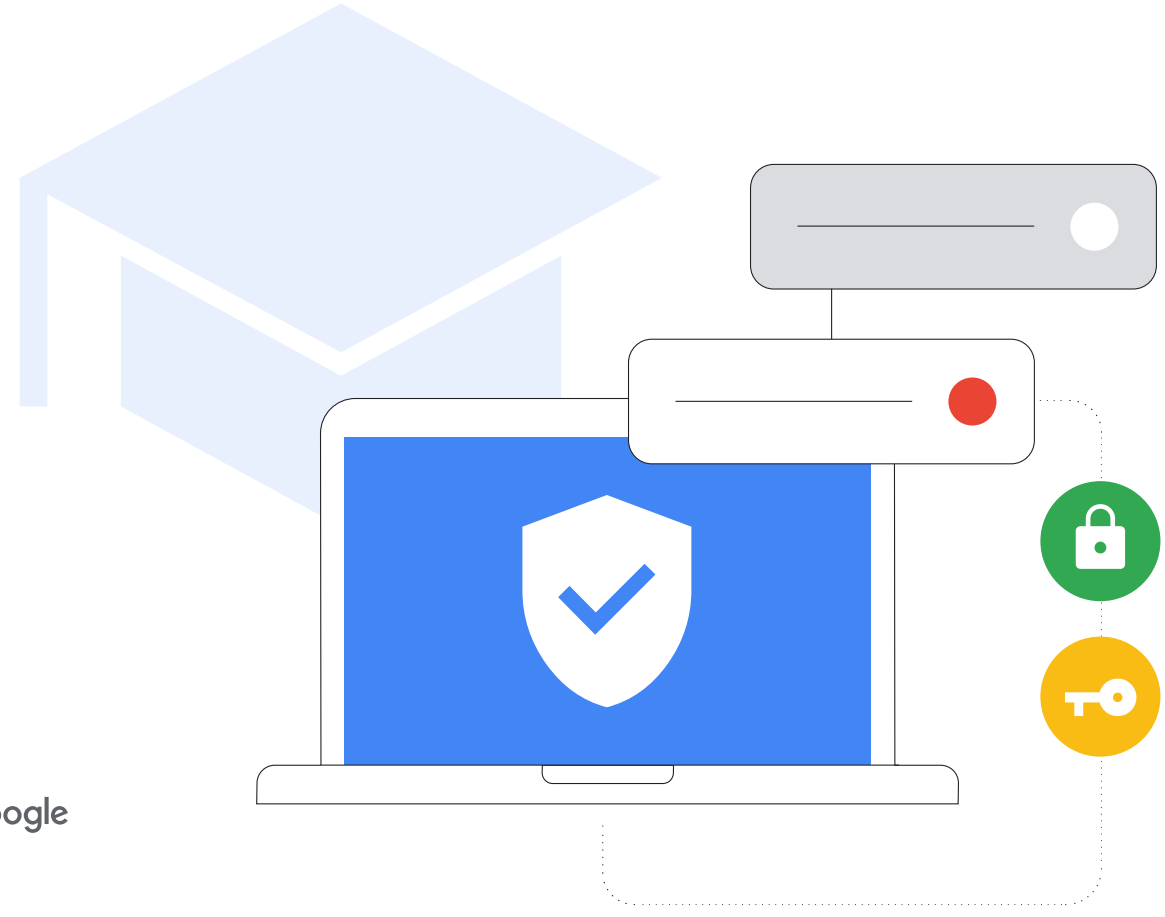
Google for Education

Guia de segurança cibernética para os ensinos fundamental e médio

Atualizado em agosto de 2023



Safer with Google

Resumo executivo

De acordo com o relatório Protecting Our Future[1] da CISA, é muito importante que as instituições de ensino fundamental e médio invistam em segurança cibernética para proteger os estudantes e seus familiares, além dos professores, funcionários e comunidades. Este documento oferece orientações e práticas recomendadas para ajudar administradores de TI a configurarem hardware e software nas instituições de ensino fundamental e médio com o objetivo de fortalecer a segurança cibernética. O documento inclui práticas recomendadas gerais e orientações específicas com relação aos produtos e serviços do Google. Nossa missão é organizar as informações mundiais, e fazer com que elas sejam universalmente acessíveis e úteis é uma das principais motivações da equipe do Google for Education: nós trabalhamos para criar ferramentas para o uso no ensino e no aprendizado. Neste guia, você vai conferir as lições que aprendemos com esse trabalho.

As práticas recomendadas de segurança estão organizadas de acordo com o tema para oferecer uma visão mais aprofundada sobre a configuração e as estratégias de redução de riscos. Além disso, vamos explicar como o Google lida com a segurança cibernética nos próprios serviços, principalmente no caso das ferramentas de educação. Embora este documento inclua orientações detalhadas sem relação a um produto ou serviço específico, acreditamos que nossos produtos oferecem muito mais proteção contra ataques instantâneos.

O risco

As instituições de ensino são o principal alvo dos ataques cibernéticos, em que usuários de má-fé tentam tirar proveito dos ambientes ricos em dados das escolas. 46% das instituições que ainda não foram alvo acreditam que um dia vão ser, já que os ataques de ransomware estão ficando mais sofisticados e mais difíceis de impedir. Além disso, 42% dessas escolas acreditam que o ransomware é tão comum que um ataque desse tipo é simplesmente inevitável. A rápida transição para o ensino a distância em 2020 foi um dos principais motivos desses problemas de segurança cibernética, deixando as escolas vulneráveis a ataques.

A defesa

É possível reduzir esses ataques. E mesmo que nenhuma tecnologia consiga eliminar o risco por completo, o setor de ensino e os fornecedores de tecnologia de educação podem trabalhar juntos para adotar e implementar práticas recomendadas. O objetivo é criar uma abordagem segura e abrangente para diminuir os riscos de maneira significativa. Com as devidas precauções e políticas para proteger os usuários e dispositivos, além de garantir a privacidade de dados, as instituições de ensino podem controlar melhor os riscos e reduzir os ataques.

Principais recomendações

- **USE UMA AUTENTICAÇÃO SEGURA** para proteger as informações sensíveis, e-mails, arquivos e outros tipos de conteúdo, além de impedir que usuários não autorizados acessem os sistemas de ensino. Adote práticas recomendadas de autenticação de usuários, incluindo senhas fortes e verificação em duas etapas (2SV, na sigla em inglês), chaves de acesso e gerenciadores de senhas quando possível. Isso é aplicável principalmente para os funcionários e administradores de TI que trabalham com informações sensíveis.
- **DEFINA AS CONFIGURAÇÕES DE SEGURANÇA APROPRIADAS** para proteger os usuários, dados e ambiente. Mesmo que os produtos do Google incluam proteção por padrão, é essencial que os administradores também utilizem e configurem redes e sistemas corretamente para garantir a segurança. Para proteger as escolas, aplique os princípios de confiança zero e privilégio mínimo: os usuários só vão ter acesso ao software, dados, aplicativos e sistemas necessários para eles trabalharem.
- **ATUALIZE OS SISTEMAS E FAÇA UPGRADE DELES** para assegurar que os usuários estejam protegidos contra as ameaças mais recentes. Use sistemas operacionais (SOs) e navegadores modernos para que os usuários executem as versões mais recentes do software em todos os dispositivos (ou versões estáveis e aprovadas de longo prazo) e elas sejam atualizadas automaticamente. Fazer upgrade para uma solução mais segura, como os Chromebooks, aumenta a segurança. Nunca nenhum ataque de ransomware foi detectado em um dispositivo ChromeOS.
- **USE SISTEMAS DE ALERTA E MONITORAMENTO EM TEMPO REAL** para aprimorar a postura de segurança e reduzir os possíveis problemas com rapidez. É possível incorporar esses recursos ao seu software principal de colaboração e comunicação, como o Google Workspace for Education, ou implantar soluções separadas de geração de registros e monitoramento de segurança. É importante acompanhar de maneira abrangente as atividades da rede, dispositivos, aplicativos, usuários e dados da escola. Monitore os logins nas contas, compartilhamento de arquivos, volume de e-mails (principalmente as tentativas de phishing e malware), atividades dos dispositivos e mudanças nas configurações. Mantenha sua solução de alerta e monitoramento atualizada para receber notificações sobre ameaças, eventos importantes e mudanças no sistema.
- **TREINE PROFESSORES, FUNCIONÁRIOS E ESTUDANTES** sobre como usar dispositivos e software com segurança, como reconhecer e denunciar possíveis ameaças e como compartilhar dados da maneira correta para evitar alguns dos ataques mais comuns. As instituições ou distritos escolares podem criar materiais de treinamento próprios, além de usar conteúdo pronto e disponibilizado sem custos, para elaborar um kit de ferramentas amplo para as escolas.

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

Recomendações específicas para usuários dos produtos do Google: produtos como o Google Workspace for Education e os Chromebooks aprimoram a segurança cibernética da sua escola e facilitam a implementação de cada uma dessas recomendações. Juntos, eles criam uma solução completa que ajuda a proteger a privacidade dos usuários e oferece a melhor segurança da categoria para sua instituição.

Essas estratégias e as orientações extras no documento a seguir criam uma ótima base para implementar a segurança nas instituições de ensino fundamental e médio.

A abordagem do Google para educação

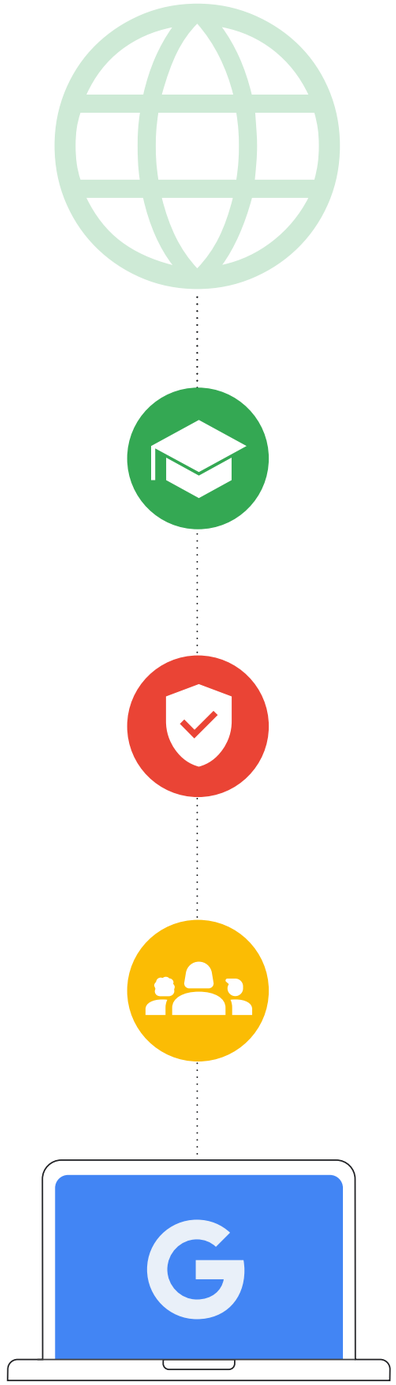
A missão do Google é organizar as informações do mundo e fazer com que elas sejam universalmente acessíveis e úteis. No caso do setor da educação, isso não é diferente. Para seguir essa missão, a equipe do Google for Education desenvolve ferramentas como os Chromebooks e o Google Sala de Aula. Com elas, os estudantes e professores têm facilidade e segurança para criar, compartilhar e organizar o próprio conteúdo, além de acessar e usar recursos educacionais e ferramentas on-line.

As escolas merecem tecnologias que sejam seguras por padrão e privativas por design, mantenham você no controle e ofereçam conteúdo e informações confiáveis. Com produtos como os Chromebooks e o Google Workspace for Education, as escolas garantem a melhor segurança da categoria, em conformidade com os mais altos padrões educacionais do mundo. Além disso, os administradores de TI têm visibilidade total e controle otimizado dos dados e políticas de segurança. Já os estudantes aproveitam uma experiência totalmente imersiva de aprendizado em um ambiente digital mais seguro que disponibiliza conteúdo com base na idade e diminui a quantidade de spam e ameaças cibernéticas.

Nossas prioridades são recursos e controles integrados, padrões de privacidade nos mais altos níveis e opções de ferramentas de proteção mais proativas para garantir a segurança no aprendizado para todos. Os dispositivos ChromeOS reduzem as ameaças de segurança e oferecem a melhor defesa contra a ameaça número um às escolas: o ransomware. Nunca nenhum ataque de ransomware contra um Chromebook foi bem-sucedido.

Já o Google Workspace for Education é um dos pacotes de comunicação e colaboração baseados na nuvem mais usados e seguros do mundo. Para saber como cada solução aprimora a segurança cibernética somada às recomendações deste documento, consulte a última seção.

Este documento é dividido em duas seções: a primeira inclui orientações práticas e gerais sobre segurança para instituições de ensino fundamental e médio sem relação a produtos específicos. A segunda seção apresenta orientações específicas sobre configuração para instituições que usam os produtos do Google for Education, como o Google Workspace for Education e os Chromebooks. Ambas as seções incluem informações que ajudam a manter você e seus estudantes seguros on-line.



Introdução

Os dispositivos e as redes das instituições de ensino fundamental e médio correm um alto risco de ataques cibernéticos. É muito importante que essas instituições implementem a melhor segurança possível para proteger os estudantes e evitar a perda de dados, serviços, recursos, tempo e dinheiro causada pelos ataques. (Fonte)

Este guia promove práticas recomendadas de segurança cibernética para sistemas e administradores de escolas aprimorarem a proteção dos seus ambientes. Com a implementação dessas práticas, as instituições de ensino fundamental e médio diminuem e evitam ataques cibernéticos graves e caros nos sistemas educacionais, além de proteger os estudantes, seus familiares, professores e funcionários das escolas.

Os ataques cibernéticos direcionados às escolas estão cada vez mais frequentes e graves. De acordo com o K-12 Cybersecurity Resource Center, entre 2016 e 2021, foram divulgados publicamente mais de 1.300 incidentes cibernéticos envolvendo organizações de ensino em todos os 50 estados americanos. Os líderes educacionais de hoje precisam proteger os dados e as informações pessoais dos estudantes, professores e funcionários da escola, além das informações e sistemas da instituição. Essa é uma tarefa complicada, principalmente se considerarmos que o setor educacional costuma ter mais dificuldade para lidar com a segurança cibernética em comparação com os outros setores.

Os ataques cibernéticos bem-sucedidos, incluindo ransomware, phishing, malware e muito mais, podem causar o vazamento em larga escala de informações de identificação pessoal (PII), prejuízos muito grandes (desde 2020, o valor médio de um resgate aumentou cinco vezes, chegando a US$ 812.260) e interrupções prolongadas no ensino e em outras operações escolares. Recentemente, um ataque bem-sucedido de ransomware levou uma escola a desligar todo seu sistema. Isso causou consequências na comunidade, já que os estudantes foram impedidos de frequentar a escola por diversos dias seguidos. Com recursos e fundos ilimitados, as organizações de ensino fundamental e médio vão continuar sendo o principal alvo dos ataques, a menos que haja investimentos para aprimorar a segurança cibernética.

Os elementos que mais aprimoram a segurança cibernética são a comunicação, colaboração e parceria. Para elaborar este documento, usamos como base as dicas de proteção e segurança do Google, as diretrizes Cybersecurity Framework do Instituto Nacional de Padrões e Tecnologia americano (NIST, na sigla em inglês) e as recomendações e ferramentas de segurança cibernética de 2023 para ensinos fundamental e médio da CISA (as fontes mais aceitas pelo setor com relação a práticas de segurança cibernética). O documento inclui as etapas gerais que os administradores de TI precisam seguir ou considerar, algumas práticas recomendadas e orientações dos produtos do Google e referências para outros serviços e dicas de segurança oferecidos por terceiros. É importante que os administradores confiram todas as orientações de segurança fornecidas pelas empresas relevantes e implementem as instruções mais recentes. Isso acontece porque essas empresas são as que melhor podem descrever seus próprios produtos e as mudanças implementadas neles.

Antes de seguir as recomendações listadas abaixo, considere também os seguintes fatores:

Considerações

1. **A proteção de todos os estudantes da escola.**
   As necessidades de cada escola variam, e talvez seja necessário tomar medidas adicionais para proteger a segurança e a privacidade de determinados estudantes. Muitas ferramentas de tecnologia de educação incluem recursos que ajudam a determinar o acesso dos estudantes por idade, como a limitação de conteúdo inadequado e a garantia da privacidade dos dados de contato e endereço.
2. **Os tipos de dados que você armazena.**
   Se você guarda dados sensíveis, é importante criptografar essas informações ou armazenar tudo em um lugar separado.
3. **Os tipos de dispositivos usados e seu modelo de implantação.**
   É importante que os dispositivos e aplicativos sejam atualizados automaticamente para aumentar a segurança, criptografar os dados e isolar as contas. Isso garante que os usuários tenham acesso apenas às próprias informações.
4. **As políticas da sua instituição, distrito escolar ou região.**
   É provável que sua escola tenha políticas específicas com relação ao uso de tecnologias. Você precisa garantir que todas as proteções aplicadas estejam de acordo com essas políticas.

Todos os dias
100 milhões
de tentativas de phishing são bloqueadas pelo Gmail.

Toda semana
300 mil
sites não seguros são identificados pelo Google.

Todos os dias
74 milhões
de pessoas usam o Gerenciador de senhas do Google.

Todos os anos
700 milhões
de usuários usam a Verificação de segurança para se proteger on-line.

Diretrizes gerais de segurança

Use a autenticação segura

A autenticação segura precisa ser uma das principais prioridades nas escolas e em outras instituições. No quarto trimestre de 2022, as contas com senhas fracas ou sem credenciais correspondiam a 48% de todos os fatores que levavam a violações. Com a implementação de determinadas recomendações importantes, você confirma a real identidade das pessoas e limita o acesso às informações apropriadas com base na função de cada usuário.

Os administradores de TI precisam implementar o uso da verificação em duas etapas (2SV), também conhecida como autenticação de dois fatores (2FA), e adotar a autenticação sem senha (por exemplo, com chaves de acesso) sempre que possível e principalmente quando alguém estiver acessando os sistemas da instituição de ensino de maneira remota. A 2SV adiciona uma camada extra de segurança às suas contas on-line para que os invasores tenham muito mais dificuldade para ganhar acesso.

Hoje, as escolas usam muitos tipos de dispositivos e modelos de implantação, e os ambientes de ensino fundamental e médio incluem aptidões técnicas variadas. A segurança dos dispositivos e contas variam de acordo com os tipos e funções de usuário com práticas recomendadas definidas: administradores de TI, professores e funcionários, além dos estudantes mais velhos que usam dispositivos atribuídos e dos mais novos que utilizam dispositivos compartilhados. Confira abaixo recomendações específicas a cada grupo.

Há diversos tipos de métodos de autenticação que são recomendados na maioria dos cenários:

- **Senhas fortes:**
  Peça aos usuários para criarem sua própria senha no primeiro login e inclua requisitos técnicos de comprimento e complexidade. As senhas mais longas aumentam a segurança devido ao comprimento e ao uso de caracteres complexos. Não é recomendado pedir que os usuários alterem suas senhas com frequência, porque isso pode encorajar a adoção de senhas mais simples ou mudanças insignificantes (por exemplo, atualizar apenas um caractere).
- **Verificação em duas etapas (2SV):**
  A 2SV protege as contas ao incluir uma segunda etapa de verificação. Muitas vezes, isso é feito com algo que o usuário tenha, como uma chave de segurança ou um app móvel que gere um código de verificação única. Mesmo que qualquer tipo de 2SV ofereça mais proteção, os administradores precisam evitar o uso dos códigos de verificação enviados por mensagens de texto ou ligações, que são vulneráveis a ataques baseados em números de telefone.
- **Autenticação sem senha:**
  As chaves de acesso são mais seguras e fáceis de usar do que as senhas. Os usuários podem fazer login nos apps e sites com um PIN, padrão, sensor biométrico (como impressão digital e reconhecimento facial) ou chave de segurança. Assim, eles não precisam mais ficar se lembrando das senhas ou gerenciar essas informações. Mesmo que não sejam adequados para todos os contextos de ensino, esses métodos estão cada vez mais substituindo as formas tradicionais de autenticação e tornando o processo de login mais seguro e rápido. As chaves de acesso protegem os usuários contra ataques de phishing, já que elas funcionam apenas nos sites e apps registrados.
- **Logon único (SSO):**
  Com o SSO, os usuários podem acessar vários aplicativos e sites usando um conjunto de credenciais. Isso diminui as chances de que eles anotem essas informações em algum lugar. Além disso, quando as escolas não precisam gerenciar vários conjuntos de credenciais de usuários, elas economizam dinheiro porque diminuem os custos do suporte de TI e help desk. O Google Workspace for Education é compatível com o SSO de maneira nativa para que os usuários façam login em aplicativos de terceiros com as credenciais das suas Contas do Google ou utilizem os dados de outro provedor para entrar nessas contas.
- **Gerenciadores de senhas:**
  Eles ajudam os usuários a criarem senhas fortes e exclusivas nas diferentes contas e serviços usados no dia de trabalho e de escola (quando o SSO não é implementado). Os gerenciadores não ajudam a fazer login no sistema operacional de um dispositivo, mas controlam as senhas depois que o usuário inicia a sessão. Os usuários do Google podem utilizar o Gerenciador de senhas no Chrome em todas as plataformas, no ChromeOS e no Android.

Ao combinar essas abordagens de autenticação ou organizar esses métodos em subconjuntos especializados, é possível atender às necessidades exclusivas de vários grupos, de acordo com a função e idade dos usuários na instituição de ensino e o tipo de sistemas e dados que eles acessam.

Administradores de escolas

Os administradores controlam os sistemas e a maior parte dos dados de uma instituição de ensino fundamental e médio. Proteger a conta deles é essencial para a segurança de todo o sistema, incluindo a infraestrutura, os dados das contas e os dispositivos que a instituição administra. Por isso, os administradores precisam adotar as melhores abordagens de autenticação, incluindo o uso de senhas fortes, um gerenciador de senhas robusto e a 2SV. Cada abordagem oferece uma camada de proteção e, quando implementadas juntas, garantem a mais reforçada segurança para os serviços empresariais e conta de administrador.

- Os administradores devem usar uma chave de segurança física ou um método de verificação em duas etapas criptograficamente seguro que requer um dispositivo confiável e prompts. Por exemplo, um serviço como o Google Authenticator ou outro app que crie códigos de verificação única. Os Chromebooks lançados após 2019 com chip TPM contêm um botão liga/desliga que pode ser usado na autenticação de dois fatores.
- Os administradores precisam usar um gerenciador de senhas confiável que seja compatível com a 2SV para armazenar as senhas de diferentes serviços.

Professores e funcionários que usam dispositivos atribuídos

Assim como os administradores, os professores e funcionários da escola têm acesso a dados sensíveis. No entanto, eles não controlam a infraestrutura digital e têm aptidões técnicas mais variadas.

- Os professores e funcionários que usam Chromebooks precisam ter a opção de fazer login com uma verificação biométrica como impressão digital, onde legalmente permitido.
- Os administradores precisam aplicar o uso da 2SV e adotar a autenticação sem senha sempre que possível e quando um membro da equipe estiver acessando os sistemas da instituição de ensino de maneira remota.

Estudantes mais velhos que usam dispositivos atribuídos (geralmente a partir do quarto ano)

Os estudantes mais velhos sabem se proteger melhor e normalmente conseguem usar mecanismos de autenticação mais seguros, o que é apropriado para os tipos de serviço que eles podem estar utilizando. Esses estudantes precisam ter acesso somente à própria conta e às informações que foram compartilhadas com eles.

- Os estudantes que usam Chromebooks precisam ter a opção de criar um PIN específico ao dispositivo para acelerar o login. Em muitos ambientes escolares, as opções de biometria podem não ser adequadas ou viáveis.
- É essencial ajudar cada estudante a criar uma senha exclusiva que não contenha informações pessoais (por exemplo, nome, turma ou aniversário). Eles precisam aprender que as senhas longas podem ser complexas e ainda assim fáceis de lembrar.

Estudantes jovens que usam dispositivos compartilhados (geralmente no maternal)

Os estudantes mais jovens ainda estão aprendendo a usar tecnologias de aprendizado. Um método perfeito para eles é a autenticação simples (essa opção também é apropriada para uso com serviços e dados limitados).

- É importante adotar medidas de segurança nas escolas que usam opções de autenticação externas menos seguras como códigos QR e login com imagens no caso dos estudantes mais jovens ou que não conseguem utilizar senhas. Os administradores precisam modificar a senha dos estudantes e atualizar o código sempre que ele for perdido ou exposto.
- As escolas precisam orientar os estudantes e seus responsáveis sobre a importância de manter as senhas em segredo e de armazenar com segurança credenciais alternativas como códigos QR.
- No caso de dispositivos atribuídos como tablets, use um PIN específico ao dispositivo como um método de autenticação seguro alternativo.

Aplique as configurações de segurança apropriada

As redes e os dispositivos escolares são um alvo de alta visibilidade e valor para invasores no mundo todo. Por isso, é essencial aplicar a melhor proteção possível para impedir a perda de serviços, recursos, tempo e dinheiro. Os administradores de sistemas precisam implementar os recursos de segurança eficazes e apropriados que vêm incluídos nos produtos usados pela instituição. No entanto, também é necessário garantir que os professores, funcionários e estudantes tenham facilidade para usar esses sistemas. É preciso definir importantes configurações de privacidade e segurança para que elas não sejam desativadas ou modificadas por usuários individuais. Além disso, o administrador precisa definir os padrões de proteção em outras configurações. É essencial aplicar a melhor proteção possível para impedir a perda de serviços, recursos, tempo e dinheiro. Se você usa Chromebooks, confira na última seção as sugestões de configuração de políticas de dispositivo.

Por fim, é recomendado incorporar a minimização de dados às suas práticas. Para isso, basta limitar as finalidades e os meios de coleta, uso e divulgação de informações pessoais ao que seja razoavelmente necessário e proporcional para disponibilizar o serviço ou de outro modo consistente com o contexto da relação.

Aplicativos e atualizações

Limite e reduza os apps que os usuários podem instalar no dispositivo, já que eles são possíveis vetores de ataque a serem explorados. Se possível, use aplicativos de fontes confiáveis. Por exemplo, recomende aos usuários que verifiquem o selo de confirmação no Google Play Store para que eles façam o download dos aplicativos oficiais, que passaram por uma análise de segurança. As modificações no SO ou no hardware (jailbreak e rooting) produzem falhas de segurança significativas e precisam ser evitadas.

Acesso e visibilidade

Os administradores precisam garantir que os usuários tenham acesso apenas aos dados, softwares, serviços e sistemas necessários para que estes realizem suas tarefas ou aprendam com eficácia. Isso ajuda a limitar o acesso indesejado e a acompanhar quem pode usar quais recursos. Dê uma atenção especial aos dados altamente sensíveis, como PII e sistemas (por exemplo, RH, folha de pagamento, avaliação, segurança e configuração). Para isso, faça uma auditoria de quais usuários podem acessar os dados e sob quais circunstâncias, além de limitar a entrada nos dispositivos da escola e assegurar que apenas membros específicos da equipe tenham acesso. .

Revise suas políticas de compartilhamento de dados nas ferramentas de colaboração para impedir o acesso não autorizado ou o compartilhamento em excesso ou inapropriado. Limite ou impeça o compartilhamento para fora do seu ambiente, principalmente no caso dos estudantes, e aplique políticas que monitorem o compartilhamento de conteúdo sensível.

Roubo ou perda de dispositivo

Quando um dispositivo é perdido, isso não significa que os dados também serão. Os administradores precisam elaborar um plano para garantir o acesso às informações e aos documentos no caso de roubo ou perda de um dispositivo, por exemplo, armazenando os documentos em um ambiente de nuvem. Faça o download dos códigos alternativos dos processos de 2SV e os imprima para evitar que o acesso à conta seja interrompido.

É essencial bloquear remotamente um dispositivo se possível quando ele é reportado como perdido ou roubado. Além disso, as contas associadas precisam ser bloqueadas ou sinalizadas para evitar o acesso não autorizado. Os Chromebooks oferecem o recurso de apagamento remoto para o caso de perda, e as contas do Google Workspace for Education podem ser monitoradas em busca de atividade suspeita ou suspensas (bloqueadas) se necessário.

Proteção avançada para usuários de alto risco

Para os usuários com alta visibilidade e informações sensíveis, incluindo os administradores do Google Workspace for Education, o Google oferece o Programa Proteção Avançada (PPA). O PPA fornece aos usuários mais proteção contra ataques direcionados, como phishing, downloads nocivos e vazamento de senha. O programa foi especificamente criado para impedir ataques on-line direcionados às Contas do Google. Ele usa automaticamente um método de autenticação forte e chaves de segurança, além de restringir o acesso de terceiros aos dados da conta. Outros provedores de contas on-line também oferecem recursos de proteção robustos para usuários de alto risco. Os administradores e funcionários precisam sempre usar esse tipo de recurso caso tenham acesso a informações pessoais ou sistemas de tecnologia.

Faça a atualização e upgrade dos sistemas

Uma das medidas mais importantes que qualquer pessoa pode tomar para se proteger é manter os aplicativos e sistema operacional do dispositivo sempre atualizados. Isso é ainda mais importante no caso das instituições de ensino fundamental e médio, já que essas ferramentas são essenciais no dia a dia e na vida escolar dos estudantes. A maioria dos ataques de malware no setor educacional e em outros contextos de alto risco é baseada no Windows. Isso inclui o incidente da SolarWinds, os ataques de ransomware no Distrito Escolar Unificado de Los Angeles e no Distrito Escolar de Albuquerque, a invasão de hacker ao Distrito Escolar de Little Rock, o vazamento de dados do Microsoft Exchange Server e a recente violação dos e-mails de uma agência federal americana no sistema da Microsoft. Esse é mais um ambiente onde o uso de produtos e serviços em nuvem facilita o trabalho dos administradores, porque diminui a superfície de ataque e garante que os sistemas e aplicativos sejam atualizados automaticamente.

Faça upgrade para um sistema operacional mais recente e o mantenha atualizado

A versão mais recente de um sistema operacional (SO) normalmente inclui novos recursos de segurança que ajudam a evitar vetores de ataque conhecidos. É preciso ativar a funcionalidade de atualização automática no SO do dispositivo ou, caso isso não esteja disponível, fazer o download de patches e atualizações de um fornecedor confiável e os instalar pelo menos a cada mês.

Como os Chromebooks executam o ChromeOS, eles recebem atualizações frequentes e automáticas com os patches de segurança mais recentes, o que viabiliza a rápida adoção das inovações de proteção mais avançadas. Além disso, esses dispositivos verificam a integridade do sistema operacional somente leitura antes da inicialização. Eles também criptografam todos os dados armazenados no dispositivo para impedir o acesso não autorizado e executar cada página da Web e aplicativo em um sandbox separado. Assim, se um site ou app estiver infectado com malware, ele não vai se espalhar para outras partes do dispositivo.

Se sua escola não estiver pronta para adotar os Chromebooks, use o ChromeOS Flex, uma versão do ChromeOS criada para modernizar os dispositivos da sua instituição. O ChromeOS Flex proporciona aos usuários uma experiência moderna e unificada de ensino e aprendizado com recursos proativos e integrados de gerenciamento baseado na nuvem e de segurança. O Flex inclui proteção automatizada e bloqueia os apps e executáveis maliciosos sem substituir o hardware atual.

Faça upgrade para um navegador mais recente e o mantenha atualizado

É importante que o navegador também esteja atualizado e protegido. Os navegadores mais recentes oferecem recursos de segurança mais avançados, incluindo instruções para os usuários os ativarem com facilidade. Além disso, os administradores podem habilitar esses recursos por padrão nos computadores da instituição, o que ajuda a proteger a confidencialidade das informações sensíveis que estão em trânsito na Internet. É essencial que os navegadores estejam sempre atualizados. Seja para o usuário trabalhar, aprender ou realizar outra atividade on-line, com um navegador mais recente e atualizado, é possível fazer o seguinte:

- **Implementar uma segurança robusta**, incluindo o isolamento de sites e navegação segura para evitar que os usuários acessem sites perigosos sem querer
- **Ativar as atualizações automáticas** para garantir que o navegador receba recursos de segurança recentes com rapidez
- **Garantir uma conexão segura,** porque os navegadores mais recentes usam o protocolo Transport Layer Security, e os usuários podem clicar ao lado do URL e verificar se a conexão é considerada segura

O Chrome foi criado com foco na segurança, com recursos como a Navegação segura ativados por padrão. E também há um gerenciador de senhas integrado que as preenche automaticamente quando você navega pela Web, o que facilita o uso de senhas fortes.

Use sistemas de alerta e monitoramento em tempo real

Com sistemas de alerta e monitoramento em tempo real, as escolas podem identificar e solucionar ameaças com rapidez, antes que elas causem problemas. É importante que as ferramentas de segurança estejam em execução em segundo plano para coletar e registrar ocorrências de segurança em todos os sistemas. As ferramentas de IA são muito boas em analisar grandes volumes de dados coletados para encontrar anomalias e padrões. Essas descobertas podem ser usadas para detectar ameaças com mais rapidez e facilidade, além de processar e solucionar vulnerabilidades. Assim, é possível priorizar quais atividades os funcionários ou o administrador de TI precisam revisar.

As escolas podem usar recursos de alerta e monitoramento integrados ao software principal de colaboração e comunicação, como o Google Workspace for Education, ou implantar soluções separadas de gerenciamento de eventos e informações de segurança (SIEM).

Os sistemas de alerta e monitoramento em tempo real rastreiam várias atividades com relação à rede, dispositivos, aplicativos, usuários e dados de uma escola, como logins, acesso a arquivos, possíveis invasões, tentativas malsucedidas ou bem-sucedidas de roubo de dados e operações do administrador.

Quando o sistema detecta atividades suspeitas, ele envia um alerta para a equipe de TI da escola. Assim, os administradores podem investigar o problema e entrar em ação para solucionar a ameaça.

Além disso, é possível usar as ferramentas de alerta e monitoramento para coletar informações mais aprofundadas sobre as ameaças à escola. Com a análise de dados nesses sistemas em tempo real, as escolas identificam tendências e padrões que as ajudam a aprimorar a segurança.

.

Confira algumas práticas recomendadas sobre o uso de sistemas de alerta e monitoramento (incluindo o SIEM):

1. **Defina metas de segurança**
   Identifique quais informações e sistemas são mais importantes para a escola e que tipos de ameaça representam os maiores riscos. Depois, tente identificar os dados que você precisa coletar para monitorar essas ameaças.

2. **Colete os dados certos e defina configurações corretamente**
   É importante coletar os dados certos e configurar os aplicativos para alcançar as metas de segurança mais relevantes. Isso inclui dados de firewalls, filtros de conteúdo, sistemas de detecção de intrusões, servidores da Web e outros dispositivos de segurança, além do software de colaboração e comunicação e dos sistemas de informações da escola e de gestão de aprendizagem.

3. **Investigue e responda aos alertas**
   Quando o sistema de monitoramento gera um alerta, é essencial investigar o problema e tomar a medida apropriada. Isso envolve a colaboração de várias equipes para investigar a fonte do alerta, determinar se representa um falso positivo ou tomar as medidas cabíveis para solucionar a ameaça. Por exemplo, suspender contas, redefinir as senhas dos usuários, excluir e-mails ou colocá-los em quarentena, alterar as permissões de arquivos ou apagar a memória dos dispositivos.

Treine os professores, funcionários e estudantes

As instituições de ensino fundamental e médio precisam conscientizar os usuários sobre segurança e os hábitos relacionados nas comunidades escolares usando campanhas e parcerias. É essencial orientar os professores, funcionários e estudantes quanto à importância da segurança para que eles possam se proteger on-line e evitar ameaças graves de segurança cibernética. Ensine a essas pessoas como usar os produtos e serviços que sua instituição adota, como identificar e denunciar ameaças como e-mails de phishing e, principalmente, como impedir esses ataques.

Como usar dispositivos e softwares com segurança

Os administradores podem formar parcerias com professores e profissionais especializados em desenvolver currículos de segurança cibernética adequados às faixas etárias. O objetivo é ajudar os estudantes a entender como usar dispositivos, softwares e sistemas com segurança. Quando uma escola ou distrito escolar cria materiais de treinamento, eles podem contextualizar as recomendações para os professores e estudantes. No entanto, também é possível utilizar conteúdo pronto e personalizar esses materiais de acordo com suas necessidades. Os exemplos incluem o Seja Incrível na Internet, disponível em Safety.Google, e a Khan Academy. Esses programas mantêm os usuários seguros onde quer que estejam, seja na escola ou na própria comunidade.

Como reconhecer ameaças

Treinar os professores, funcionários e estudantes para reconhecer ameaças é essencial para manter essas pessoas seguras. É preciso ensinar às crianças essa habilidade de reconhecimento, porque elas podem não ter a capacidade de saber quando algo é realmente legítimo. Há alguns tipos de ameaças que elas precisam reconhecer e entender como denunciar. Além disso, é essencial que os administradores se concentrem nos temas que vão poder gerar um retorno do investimento maior. O treinamento precisa ensinar não só como reconhecer uma ameaça, mas também como proceder. As ameaças comuns que os usuários precisam reconhecer incluem ransomware, phishing, engenharia social, malware e golpes. No entanto, se um tipo de ameaça é mais predominante em uma determinada instituição, é importante que a comunidade escolar saiba tudo sobre ela.

Proteja o compartilhamento de arquivos e dados

Os professores e funcionários precisam receber treinamento sobre o compartilhamento adequado de arquivos e dados, além de como reconhecer solicitações inapropriadas enviadas por e-mail. O mais importante é que as informações pessoais sensíveis sejam compartilhadas ou processadas apenas quando necessário ou que incluam camadas adicionais de proteção. Por exemplo, nunca compartilhar esses dados por e-mail ou com partes externas. Os professores e funcionários precisam usar recursos de prevenção contra perda de dados (incluídos no ChromeOS e Workspace for Education) para alertar e impedir os usuários finais de compartilhar arquivos que incluam dados sensíveis (como CPF ou CNPJ) ou copiar e colar conteúdo confidencial fora do domínio.

A abordagem do Google na prática: dispositivos e serviços para educação

A compra de softwares é um dos melhores métodos que um distrito escolar pode ter para se proteger. O software precisa ter uma arquitetura e design robustos para diminuir os riscos de vulnerabilidades, com segurança integrada em todas as camadas. A exigência de que as escolas comprem softwares seguros ou fornecidos por empresas com um histórico de segurança comprovado diminui de maneira significativa os riscos cibernéticos mais amplos. No Google, por exemplo, fortalecemos o ChromeOS sem deixar de implantar soluções mais proativas e inteligentes que aproveitam os pontos fortes da nossa experiência em aprendizado de máquina, nuvem e identidade.

O Google tem o compromisso de criar produtos que ajudem a proteger a privacidade de estudantes e professores, além de oferecerem a melhor segurança da categoria para sua instituição. Os produtos e serviços do Google for Education merecem sua confiança porque protegem usuários, dispositivos e dados continuamente contra ameaças cada vez mais complexas. Esta seção oferece aos administradores de TI nas escolas recomendações de segurança ao usar os produtos do Google for Education.

Google Workspace for Education

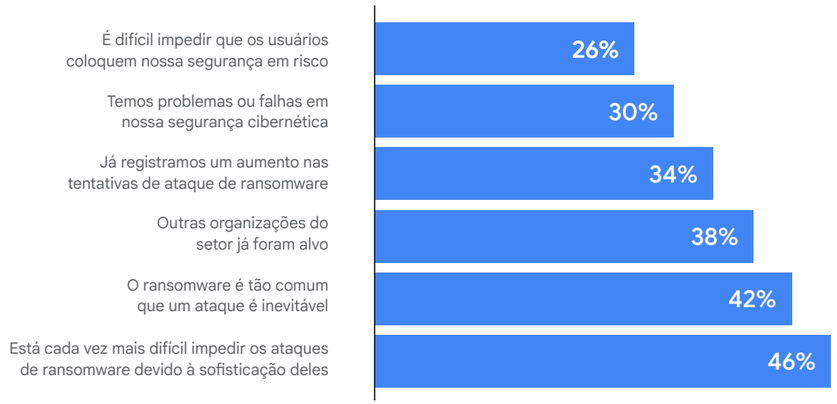
O Google Workspace for Education é um conjunto de ferramentas e serviços adaptados às escolas para viabilizar a colaboração, simplificar o ensino e manter o aprendizado seguro. Os produtos e serviços do Google for Education protegem usuários, dispositivos e dados continuamente contra ameaças cada vez mais complexas. Além disso, eles oferecem ferramentas como alertas e centrais de segurança, o Vault para e-discovery, prevenção contra perda de dados e gerenciamento de identidade e acesso.

Criamos materiais úteis para ajudar você caso esteja começando a usar o Google Workspace for Education. Além disso, boa parte desse conteúdo oferece orientações para você definir suas configurações com base nas dicas deste guia. Se quiser ajuda para começar a usar o Google Workspace for Education, consulte este Guia de início rápido sobre configuração de TI.

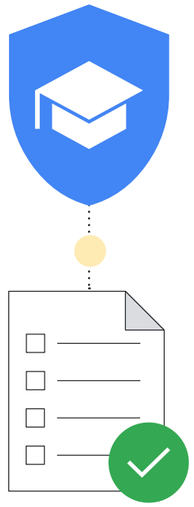
Listas de verificação de segurança

Confira as listas de verificação de segurança para saber mais sobre como reforçar a proteção e a privacidade da sua instituição. As escolas que usam as edições Standard e Plus do Google Workspace for Education também têm acesso à página Integridade da segurança para monitorar as configurações do Admin Console. Por exemplo, é possível verificar o status de configurações como o encaminhamento automático de e-mail, a criptografia de dispositivos, as configurações de compartilhamento do Drive e muito mais. Se precisar, ajuste as configurações do seu domínio com base nas práticas recomendadas e nas diretrizes gerais de segurança e adapte essas diretrizes às necessidades comerciais e à política de gerenciamento de riscos da sua organização.

Por que o setor de educação pode ser atingido



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



Confira a seguir outras dicas para aproveitar ao máximo os recursos de proteção incluídos no Google Workspace for Education:

Configure unidades organizacionais (UOs)

É fato que todas as pessoas incluídas na sua conta do Google Workspace for Education precisam ter as mesmas configurações. As unidades organizacionais são grupos de usuários que permitem atribuir diferentes serviços, configurações e permissões a diferentes usuários. Por exemplo, é possível aplicar a 2SV para os professores e funcionários e usar a autenticação adequada à faixa etária dos estudantes mais jovens. Configure unidades organizacionais separadas para funcionários, professores e estudantes. Assim, é possível aplicar políticas a cada grupo de usuários de forma separada. Uma estrutura bem definida é essencial para gerenciar sua conta do Google Workspace for Education com eficiência e flexibilidade.

Defina políticas de senha e proteções da conta do administrador

Como você já sabe, a autenticação dos usuários é essencial para manter sua instituição segura. É por isso que oferecemos aos administradores maneiras flexíveis de gerenciar a autenticação para fornecer aos usuários uma proteção de conta reforçada e apropriada. Defina políticas de senha para que os usuários criem senhas fortes e exija o uso da 2SV quando apropriado, com base nos agrupamentos recomendados na seção Logon único. É possível aplicar o uso da 2SV em um subconjunto de usuários (dando tempo para eles realizarem as devidas configurações) e implantar essa abordagem usando vários métodos, incluindo: chaves de segurança (opção mais segura), uma solicitação do Google (usando os apps do Google para Android e iOS), apps geradores de verificação (como o Google Authenticator) e mensagens de texto ou ligações telefônicas (apesar de serem os métodos menos seguros).

É possível definir o logon único (SSO) por meio de um provedor de identidade (IdP) externo caso sua empresa não use o Google para fazer isso. Se quiser, você ainda pode usar a 2SV com o SSO nas contas que não sejam de superadministrador.

Ative ou desative serviços

Os administradores podem controlar quais serviços do Google os usuários acessam com a conta do Google Workspace for Education no Google Admin Console. Para controlar o acesso aos serviços do Google como Agenda, Drive e Meet, basta ativar ou desativar esses serviços de acordo com a unidade organizacional (a ativação também pode ser feita ao usar grupos). Também é possível conferir as diferenças entre os serviços básicos e adicionais do Workspace antes de ativar opções extras como o YouTube, Google Maps e Blogger. Recomendamos aos administradores que configurem o acesso aos serviços do Google com base na faixa etária. No caso dos usuários com menos de 18 anos, são aplicadas restrições automaticamente a alguns serviços do Google após o login na conta do Google Workspace for Education.

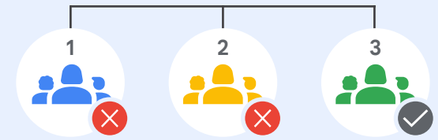
Você também pode usar o acesso baseado no contexto, disponível nas edições Standard e Plus do Workspace for Education, para permitir ou negar o acesso a apps do Google, como Gmail, Drive e Agenda. Isso pode ser feito com base nas características de um dispositivo, como endereço IP, origem geográfica, políticas de segurança ou SO. Por exemplo, permita o Drive para computador apenas em dispositivos da empresa em países/regiões específicos.

Métodos para conceder aos usuários acesso aos serviços

No Google Admin Console, você pode desativar o acesso de uma unidade organizacional a um Serviço do Google, como o Google Drive. Se alguns usuários dessa unidade organizacional precisarem usar o Drive, você terá duas opções:

1. Mova os usuários para uma unidade organizacional com o Drive ativado.
2. Adicione os usuários a um grupo de acesso e ative o Drive para o grupo. Cada participante poderá acessar o serviço, ainda que ele esteja desativado na unidade organizacional.

Unidades organizacionais



O Google Drive está desativado para as unidades organizacionais 1 e 2.

Em um grupo de acesso

No entanto, um **grupo de usuários** nas unidades organizacionais 1 e 2 pode acessar o Google Drive

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

Defina políticas de compartilhamento e regras de retenção de dados

O papel de administrador permite controlar se os usuários podem compartilhar os arquivos e pastas do Google Drive com pessoas fora da organização. Isso ajuda a evitar o compartilhamento não intencional ou em excesso de dados e arquivos, o que impede vazamentos. É importante separar arquivos e drives, criar unidades organizacionais e operar com base no princípio de privilégio mínimo. Assim, você impede que os invasores se movimentem pelas redes caso consigam se infiltrar em uma conta. Quanto menos dados e redes um possível invasor pode acessar, menor é o dano causado.

Desative o compartilhamento externo de arquivos para os estudantes (ou limite esse recurso apenas a domínios permitidos) e defina "Verificador de acesso" como "Somente destinatários". Se você permite que alguns ou todos os usuários compartilhem arquivos para fora do seu domínio, ative a exibição de um aviso, que é mostrado antes do compartilhamento. Outra dica é desativar a publicação de arquivos na Web e exigir que os colaboradores externos façam login com uma Conta do Google.

Os clientes das edições Standard e Plus do Workspace for Education também podem usar os recursos Públicos-alvo e Regras de confiabilidade para definir restrições e recomendações de compartilhamento com mais granularidade. Por exemplo, use os públicos-alvo para determinar que os professores possam compartilhar links apenas com "professores e funcionários" por padrão, e não com todas as pessoas da sua instituição. Com as regras de confiabilidade, você impede que estudantes do ensino fundamental compartilhem arquivos com alunos mais velhos.

No caso dos drives compartilhados, defina as políticas relacionadas para permitir que eles só possam ser criados por usuários apropriados e para impedir usuários externos de acessar esses drives. O recomendado é que apenas os administradores (ou funcionários e professores) possam criar drives compartilhados, e que você gerencie de perto o acesso a esses drives.

Limite a visibilidade e o compartilhamento de contatos do Diretório quando possível. Para isso, desative o compartilhamento de contatos para alguns ou todos os usuários e crie diretórios personalizados para limitar quem fica visível para quem.

Defina políticas de prevenção contra perda de dados (DLP) no Drive e no Gmail para detectar e bloquear informações sensíveis. Há opções pré-criadas que você pode usar para proteger informações sensíveis comuns, como números de cartão de crédito e contas bancárias. Além disso, é possível criar políticas personalizadas com base em palavras-chave, listas de palavras e expressões regulares (regex).

Gerencie as configurações do Gmail

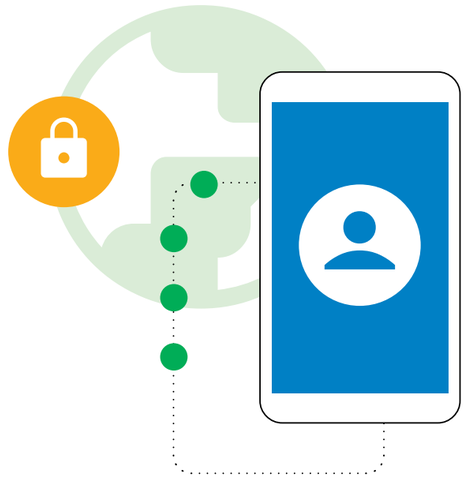
O Gmail é um dos principais serviços do Google Workspace for Education e oferece muitas configurações que os administradores podem usar para proteger a instituição e os usuários. Evite o spam, spoofing e phishing com a autenticação do Gmail. Personalize as configurações de filtro de spam, incluindo a exigência de autenticação para todos os remetentes aprovados, e proíba os usuários internos de desativar esses filtros.

Desative o acesso por POP/IMAP quando possível e ative a verificação aprimorada de mensagens antes da entrega e a proteção avançada contra phishing e malware. Se você permitir que alguns ou todos os usuários enviem e-mails para fora da sua instituição, ative os avisos de destinatário externo.

Os clientes das edições Standard e Plus do Workspace for Education também podem se proteger contra malware e ransomware com a definição de regras para detectar anexos nocivos usando o sandbox de segurança.

Aplicativos de terceiros

Use fluxos de trabalho integrados para aprovar aplicativos de terceiros que acessam os dados das contas com APIs. Assim, você impede o compartilhamento não autorizado de dados com aplicativos externos que não foram aprovados para uso na escola.



Relatórios e monitoramento

O papel de administrador permite consultar relatórios e eventos de registro no Google Admin Console para analisar a atividade na sua organização (como possíveis riscos à segurança), monitorar quem faz login e quando e entender como os usuários criam e compartilham conteúdo. Também é possível visualizar os dados do domínio e informações detalhadas sobre os usuários em gráficos e tabelas. Confira relatórios e registros de auditoria (incluindo a central de alertas) para identificar os riscos à segurança, analisar o uso dos serviços, diagnosticar os problemas de configuração, monitorar a atividade dos usuários e muito mais.

Os administradores das edições Standard e Plus do Google Workspace for Education podem utilizar o Painel de segurança para ter uma visão geral de diferentes relatórios de segurança, identificar tendências e comparar dados históricos e atuais. Por exemplo, o compartilhamento de arquivos no Drive, mensagens de spam, phishing e malware no Gmail, logins suspeitos em contas de usuário e atividades incomuns nos dispositivos. A maioria dos registros de auditoria, atividade e uso (incluindo os eventos de registro do Chat, administrador, Drive e Meet) e dos relatórios de segurança abrange um período de seis meses.

Aproveite a central de segurança

Os administradores das edições Standard e Plus do Google Workspace for Education têm acesso à central de segurança. Lá, eles encontram análise de dados e informações avançadas sobre segurança e têm mais visibilidade e controle sobre os problemas de proteção que afetam o domínio.

A central inclui a ferramenta de investigação de segurança, que ajuda os administradores a identificar, categorizar e solucionar problemas de proteção e privacidade, como ataques de phishing, compartilhamentos inapropriados de arquivos, atividades suspeitas de usuários e dispositivos e muito mais.

O Google Workspace é o pacote de comunicação e colaboração nativo da nuvem mais seguro do mundo

0

vulnerabilidades de software exploradas no Google Workspace desde novembro de 2021*

50%

de economia no pagamento de prêmios de seguro cibernético com o Google Workspace

2x menos

incidentes de segurança nas organizações que usam o Google Workspace em comparação com as que utilizam o Microsoft 365

2.5x menos

incidentes de segurança nas organizações que usam o Google Workspace em comparação com as que utilizam o Microsoft Exchange

* De acordo com a CISA, esse número é consideravelmente menor em comparação com outros fornecedores de recursos de produtividade do mercado.

Google Chromebooks para educação

Professores e estudantes usam com facilidade os Chromebooks, computadores muito seguros e escalonáveis, graças aos recursos de segurança integrados e prontos para utilização. Nunca nenhum ataque de ransomware foi reportado nos dispositivos ChromeOS de empresas, escolas ou consumidores. Os Chromebooks usam recursos atualizados para proteger as escolas contra ameaças em constante evolução. As atualizações acontecem automaticamente em segundo plano para que os usuários voltem para suas tarefas em poucos segundos.

Atualizações automáticas do SO e aplicativo, com proteção integrada contra malware

Os invasores estão sempre tentando tirar proveito dos bugs e falhas nos sistemas operacionais, navegadores e apps conhecidos para instalar malware e roubar os dados dos usuários. Para proteger você e seus usuários, os Chromebooks sempre executam o SO e os aplicativos mais recentes porque esses dispositivos são seguros por padrão graças às atualizações de segurança. Além disso, o software dos aplicativos na nuvem não exigem atualização da mesma maneira que o de apps locais. O chip de segurança desenvolvido pelo Google e incorporado aos Chromebooks mantém os dispositivos seguros, protege a identidade dos usuários e garante a integridade do sistema.

Os Chromebooks da sua frota de dispositivos executam automaticamente as atualizações mais recentes de proteção contra malware. Os estudantes e educadores ficam protegidos contra ameaças cibernéticas graças aos recursos integrados de segurança como criptografia de dados, inicialização verificada, sandbox e atualizações automáticas.

Proteja os dados do usuário

Quando você faz login em um Chromebook usando a Conta do Google, todos os seus dados são armazenados em arquivos criptografados. Isso garante que nenhuma outra pessoa no dispositivo possa acessar seus dados ou fazer login em aplicativos usando sua conta. Assim, os estudantes compartilham dispositivos em uma sala de aula e as escolas diminuem o custo total de computação, tudo com muita facilidade e segurança. Para garantir recursos de segurança mais avançados, o Upgrade do Chrome Education, a licença de gerenciamento de dispositivos, oferece visibilidade aprimorada.

Políticas de segurança remotas nos dispositivos gerenciados pelo usuário

Os administradores de escolas podem definir políticas do ChromeOS e instalar/atualizar os aplicativos remotamente usando o Google Admin Console. Com apenas um clique, o administrador de TI pode atualizar as políticas e configurações de centenas de milhares de Chromebooks de uma só vez.

Isso garante que:

- Os estudantes só possam acessar aplicativos e conteúdo aprovados pela escola;
- Todos os aplicativos e extensões sejam atualizados com as correções de segurança mais recentes;
- Os usuários não possam copiar, transferir ou compartilhar dados da escola para fora do dispositivo;
- Os administradores tomem decisões baseadas em dados com as recomendações de segurança personalizadas do Google para lidar com ameaças;
- Os administradores gerenciem de maneira centralizada as políticas de segurança e gerenciamento de identidade e acesso de todos os usuários direto do Admin Console.

Estas são algumas políticas importantes que os administradores precisam configurar:

Políticas de dispositivos

- **Modo convidado**
  É recomendado desativar o modo convidado nos dispositivos para que os estudantes e professores façam login usando as próprias credenciais, em vez de permanecerem anônimos.
- **Restrições de login**
  Não é recomendado que os estudantes e professores usem contas pessoais do Gmail para fazer login nos Chromebooks da escola. Limite os logins apenas ao domínio do Workspace nos dispositivos usados exclusivamente pelos estudantes.
- **Relatórios de usuários e dispositivos**
  Os administradores precisam ativar os relatórios de usuários e dispositivos para coletar métricas sobre como os Chromebooks são usados, quem os utiliza e o estado do hardware.
- **Nova inscrição forçada**
  Éessencial que os Chromebooks de uma escola permaneçam nela, a menos que o administrador faça seu desprovisionamento. Os administradores precisam ativar as novas inscrições forçadas nos Chromebooks para que esses dispositivos se registrem novamente no caso de exclusão permanente ou tentativa de roubo.

Políticas de usuário

- **Modo de navegação anônima**
  Você precisa garantir a melhor experiência para os estudantes na hora de usar os Chromebooks da escola. Isso inclui limitar os usuários ao navegador autenticado para que os filtros de conteúdo da Web evitem o acesso a sites inapropriados. Os administradores precisam desativar o modo de navegação anônima para que os estudantes não consigam driblar os filtros da Web.
- **Modo de proxy**
  Mesmo que algumas escolas usem proxies nos filtros da Web, é importante desativar a capacidade dos usuários de alterar as configurações de proxy.
- **Acesso por login múltiplo**
  Quando os usuários têm permissão para fazer login em uma conta secundária nos Chromebooks e Workspace da escola, isso dá a eles a oportunidade de exfiltrar com facilidade as informações/dados sensíveis da instituição ou dos estudantes para essa conta. Os administradores precisam bloquear o acesso por login múltiplo.
- **Histórico do navegador**
  No caso dos estudantes, vale a pena desativar a capacidade de limpar o histórico do navegador. Se um incidente de segurança na Internet acontecer, esses registros do histórico vão ajudar nas investigações.

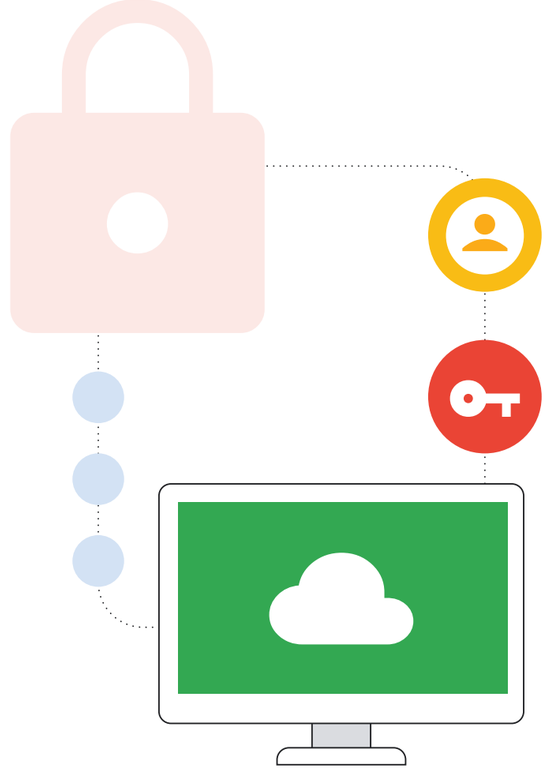
Essa lista é um ótimo ponto de partida para você proteger suas redes contra os tipos mais comuns de erros que produzem incidentes cibernéticos significativos. Você encontra mais políticas de proteção recomendadas na nossa Lista de verificação de segurança.

Gerenciamento de endpoints para proteger o uso em qualquer momento e lugar

Com o sistema de gerenciamento remoto de políticas do ChromeOS, os administradores de escolas aplicam configurações de proteção e executam ferramentas de segurança como os filtros de conteúdo no dispositivo, e não nos servidores de rede da instituição. Assim, os estudantes aproveitam em casa os mesmos benefícios de segurança dos Chromebooks da escola, como se estivessem em sala de aula. Isso é cada vez mais importante porque as escolas estão adotando materiais digitais e ferramentas de aprendizado on-line, e os estudantes costumam levar os computadores para fazer as tarefas em casa.

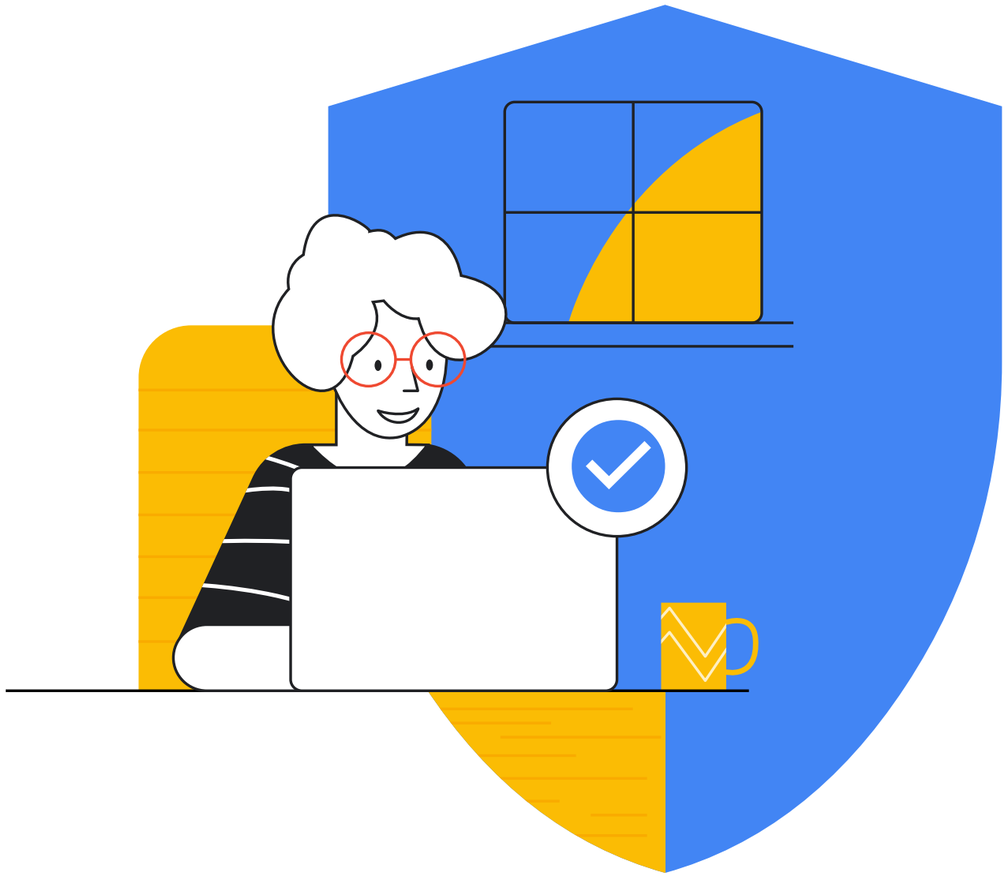
Conclusão

Proteger as instituições de ensino fundamental e médio contra incidentes cibernéticos é uma tarefa complexa e desafiadora. No entanto, garantir sua proteção e a dos estudantes, professores, funcionários e ecossistema on-line mais amplo é um investimento que vale a pena. Os itens abordados neste documento são um ótimo ponto de partida, mas cada escola precisa ajustar as recomendações de acordo com suas necessidades específicas e continuar acompanhando as novas tecnologias e o cenário de ameaças, que está em constante transformação. Esse recurso funciona como uma base sólida para todos os tipos de programa de segurança para ensinos fundamental e médio, incluindo as próximas etapas possíveis e as ações necessárias que podem ser implementadas. O Google também conta com vários recursos, treinamentos e profissionais especializados em segurança cibernética para ajudar as escolas e organizações a seguir as instruções deste guia e com relação a novas tecnologias, como a IA. Os produtos do Google personalizados para o setor educacional oferecem soluções prontas para os vários problemas de segurança cibernética descritos neste documento. Vamos adorar trabalhar com você na elaboração e implementação dos seus programas de segurança.



Lista de recursos

- Google. “Dicas de segurança on-line”. Central de segurança do Google, https://safety.google/security/security-tips/. Acessado em 6 de outubro de 2022.
- NIST. “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1”. NIST Technical Series Publications, 16 de abril de 2018, https://doi.org/10.6028/NIST.CSWP.04162018. Acessado em 6 de outubro de 2022.
- Microsoft. “Programa Microsoft AccountGuard”. Programa Microsoft AccountGuard, https://www.microsoftaccountguard.com/pt-pt/. Acessado em 6 de outubro de 2022.
- Google. “Programa Proteção Avançada.” Programa Proteção Avançada do Google, https://landing.google.com/advancedprotection. Acessado em 6 de outubro de 2022.
- Google. “Central de segurança do Google”. Central de segurança do Google – Maior proteção on-line, https://safety.google. Acessado em 6 de outubro de 2022.
- Meta. “Fundamentos básicos da Meta: proteja sua conta”. Proteger sua conta, https://www.facebook.com/gpa/resources/basics/security. Acessado em 6 de outubro de 2022.
- Meta. “Facebook Protect”. Facebook, https://www.facebook.com/gpa/facebook-protect. Acessado em 6 de outubro de 2022.
- NIST. “SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise”. NIST Technical Series Publications, https://doi.org/10.6028/NIST.SP.800-124r1. Acessado em 6 de outubro de 2022.
- Chaves de acesso: https://developers.google.com/identity/passkeys
- Relatório Protecting Our Future da CISA para segurança cibernética nos ensinos fundamental e médio: https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- Relatório do GAO (órgão de prestação de contas dos EUA): https://www.gao.gov/products/gao-20-644
- Para saber mais sobre como o Google for Education ajuda a proteger sua instituição, consulte nossa Central de privacidade e segurança.
- Relatório da Zcaler sobre phishing



Google for Education