 동시에 교사, 교직원, 학생이 이러한 시스템을 쉽게 사용할 수 있도록 해야 합니다. 중요한 보안 및 개인 정보 보호 설정은 개별 사용자가 중지하거나 수정할 수 없도록 구성해야 하며, 기타 설정은 관리자가 설정한 기본 보호 설정을 사용해야 합니다. 서비스, 리소스, 시간, 비용의 손실을 방지하기 위해 가능한 한 최고의 보안을 적용하는 것이 중요합니다. Chromebook을 사용하는 경우 마지막 섹션에서 기기 정책 설정에 대한 권장사항을 확인할 수 있습니다.

마지막으로, 서비스 제공에 합리적으로 필요하고 비례하는 수준으로 또는 관계의 맥락에 부합하는 것으로 개인 정보의 수집, 사용, 공개의 목적과 수단을 제한하여 '데이터 수집 최소화'를 보안 관행에 반영하세요.

애플리케이션 및 업데이트

기기에 설치된 모든 애플리케이션은 악용될 수 있는 잠재적인 공격 벡터이므로 사용자가 설치할 수 있는 애플리케이션을 제한하고 최소화하세요. 가능하면 신뢰할 수 있는 소스의 애플리케이션을 사용합니다. 예를 들어 사용자에게 Google Play 스토어에서 인증 배지를 확인하여 사용자가 보안 검토를 거친 공식 애플리케이션을 다운로드하도록 권장합니다. 모든 OS 또는 하드웨어 수정(탈옥 또는 루팅)은 심각한 보안 결함을 초래할 수 있으므로 피해야 합니다.

액세스 및 가시성

관리자는 사용자가 업무를 수행하거나 효과적으로 학습하는 데 필요한 데이터, 소프트웨어, 서비스, 시스템에만 액세스할 수 있도록 해야 합니다. 이렇게 하면 의도하지 않은 액세스를 제한하고 누가 어떤 리소스에 액세스할 수 있는지 추적하는 데 도움이 됩니다. 학교 소유 기기에 대한 액세스를 제한하고 특정 교직원만 액세스할 수 있도록 하여 어떤 사용자가 어떤 상황에서 데이터에 액세스할 수 있는지 감사함으로써 사용자 개인 식별 정보 및 시스템(예: 인사 관리, 급여, 평가, 보안 및 구성)과 같이 매우 민감한 정보에 특별한 주의를 기울여야 합니다.

공동작업 도구에서 데이터 공유 정책을 검토하여 부적절하거나 과도한 공유 또는 승인되지 않은 액세스를 방지합니다. 기관 외부에서의 공유를 제한하거나 차단하고 (특히 학생의 경우) 민감한 콘텐츠의 공유를 모니터링하는 정책을 사용합니다.

기기 분실 또는 도난

기기를 분실하더라도 데이터는 잃어버리지 않을 수 있습니다. 관리자는 클라우드 환경에 문서를 보관하는 등 기기를 분실하거나 도난당한 경우 정보 및 문서에 액세스할 수 있는 계획을 표준화해야 합니다. 계정 액세스 중단을 방지하기 위해 2단계 인증 프로세스에 대한 복구 코드를 다운로드하여 인쇄하세요.

기기 분실 또는 도난 신고가 접수되면 가능한 경우 해당 기기를 원격으로 잠그고, 관련 계정을 잠그거나 플래그를 지정하여 무단 액세스에 사용되지 않도록 합니다. Chromebook을 분실한 경우 원격으로 초기화할 수 있으며 의심스러운 활동이 있는지 Google Workspace for Education 계정을 모니터링하거나 필요한 경우 일시 중지 (잠금)할 수 있습니다.

고위험 사용자를 위한 고급 보호 기능

눈에 잘 띄고 민감한 정보가 있는 사용자(Google Workspace for Education 관리자 포함)를 위해 Google은 고급 보호 프로그램(APP)을 제공합니다. APP는 피싱 시도, 유해한 다운로드 및 비밀번호 유출과 같은 표적 공격으로부터 사용자를 추가로 보호합니다. APP는 Google 계정에 대한 온라인 표적 공격을 차단하도록 특별히 설계되었으며, 강력한 인증 및 보안 키를 자동으로 사용하고 계정 데이터에 대한 서드 파티 액세스를 제한합니다. 다른 온라인 계정 제공업체에서도 고위험 사용자를 위한 강력한 계정 보호 기능을 제공하며, 관리자와 교직원은 개인 정보 또는 기술 시스템에 액세스할 때는 항상 이러한 기능을 사용해야 합니다.

시스템 업데이트 및 업그레이드

Bland 자신을 보호하기 위해 할 수 있는 가장 중요한 일 중 하나는 기기 운영체제와 애플리케이션을 최신 상태로 유지하는 것입니다. K-12 교육 기관은 자녀의 교육과 일상 생활에서 매우 중요한 부분을 차지하기 때문에 이 점이 더욱 중요합니다. 솔라윈즈(SolarWinds), 로스앤젤레스 통합 교육구 랜섬웨어 공격, 리틀락 교육구 해킹, Microsoft Exchange Server 정보 유출, 앨버커키 교육구 랜섬웨어 공격, 최근 발생한 Microsoft 연방 기관 유출 등 교육 환경과 기타 고위험 환경에서 발생한 대부분의 멀웨어 공격은 Windows 기반이었습니다. 클라우드 제품 및 서비스를 사용하면 공격 표면을 줄이고 시스템과 애플리케이션을 최신 상태로 유지하는 것이 자동화되어 관리자의 작업을 더 쉽게 할 수 있습니다.

최신 운영체제로 업그레이드하고 최신 상태 유지

운영체제(OS)의 최신 버전에는 일반적으로 알려진 공격 벡터를 차단하는 데 도움이 되는 새로운 보안 기능이 포함되어 있습니다. 기기 OS 내에서 자동 업데이트 기능을 사용 설정하거나 자동 업데이트가 불가능한 경우 신뢰할 수 있는 공급업체로부터 최소 한 달에 한 번 패치와 업데이트를 다운로드하여 설치하세요.

Chromebook은 ChromeOS에서 실행되므로 최신 보안 패치가 자동으로 자주 업데이트되어 최신 보안 기술을 빠르게 적용할 수 있으며 부팅하기 전에 읽기 전용 운영체제의 무결성을 확인합니다. 또한 기기에 저장된 모든 데이터를 암호화하여 무단 액세스로부터 보호하고 모든 웹페이지와 애플리케이션을 별도의 샌드박스에서 실행하므로 하나의 웹사이트나 앱이 멀웨어에 감염되더라도 기기의 다른 부분으로 확산되지 않습니다.

학교에서 아직 Chromebook으로 전환할 준비가 되지 않았다면 학교 기기의 현대화를 위해 설계된 ChromeOS Flex 버전을 사용하세요. ChromeOS Flex는 능동적인 보안 기능을 기본으로 제공하고 클라우드 기반 관리 기능을 갖춘 통합된 최신 교육 및 학습 환경을 모두에게 제공합니다. Flex는 기존 하드웨어 교체 없이 자동화된 보호 기능을 제공하고 악성 실행 파일과 앱을 차단할 수 있습니다.

최신 브라우저로 업그레이드하고 최신 버전 유지

최신 브라우저를 사용하고 안전하게 유지하는 것은 매우 중요합니다. 최신 브라우저는 고급 보안 기능을 제공하며 사용자가 쉽게 사용 설정하거나 관리자가 기관의 컴퓨터에서 이러한 기능을 기본적으로 사용하도록 구성하여 인터넷을 통해 전송되는 민감한 정보의 기밀성을 보호할 수 있습니다. 브라우저를 최신 상태로 유지 하는 것이 중요합니다. 업무, 학습 또는 기타 온라인 활동 중에 업데이트된 최신 브라우저를 사용하면 다음과 같은 이점이 있습니다.

- **강력한 보안 기능:** 사이트 격리 및 세이프 브라우징 보호 등 강력한 보안을 사용하여 사용자가 실수로 위험한 웹사이트로 이동하는 것을 방지합니다.
- **자동 업데이트 활성화:** 브라우저에 보안 업데이트가 빠르게 적용되도록 합니다.
- **연결이 안전한지 확인:** 최신 브라우저는 전송 계층 보안을 사용해야 하며, 사용자는 URL 옆을 클릭하여 연결이 보안으로 표시되어 있는지 확인할 수 있습니다.

Chrome은 보안을 염두에 두고 개발되어 세이프 브라우징과 같은 기본적으로 활성화된 보안 기능이 사용 설정되어 있습니다. 또한 웹을 탐색할 때 비밀번호를 자동 완성하는 비밀번호 관리자가 통합되어 있어 안전한 비밀번호를 쉽게 관리 할 수 있습니다.

실시간 알림 및 모니터링 시스템 사용

실시간 알림 및 모니터링 시스템은 피해가 발생하기 전에 위협을 신속하게 식별하고 대응할 수 있도록 도와줍니다. 보안 도구가 백그라운드에서 실행되어 시스템 전반에서 보안 관련 활동을 수집하고 로깅하도록 하는 것이 중요합니다. AI 도구는 특히 수집된 대량의 데이터를 선별하고 이상 징후와 패턴을 찾아내는 데 탁월하며, 이를 통해 위협을 더 빠르고 쉽게 탐지하고 취약점을 처리하고 해결할 수 있습니다. 이를 통해 IT 관리자나 교직원은 검토해야 하는 활동의 우선순위를 정할 수 있습니다.

학교에서는 Google Workspace for Education과 같은 기본 공동작업 및 커뮤니케이션 소프트웨어에 내장된 알림과 모니터링 기능을 사용하거나 별도의 보안 정보 및 이벤트 관리(SIEM) 솔루션을 배포할 수 있습니다.

실시간 알림 및 모니터링 시스템은 사용자 로그인, 파일 액세스, 잠재적 침입, 데이터 도난 또는 시도, 관리자 활동 등 학교 네트워크, 기기, 애플리케이션, 사용자 및 데이터 전반의 다양한 활동을 추적할 수 있습니다.

시스템에서 의심스러운 활동을 감지하면 학교의 IT 직원에게 알림을 보낼 수 있습니다. 이를 통해 관리자는 문제를 조사하고 위협을 완화하기 위한 조치를 취할 수 있습니다.

또한 알림 및 모니터링 도구를 사용하여 학교가 직면한 위협에 대해 더 깊이 파악할 수 있습니다. 학교는 이러한 실시간 시스템의 데이터를 분석하여 트렌드와 패턴을 식별해 스스로를 더 잘 보호할 수 있습니다.

다음은 알림 및 모니터링(SIEM 포함) 시스템 사용에 대한 몇 가지 권장사항입니다.

1. **보안 목표 정의하기**
   어떤 정보와 시스템이 학교에 가장 중요한지, 어떤 유형의 위협이 가장 큰 위험을 초래하는지 확인합니다. 그런 다음 이러한 위협을 모니터링하기 위해 수집해야 하는 데이터를 식별합니다.

2. **올바른 데이터 수집 및 적절한 구성**
   가장 관련성이 높은 보안 목표를 달성할 수 있도록 올바른 데이터를 수집하고 애플리케이션을 구성하는 것이 중요합니다. 여기에는 방화벽, 콘텐츠 필터, 침입 감지 시스템, 웹 서버 및 기타 보안 기기와 커뮤니케이션 및 공동작업 소프트웨어, 학교 정보 시스템 및 학습 관리 시스템의 데이터가 포함될 수 있습니다.

3. **알림 조사 및 응답**
   모니터링 시스템에서 알림이 발생하면 문제를 조사하고 적절한 조치를 취하는 것이 중요합니다. 여기에는 여러 팀에 연락하여 알림의 출처를 조사하고, 잘못 발생한 알림인지 확인하거나, 계정 사용 중지, 사용자 비밀번호 재설정, 이메일 격리 또는 삭제, 파일 권한 변경, 기기 완전 삭제 등 위협을 완화하기 위한 조치를 취하는 것이 포함될 수 있습니다.

교사, 교직원, 학생 교육

K-12 교육 기관은 사용자에게 권한을 부여할 수 있도록 캠페인과 파트너십을 통해 학교 커뮤니티의 보안 인식과 습관을 개선해야 합니다. 교사, 교직원, 학생에게 보안의 중요성에 대해 교육하는 것은 온라인에서 스스로를 보호하고 심각한 사이버 보안 위협을 예방하는 데 매우 중요합니다. 교육 기관 전반에서 제공되는 제품과 서비스를 사용하는 방법, 피싱 이메일과 같은 위협을 발견하고 신고하는 방법, 무엇보다도 이러한 공격을 방지하기 위한 조치를 취하는 방법을 교육하세요. 학교 및 교육구는 사용자에게 권한을 부여할 수 있도록 캠페인과 파트너십을 통해 학교 커뮤니티의 보안 인식과 습관을 개선해야 합니다.

기기 및 소프트웨어를 안전하게 사용하는 방법

관리자는 교사 및 전문가와 협력하여 연령에 맞는 수준의 사이버 보안 교육과정을 개발하여 학생이 기기, 소프트웨어, 시스템의 안전한 사용 방법을 이해하도록 도울 수 있습니다. 학교 나 교육구 자체의 교육 자료를 개발하면 교사와 학생을 위한 권장사항을 상황에 맞게 수정하는 데 도움이 되지만, safety.Google에서 제공되는 Be Internet Awesome이나 Khan Academy의 자료와 같은 기존 자료를 필요에 맞게 수정해 사용할 수도 있습니다. 이러한 프로그램은 사용자가 학교나 커뮤니티 중 어디에 있든 보안을 유지하도록 도와줍니다.

위협 인식

교사, 교직원, 학생에게 위협을 인식하도록 교육하는 것은 안전을 유지하는 데 중요한 부분입니다. 어린 학생 들은 합법적인 것과 그렇지 않은 것을 구 분하기 어려울 수 있으므로 특정 상황이 위협인지 아닌지 구분하는 방법을 가르치는 것이 중요합니다. 아이들은 몇 가지 유형의 위협을 인식하고 신고 방법을 이해해야 하며, 관리자는 투자 대비 효과 적일 것이라고 생각되는 주제에 집중해야 합니다. 중요한 것은 교육을 통해 사용자에게 위협을 인식하는 데 그치지 않고, 인식한 위협에 대해 적절한 조치를 취하도록 가르쳐야 한다는 것입니다. 사용자가 인식해야 하는 일반적인 위협에는 랜섬웨어, 피싱, 소셜 엔지니어링, 멀웨어, 사기가 포함 됩니다. 하지만 특정 교육 기관 내에서 더 자주 발생하는 특정 위협이 있다면, 해당 위협에 대한 교육을 학교 커뮤니티에 제공하는 것이 좋습니다.

안전한 데이터 및 파일 공유

교사와 교직원은 파일 및 데이터의 적절한 공유 방법과 이메일을 통한 부적절한 요청을 인식하는 방법에 대해 교육을 받아야 합니다. 중요한 것은 민감한 개인 정보는 필요한 경우에만 공유하거나 처리하고, 이메일을 통한 공유 또는 외부 당사자와의 공유는 절대 하지 않는 등 데이터에 대한 추가적인 보호 조치를 취해야 한다는 것입니다. 데이터 손실 방지 기능(ChromeOS 및 Workspace for Education에 포함)을 사용하여 최종 사용자가 민감한 정보(예: 주민등록번호)가 포함된 파일을 공유하거나 민감한 콘텐츠를 도메인 외부로 복사하여 붙여넣지 못하도록 경고하고 방지해야 합니다.

Google의 실제 접근 방식: 교육용 기기 및 서비스

소프트웨어 조달은 교육구가 스스로를 보호할 수 있는 강력한 도구 중 하나입니다. 소프트웨어는 레이어마다 보안이 내장되어 취약성 위험을 최소화하도록 견고하게 설계 및 구축되어야 합니다. 보안 소프트웨어 또는 보안 실적이 입증된 회사의 소프트웨어를 구매하도록 학교에 요 청하여 광범위한 사이버 위험을 크게 줄일 수 있습니다. 예를 들어 Google에서는 ChromeOS를 강화하는 동시에 머신러닝, 클라우드 및 신원 확인 전문 지식의 강점을 활용하는 더욱 능동적이고 지능적인 솔루션을 계속해서 제공하고 있습니다.

Google에서는 학생과 교사의 개인 정보를 보호하고 학교에 최고 수준의 보안을 제공할 수 있는 제품을 만들기 위해 최선을 다하고 있습니다. 신뢰할 수 있는 Google for Education 제품 및 서비스가 나날이 복잡해지는 위협으로부터 사용자, 기기, 데이터를 지속적으로 보호해 줍니다. 이 섹션에서는 학교 IT 관리자가 Google for Education 제품을 사용할 때 필요한 보안 권장사항을 안내합니다.

Google Workspace for Education

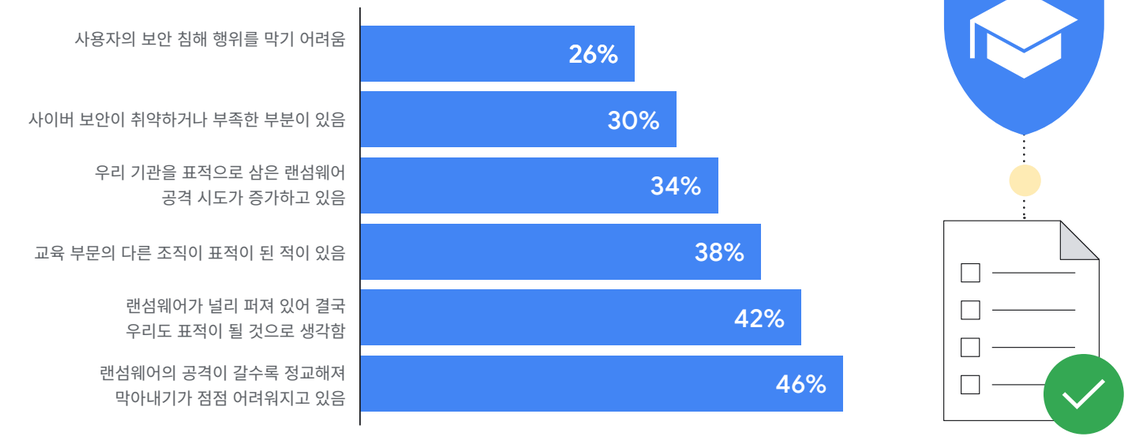
Google Workspace for Education은 학교에 특화된 Google 도구 및 서비스 모음으로, 이를 통해 공동작업을 수행하고 수업 효율성을 높이며 안전한 학습 환경 구축에 사용됩니다. Google for Education 제품 및 서비스는 점점 더 복잡해지는 위협으로부터 사용자, 기기, 데이터를 지속적으로 보호하고 알림 및 보안 센터, 디지털 증거 검색을 위한 vault, ID 및 액세스 관리, 데이터 손실 방지 등의 도구를 제공합니다.

Google Workspace for Education을 처음 사용하는 경우 도움이 필요한 분들을 위한 자료와 이러한 권장사항을 설정하는 데 도움이 되는 가이드도 제공됩니다. Google Workspace for Education을 시작하는 데 도움이 필요하면 이 빠른 시작 IT 설정 가이드를 참조하세요.

보안 체크리스트

보안 체크리스트를 검토하여 기관의 보안 및 개인 정보 보호를 강화하는 방법에 대해 자세히 알아보세요. Google Workspace for Education Standard 및 Plus 버전을 사용하는 학교에서는 보안 상태 페이지를 사용하여 관리 콘솔 설정의 구성을 모니터링할 수도 있습니다. 예를 들어 자동 이메일 전달, 기기 암호화, 드라이브 공유 설정 등과 같은 설정 상태를 확인할 수 있습니다. 필요한 경우 일반적인 보안 가이드라인 및 권장사항을 기반으로 도메인 설정을 조정하면서 조직의 비즈니스 요구사항 및 위험 관리 정책을 고려 여 이 가이드라인을 적용할 수 있습니다.

교육 부문이 공격의 표적이 되리라 예상되는 이유



출처: https://assets.sophos.com/X24WTUEQ/at/q523b3nmgcfk5r5hc5sns6g/sophos-state-of-ransomware-in-education-2021-wp.pdf

다음은 Google Workspace for Education에서 기본적으로 제공하는 보호 기능을 극대화하는 데 도움이 되는 몇 가지 유용한 도움말입니다.

조직 단위(OU) 구성하기

Google Workspace for Education 계정에서 모든 사용자의 설정이 동일해야 한다고 주장하는 사람은 아무도 없습니다. 조직 단위는 사용자별로 다양한 서비스, 설정, 권한을 부여하기 위한 사용자 그룹으로, 예를 들어 교사와 교직원에게는 2단계 인증을 사용하고 저학년 학생에게는 연령에 적합한 인증을 사용할 수 있습니다. 교직원, 교사, 학생을 위한 별도의 조직 단위를 설정하여 각 사용자 그룹에 정책을 개별적으로 적용하세요. Google Workspace for Education 계정을 효과적이고 유연하게 관리하려면 조직 구조를 잘 설계해야 합니다.

비밀번호 정책 및 관리자 계정 보호 기능 설정하기

앞서 설명한 바와 같이 사용자 인증은 교육 기관의 보안을 유지하는 데 있어 매우 중요한 부분입니다. 이에 Google에서는 관리자가 사용자에게 적절하고 안전한 계정 보호 기능을 제공할 수 있도록 관리자용 인증을 유연하게 관리할 수 있는 방법을 마련했습니다. 비밀번호 정책을 설정하여 사용자가 안전한 비밀번호를 만들도록 하고, 보안 로그온 섹션의 권장 그룹에 따라 적절한 경우 2단계 인증을 사용하도록 요구할 수 있습니다. 일부 사용자에게 2단계 인증을 반드시 사용하게 하고(설정할 시간 제공), 보안 키(가장 안전함), Google 메시지(Android 및 iOS에서 Google 앱 사용), 인증 앱 생성기(Google OTP 등), 문자 메시지 또는 전화 통화(가장 안전하지 않은 방법) 등 다양한 방법을 사용하여 2단계 인증을 적용할 수 있습니다.

조직에서 Google 이외의 ID 공급업체(IdP)를 사용하는 경우 서드 파티 ID 공급업체를 통해 싱글 사인온(SSO)을 설정할 수 있습니다. 원하는 경우 최고 관리자가 아닌 계정에도 SSO와 함께 2단계 인증을 사용할 수 있습니다.

서비스 사용 또는 사용 중지

관리자는 Google 관리 콘솔에서 사용자가 Google Workspace for Education 계정으로 액세스할 수 있는 Google 서비스를 제어할 수 있습니다. 조직 단위(OU)별로 서비스를 사용하거나 사용 중지하여 Calendar, Drive, Meet 등의 Google 서비스에 대한 액세스를 제어할 수 있습니다(그룹 사용 시에도 서비스를 사용할 수 있음). YouTube, Google 지도 및 Blogger와 같은 추가 서비스를 사용 설정하기 전에 Workspace 핵심 서비스와 추가 서비스 간의 차이점을 검토할 수도 있습니다. 관리자는 연령에 따라 Google 서비스에 대한 액세스 권한을 설정하는 것이 바람직하며, 만 18세 미만으로 지정된 사용자는 Google Workspace for Education 계정에 로그인하면 일부 Google 서비스에서 자동으로 사용이 제한된다는 점에 유의하세요.

또한 컨텍스트 인식 액세스(Workspace for Education Standard 및 Plus에서 사용 가능)를 사용하여 기기의 IP 주소, 지리적 출처, 보안 정책 또는 OS를 기반으로 Gmail, Drive, Calendar와 같은 Google 앱에 대한 액세스를 허용하거나 차단할 수 있습니다. 예를 들어 일부 국가/지역에서는 회사 소유 기기에서만 데스크톱용 Drive를 사용하도록 설정할 수 있습니다.

사용자에게 서비스 액세스 권한을 부여하는 방법

Google 관리 콘솔에서 Google Drive와 같은 Google 서비스에 대한 조직 단위의 액세스를 사용 중지할 수 있습니다. 해당 조직 단위의 일부 사용자가 Drive를 사용해야 하는 경우 다음 두 가지 옵션이 있습니다.

1. Drive가 사용 설정된 조직 단위로 사용자를 이동합니다.
2. 사용자를 액세스 그룹에 추가하고 그룹에 대해 Drive를 사용 설정합니다. 그룹의 각 구성원은 해당 서비스가 조직 단위에서 사용 중지되어 있더라도 서비스에 액세스할 수 있습니다.

조직 단위

조직 단위 1과 2에서는 Google Drive가 사용 중지됨

액세스 그룹 내

하지만 조직 단위 1과 2 안에 **있는 사용자 그룹은** Google Drive를 사용할 수 있음

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

데이터 공유 정책 및 보관 규칙 설정

관리자는 사용자가 조직 외부의 사람들과 Google Drive 파일 및 폴더를 공유할 수 있는지 여부를 제어 하는 데 도움이 됩니다. 이를 통해 의도하지 않은 또는 지나친 데이터와 파일의 공유를 방지하여 데이터 유출을 막을 수 있습니다. 파일과 드라이브를 분리하고, 조직 단위를 만들고, 최소 권한의 원칙에 따라 운영하는 것은 공격자가 하나의 계정에 침투한 경우 네트워크 간에 이동하는 것을 방지하는 데 중요합니다. 잠재적인 공격자가 액세스할 수 있는 데이터 및 네트워크 액세스가 적을수록 피해를 줄일 수 있습니다.

학생의 외부 파일 공유를 사용 중지(또는 외부 공유를 허용된 도메인으로만 제한)하고 '액세스 검사기'를 '수신자만'으로 설정합니다. 일부 또는 모든 사용자가 도메인 외부에서 파일을 공유할 수 있도록 허용하는 경우 사용자가 해당 파일을 공유할 때 경고가 표시되도록 사용 설정하세요. 또한 웹에서 파일 게시를 중지하고 외부 공동작업자가 Google 계정으로 로그인하도록 하세요.

또한 Workspace for Education Standard 및 Plus 고객은 공유 대상 그룹 및 신뢰 규칙을 사용하여 공유 권장사항 및 제한사항을 더욱 세분화된 수준으로 설정할 수 있습니다. 예를 들어 공유 대상 그룹을 사용하면 교사의 기본 링크 공유 대상을 교육 기관의 모든 사람이 아닌 '교사 및 교직원'으로 설정할 수 있습니다. 신뢰 규칙을 사용하면 초등학생이 고학년 학생과 파일을 공유하지 못하도록 차단할 수 있습니다.

공유 드라이브 정책을 검토하여 적절한 사용자만 공유 드라이브를 만들 수 있도록 하고 외부 사용자가 공유 드라이브에 액세스하지 못하도록 방지하세요. 관리자(또는 교직원 및 교사)만 공유 드라이브를 만들 수 있도록 허용하고 공유 드라이브 액세스를 면밀히 관리하는 것이 좋습니다.

가능하면 일부 또는 모든 사용자에 대한 연락처 공유를 중지하거나 맞춤 디렉터리를 만들어 어떤 사용자가 누구에게 표시되는지 제한하는 등 디렉터리 공개 상태와 연락처 공유를 제한하는 것이 좋습니다.

Drive와 Gmail에서 데이터 손실 방지(DLP) 정책을 설정하여 민감한 정보를 감지하고 차단합니다. 일반적으로 민감한 정보(예: 은행 또는 신용카드 번호)를 보호하기 위해 활용할 수 있는 기본 제공 정책이 있습니다. 키워드, 단어 목록 및 정규 표현식(Regex)을 기반으로 맞춤 정책을 만들 수도 있습니다.

Gmail 설정 관리

Gmail은 Google Workspace for Education의 핵심 서비스 중 하나로, 관리자가 기관과 사용자를 보호하기 위해 활용할 수 있는 다양한 설정이 있습니다.

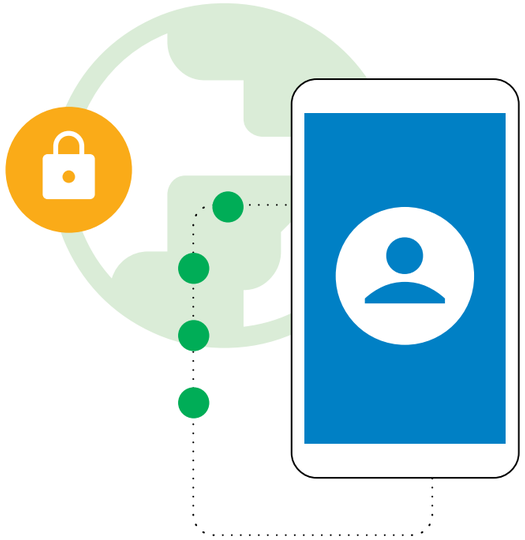
Gmail 인증을 통해 스팸, 스푸핑, 피싱을 방지하세요. 승인된 모든 발신자에 대해 발신자 인증을 요구하고 내부 발신자에 대한 스팸 필터 우회 기능을 중지하는 등 스팸 필터 설정을 맞춤설정할 수 있습니다.

가능하면 POP/IMAP 액세스를 중지하고 전송 전 메시지 검사 강화 및 피싱 및 멀웨어 차단(고급)을 사용 설정합니다. 일부 또는 모든 사용자에 대해 외부 이메일을 허용하는 경우 외부 수신자 경고를 사용 설정할 수 있습니다.

Google Workspace for Education Standard 및 Plus 고객은 보안 샌드박스를 사용하여 유해한 첨부파일을 감지하는 규칙을 설정하여 멀웨어 및 랜섬웨어로부터 보호할 수도 있습니다.

서드 파티 애플리케이션

기본으로 제공되는 승인 워크플로를 사용하여 API를 통해 계정 데이터에 액세스하는 서드 파티 애플리케이션을 승인하세요. 이렇게 하면 학교에서 사용하도록 승인되지 않은 서드 파티 애플리케이션과의 승인되지 않은 데이터 공유를 방지할 수 있습니다.



보고서 및 모니터링

관리자는 Google 관리 콘솔에서 보고서와 로그 이벤트를 확인하여 잠재적인 보안 위험과 같은 조직의 활동을 검토하고, 누가 언제 로그인했는지 확인하고, 사용자가 콘텐츠를 만들고 공유하는 방식을 파악할 수 있습니다. 그래프 및 표를 통해 세분화된 사용자 수준 세부정보와 함께 도메인 수준 데이터도 볼 수 있습니다. 보고서 및 감사 로그(알림 센터 포함)를 확인하여 보안 위험을 파악하고, 서비스 사용량을 분석하며, 구성 문제를 진단하고, 사용자 활동을 추적하는 등의 작업을 수행할 수 있습니다.

Google Workspace for Education Standard 및 Plus 관리자는 보안 대시보드를 활용하여 다양한 보안 보고서의 개요를 확인하고, 트렌드를 파악하며, 현재 및 과거 데이터(예: Drive의 파일 공유, Gmail의 스팸, 피싱, 멀웨어 활동, 의심스러운 사용자 계정 로그인, 의심스러운 기기 활동)를 비교할 수 있습니다. 관리자, Drive, Meet, Chat 로그 이벤트를 포함한 대부분의 사용, 활동 및 감사 로그와 보안 보고서는 6개월 동안 사용할 수 있습니다.

보안 센터 활용하기

Google Workspace for Education Plus 및 Standard 관리자는 보안에 관한 고급 정보 및 분석을 제공하고 도메인에 영향을 미치는 보안 문제에 대해 자세히 살펴보고 관리할 수 있도록 지원하는 보안 센터를 활용할 수 있습니다.

보안 센터에는 관리자가 피싱 공격, 부적절한 파일 공유, 의심스러운 사용자 및 기기 활동 등과 같은 보안 및 개인 정보 보호 문제를 식별하고 분류하여 조치를 취할 수 있도록 도와주는 보안 조사 도구가 포함되어 있습니다.

Google Workspace 는 세계에서 가장 안전한 클라우드 기반 커뮤니케이션 및 공동작업 제품군입니다.

0

2021년 11월 이후 Workspace에서 적극적으로 악용된 소프트웨어 취약점 수 0개*

50%

Workspace를 사용했을 때 절감할 수 있는 사이버 보안 보험료 비율 50%

2배 적음

Microsoft 365보다 Workspace를 사용하는 조직의 보안 사고가 2배 적음

2.5배 적음

Microsoft Exchange보다 Workspace를 사용하는 조직의 보안 사고가 2.5배 적음

*CISA에 따르면 이 분야의 다른 생산성 공급업체에 비해 훨씬 적은 수치입니다.

교육용 Google Chromebook

Chromebook은 별도의 구성이나 기능을 추가하지 않고도 바로 사용할 수 있는 보안 기능이 내장되어 있어 학생과 교사에게 매우 안전하고 확장 가능하며 사용하기 쉬운 컴퓨터입니다. 지금까지 기업, 학교 또는 일반 소비자용 ChromeOS 기기에 대해 랜섬웨어 공격이 보고된 적이 없었습니다. Chromebook은 업데이트된 기능을 사용해 진화하는 위협으로부터 학교를 보호하고, 백그라운드에서 자동으로 업데이트가 이루어지므로 사용자는 몇 초 만에 작업에 복귀할 수 있습니다.

맬웨어 방지 기능이 내장된 자동 OS 및 애플리케이션 업데이트

공격자는 운영체제, 브라우저, 자주 사용되는 앱의 버그와 허점을 이용해 멀웨어를 설치하고 사용자 데이터를 도용하려고 끊임없이 시도합니다. Chromebook은 기본적으로 보안 업데이트를 통해 안전하게 보호되도록 설계되어 있으므로 관리자와 사용자를 보호하기 위해 OS와 애플리케이션을 최신 상태로 유지합니다. 클라우드 애플리케이션은 로컬 앱처럼 소프트웨어 업데이트가 필요하지 않습니다. Google에서 설계한 Chromebook의 보안 칩은 기기를 안전하게 유지하고 사용자 신원을 보호하며 시스템 무결성을 보장하는 데 도움이 됩니다.

사용 중인 Chromebook은 최신 멀웨어 방지 업데이트를 자동으로 실행합니다. 데이터 암호화, 자체 검사 부팅, 샌드박스, 자동 업데이트 같이 기본적으로 제공되는 보안 기능으로 학생과 교육자를 사이버 위협으로부터 보호합니다.

사용자 데이터 보호

Google 계정으로 Chromebook에 로그인하면 모든 데이터가 암호화된 파일에 저장되므로 해당 기기를 사용하는 다른 사용자가 내 데이터를 보거나 내 계정을 사용해 애플리케이션에 로그인할 수 없습니다. 이를 통해 학생은 교실 내에서 매우 쉽고 안전하게 기기를 공유할 수 있으며, 학교는 총컴퓨팅 비용을 절감할 수 있습니다. 고급 보안 기능을 사용하려면 기기 관리 라이선스인 Chrome Education 업그레이드를 통해 향상된 가시성을 확보할 수 있습니다.

원격 사용자 관리 기기에 대한 보안 정책

학교 관리자는 Google 관리 콘솔을 사용하여 원격으로 ChromeOS 정책을 구성하고 애플리케이션을 설치/업데이트할 수 있습니다. 한 명의 IT 관리자가 버튼 클릭만으로 수십만 대의 Chromebook에 대한 정책과 구성을 순식간에 업데이트할 수 있습니다.

이렇게 하면 다음과 같은 이점이 있습니다

- 학생은 학교에서 승인한 콘텐츠 및 애플리케이션에만 액세스할 수있습니다.
- 모든 애플리케이션과 확장 프로그램이 최신 보안 수정 사항으로 업데이트됩니다.
- 사용자가 기기 외부에서 학교 데이터를 복사, 전송 또는 공유할 수 없습니다.
- 보안 위협에 대응하기 위한 Google의 맞춤형 보안 권장사항으로 데이터에 기반한 의사 결정을 내릴 수 있습니다.
- 관리 콘솔에서 모든 사용자의 보안과 ID 및 액세스 관리 정책을 중앙에서 관리할 수 있습니다.

관리자가 구성할 수 있는 몇 가지 중요한 정책은 다음과 같습니다:

기기 정책

- **게스트 모드**
  학생과 교사가 기기를 익명으로 사용하는 대신 반드시 자신의 사용자 인증 정보를 사용하여 로그인하도록 기기의 게스트 모드를 중지하는 것이 좋습니다.
- **로그인 제한**
  학생과 교사가 개인 Gmail 계정을 사용하여 학교용 Chromebook에 로그인하지 않도록 하려면 학생만 사용하는 기기에서는 로그인 제한을 Workspace 도메인으로 한정하도록 적용합니다.
- **사용자 및 기기 보고**
  관리자는 Chromebook 사용 빈도, 사용자, 하드웨어 상태에 대한 측정항목을 수집할 수 있도록 사용자 및 기기 보고 기능을 사용하는 것이 좋습니다.
- **강제 재등록**
  학교 소유의 Chromebook은 관리자가 프로비저닝을 해제하지 않는 한 학교에서만 사용하는 것이 중요합니다. 관리자는 Chromebook이 완전 삭제되거나 도용하려는 시도가 있는 경우 항상 재등록하도록 Chromebook의 강제 재등록을 사용 설정해야 합니다.

사용자 정책

- **시크릿 모드**
  학생이 학교용 Chromebook을 성공적으로 사용할 수 있도록 설정이 올바르게 이루어져야 합니다. 여기에는 웹 콘텐츠 필터가 부적절한 웹사이트를 차단할 수 있도록 인증된 브라우저만 사용하도록 하는 것이 포함됩니다. 관리자는 학생이 웹 필터를 우회할 수 없도록 시크릿 모드를 중지해야 합니다.
- **프록시 모드**
  일부 학교에서는 웹 필터링에 프록시를 사용할 수 있지만, 사용자가 프록시 설정을 직접 변경할 수 없도록 설정하는 것이 중요합니다.
- **멀티 로그인 액세스**
  사용자가 학교의 Chromebook과 Workspace 계정을 사용하는 동안 보조 계정에 로그인하는 것이 허용되는 경우 민감한 학생 또는 학교 데이터/정보 가 해당 보조 계정으로 쉽게 유출 될 수 있습니다. 관리자는 멀티 로그인 액세스를 차단해야 합니다.
- **브라우저 방문 기록**
  학생의 경우 브라우저 방문 기록을 지우는 기능을 중지하는 것이 도움이 될 수 있습니다. 인터넷 보안 사고가 발생하면 이러한 인터넷 방문 기록 로그가 조사 과정에서 유용하게 사용될 수 있습니다.

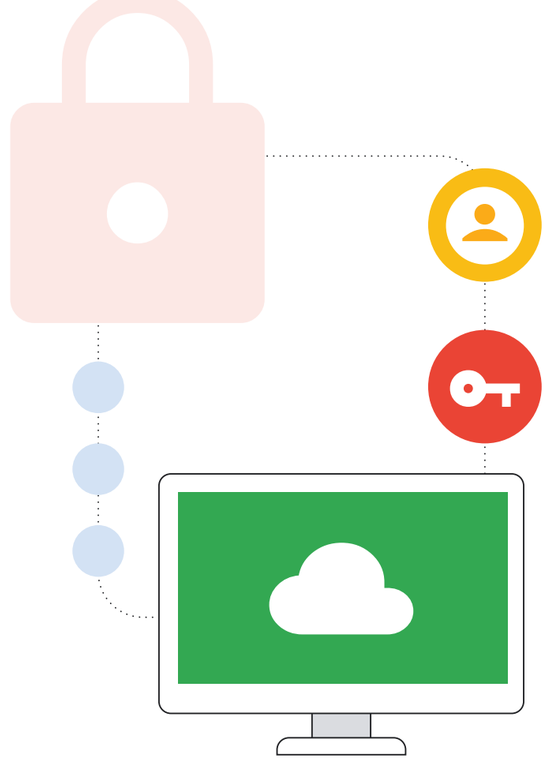
이 목록은 심각한 사이버 사고로 이어지는 가장 일반적인 유형의 실수로부터 네트워크를 안전하게 보호하기 위한 좋은 출발점이 됩니다. 기타 추가적인 권장 보안 정책은 보안 체크리스트에서 확인할 수 있습니다.

언제 어디서나 안전하게 사용할 수 있는 엔드포인트 관리

학교 관리자는 ChromeOS의 원격 정책 관리 시스템을 사용해 학교의 네트워크 서버가 아닌 기기에서 보안 설정을 적용하고 콘텐츠 필터링 시스템과 같은 보안 도구를 실행할 수 있습니다. 이를 통해 학생은 교실에서와 마찬가지로 집에서도 안전하게 학교용 Chromebook을 사용할 수 있습니다. 이는 학교가 디지털 교과서와 온라인 학습 도구로 전환하고 학생이 숙제를 위해 집으로 컴퓨터를 가져갈 수 있도록 하면서 점점 더 중요해지고 있습니다.

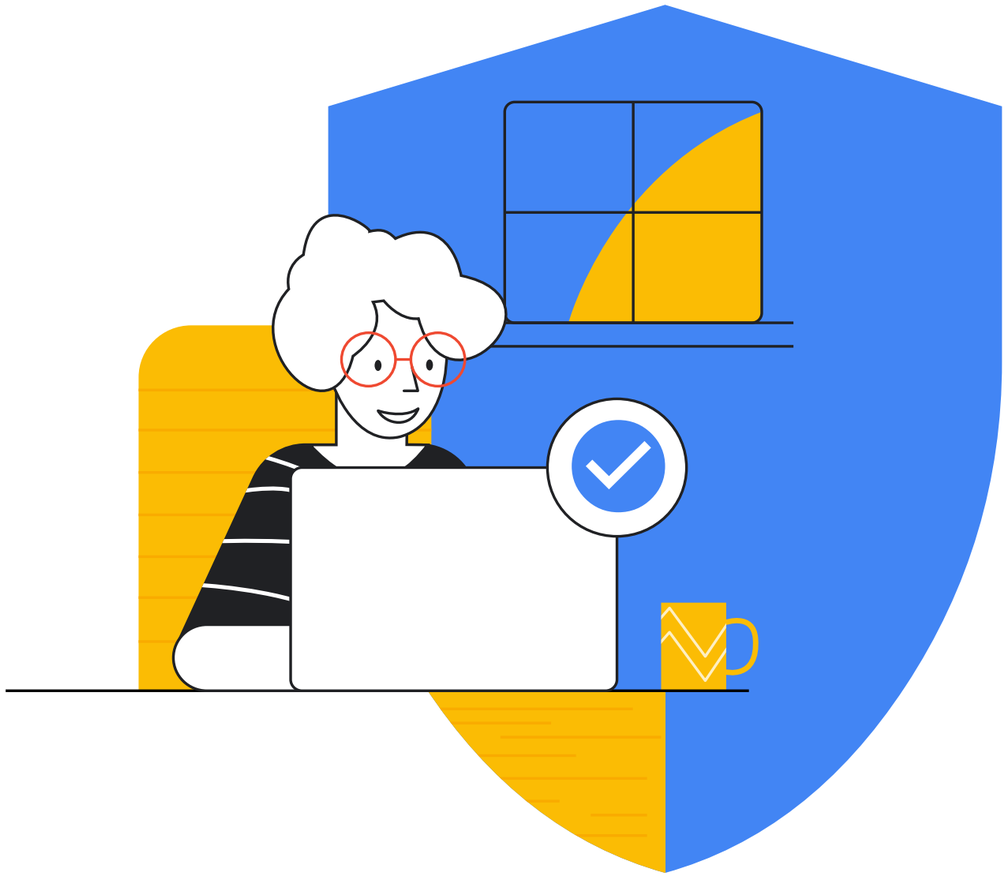
결론

사이버 사고로부터 K-12 교육 기관을 보호하는 것은 쉽지 않지만, 관리자와 학생, 교사, 교직원, 나아가 더 넓은 온라인 생태계를 보호하기 위해 투자할 만한 가치가 있습니다. 이 가이드에서 다룬 항목은 이러한 노력을 시작하는 좋은 출발점이 될 수 있지만, 각 학교는 고유한 요구사항에 맞게 권장사항을 조정하고 진화하는 위협 환경과 새로운 기술에 계속 발맞춰 나가야 합니다. 이 가이드는 K-12 교육 기관에 보안 프로그램을 도입할 때 활용할 수 있는 기본적인 지침 을 제공하며, 앞으로 실행할 수 있는 단계와 실행 가능한 작업 항목에 대한 리소스를 제공합니다. 또한 Google은 학교와 조직이 이 가이드북의 권장사항을 구현하고 AI와 같은 새로운 기술을 활용할 때 도움을 줄 수 있는 다양한 리소스, 교육, 숙련된 사이버 보안 전문가를 보유하고 있습니다. 교육용으로 맞춤화된 Google 제품은 이 가이드에서 설명한 사이버 보안상의 많은 함정에 대해 즉시 적용할 수 있는 솔루션을 제공합니다. 보안 프로그램을 설계하고 구현하는 과정에서 여러분과 협력할 수 있기를 바랍니다.



리소스 목록

- [1]Google. ‘Tips to Stay Safe & Secure Online(온라인에서 안전과 보안을 유지하기 위한 팁).’ Google 안전 센터, https://safety.google/security/security-tips/. 2022년 10월 6일 액세스.
- [2]NIST. ‘Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1(중요한 인프라의 사이버 보안 개선을 위한 프레임워크, 버전 1.1).’ NIST Technical Series Publications, 2018년 4월 16일, https://doi.org/10.6028/NIST.CSWP.04162018. 2022년 10월 6일 액세스.
- [3]Microsoft. ‘Microsoft AccountGuard 프로그램.’ Microsoft AccountGuard 프로그램, https://www.microsoftaccountguard.com/ko-kr/. 2022년 10월 6일 액세스.
- [4]Google. ‘고급 보호 프로그램’ Google 고급 보호 프로그램, https://landing.google.com/advancedprotection. 2022년 10월 6일 액세스.
- [5]Google. ‘Google 안전 센터’ Google 안전 센터 - 안전한 온라인 환경 조성, https://safety.google. 2022년 10월 6일 액세스.
- [6]Meta. ‘기본 정보: 계정 보호하기’ 계정 보호하기, https://www.facebook.com/gpa/resources/basics/security. 2022년 10월 6일 액세스.
- [7]Meta. ‘Facebook Protect.’ Facebook, https://www.facebook.com/gpa/facebook-protect. 2022년 10월 6일 액세스.
- [8]NIST. ‘SP 800-124 Rev. 1: 기업 내 모바일 기기의 보안 관리를 위한 가이드라인(Guidelines for Managing the Security of Mobile Devices in the Enterprise).’ NIST Technical Series Publications, https://doi.org/10.6028/NIST.SP.800-124r1. 2022년 10월 6일 액세스.
- 패스키: https://developers.google.com/identity/passkeys
- CISA 보고서: 미래를 보호하기 위한 K-12의 사이버 보안: https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAO 보고서 https://www.gao.gov/products/gao-20-644
- Google for Education이 기관을 보호하는 데 어떻게 도움이 되는지 자세히 알아보려면 Google for Education 개인 정보 보호 및 보안 센터를 참조하세요.
- Zcaler 피싱 보고서



Google for Education

Safer with Google