NDI
NATIONAL DEMOCRATIC INSTITUTE

Manual de segurança cibernética

para

organizações da sociedade civil

Um guia para organizações da sociedade civil que desejam implantar um plano de segurança cibernética



NDI
NATIONAL DEMOCRATIC INSTITUTE

Manual de segurança cibernética

para

organizações da sociedade civil

Um guia para organizações da sociedade civil que desejam implantar um plano de segurança cibernética

Esta obra está licenciada sob a Creative Commons Attribution-ShareAlike 4.0 International License. Para ver uma cópia desta licença, visite http://creativecommons.org/licenses/by-sa/4.0/ ou envie uma carta para Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.



Índice

Legenda visual 4

Os 10 melhores 6

Autores e agradecimentos 7

Quem somos? 7

A quem se destina este manual? 8

O que é um plano de segurança e por que minha organização deveria adotar um? 8

Quais ativos sua organização possui e o que você deseja proteger? 9

Quem são seus adversários e quais são suas capacidades e motivações? 9

Quais ameaças sua organização enfrenta? Em que medida essas ameaças são plausíveis e de alto impacto? 10

Como criar um plano de segurança cibernética organizacional 11

Desenvolvimento de uma cultura de segurança 12

Integre a segurança em sua estrutura operacional regular 13

Obtenha adesão organizacional 14

Estabeleça um plano de treinamento 14

Uma base forte: Como proteger contas e dispositivos 16

Contas seguras: Senhas e autenticação de dois fatores 18

Dispositivos seguros 26

Phishing: Uma ameaça comum a dispositivos e contas 32

Comunicação e armazenamento de dados com segurança 37

Comunicações e compartilhamento de dados 38

Como armazenar dados com segurança 50

Como estar seguro na Internet 53

Navegação com segurança 54

Segurança de mídia social 64

Mantenha seus sites online 66

Proteja sua rede Wi-Fi 67

Proteção da segurança física 68

Proteção de ativos físicos 70

O que fazer diante de imprevistos 74

Apêndice A: Recursos recomendados 78

Apêndice B: Kit básico do plano de segurança 79

Legenda visual

Ao longo do manual, além do texto principal, há alguns elementos diferentes que são recorrentes e estão em destaque. Aqui está uma breve "legenda" para ajudá-lo a entender os elementos principais:



Estudo de caso

Indica estudos de caso que destacam o impacto na vida real de determinado tópico em organizações da sociedade civil mundialmente ou em um país específico.



Dicas extras

Destaca dicas e informações adicionais que merecem atenção durante a leitura do manual.



Mundo real

Designa exemplos comuns de ferramentas de táticas de segurança cibernética usadas no "mundo real", tanto para fins lícitos quanto ilícitos.



Avançado

Indica um tópico avançado, informações que são importantes para sua organização considerar, mas que podem ser um pouco mais técnicas ou complicadas.



Componentes básicos do plano de segurança

Indica os "Componentes básicos do plano de segurança", que são as principais conclusões de cada seção do manual.

1



Desenvolvimento de uma cultura de segurança

2



Uma base forte: Como proteger contas e dispositivos

3



Comunicação e armazenamento de dados com segurança

4



Como estar seguro na Internet

5



Proteção da segurança física

6



O que fazer diante de imprevistos

Os 10 melhores

Esses dez elementos são essenciais para o plano de segurança da sua organização. Se não sabe por onde começar, leia isto primeiro.

1. **Realize treinamentos regulares de segurança em sua organização.**
2. **Esteja alerta para evitar o phishing e mantenha um sistema de denúncias.**
3. **Use criptografia para todas as comunicações, de ponta a ponta, quando possível.**
4. **Exija senhas fortes e implemente um gerenciador de senhas em sua organização.**
5. **Exija autenticação de dois fatores sempre que possível.**
6. **Verifique se todos os dispositivos e softwares da equipe estão sendo atualizados.**
7. **Utilize armazenamento em nuvem seguro.**
8. **Use HTTPS e, se for o caso, uma VPN para acessar a Internet.**
9. **Proteja os ativos físicos da sua organização.**
10. **Desenvolva um plano organizacional de resposta a incidentes.**

Autores e agradecimentos

Autor principal: **Evan Summers (NDI)**
Autores contribuintes: **Sarah Moulton (NDI); Chris Doten (NDI)**

Ao desenvolver este manual, gostaríamos de agradecer especialmente aos nossos revisores externos especializados que nos forneceram feedback, edições e sugestões valiosas à medida que compilamos este conteúdo, incluindo:

Fiona Krakenburger, Open Technology Fund; Bill Budington e Shirin Mori, Electronic Frontier Foundation; Jocelyn Woolbright, Cloudflare; Martin Shelton, Freedom of the Press Foundation; Dave Leichtman, Microsoft; Stephen Boyce, International Foundation for Electoral Systems; Amy Studdart, International Republican Institute; Emma Hollingsworth, Global Cyber Alliance; Caroline Sinders, Convocation Design + Research; Dhyta Caturani; Sandra Pepera, NDI; Aaron Azelton, NDI; e Whitney Pfeifer, NDI.

Também queremos agradecer por todos os incríveis manuais, guias, pastas de trabalho, módulos de treinamento e outros materiais desenvolvidos e mantidos pela Comunidade de Segurança Organizacional (OrgSec). Este manual foi desenvolvido para complementar esses materiais mais aprofundados, combinando lições importantes em um recurso único e fácil de ser lido para organizações da sociedade civil que desejam iniciar um plano de segurança cibernética.

Além da inspiração indireta que extraímos de diversos recursos extraordinários compilados pela comunidade, também copiamos diretamente a linguagem útil de vários recursos existentes e a aplicamos ao longo deste manual, principalmente o Guia de autodefesa contra vigilância da **Electronic Frontier Foundation**, o Manual de segurança holística da **Tactical Tech** e uma série de explicadores do **Center for Democracy and Technology** e da **Freedom of the Press Foundation**. Você pode encontrar citações específicas a esses recursos nas seções abaixo e links completos, autores e informação sobre licenças no **Apêndice A**.

Também recomendamos que qualquer pessoa que leia este manual faça uso da extensa **biblioteca** de guias e recursos de segurança digital compilados e atualizados pelo Open Technology Fund.

Quem somos?

O National Democratic Institute for International Affairs (NDI) é uma organização apartidária, sem fins lucrativos, com sede em Washington DC, que desenvolve um trabalho mundial através de parcerias para fortalecer e salvaguardar instituições, processos, normas e valores democráticos. O objetivo é garantir uma melhor qualidade de vida para todos.

O NDI acredita que todas as pessoas têm o direito de viver em um mundo que respeite sua dignidade, segurança e direitos políticos, e o ambiente digital faz parte desse mundo.

Dentro do NDI, o time de Democracia e Tecnologia busca promover um ecossistema digital global onde os valores democráticos sejam protegidos, promovidos e possam prosperar, os governos sejam mais transparentes e inclusivos, e todos os cidadãos sejam empoderados a responsabilizar seu governo. Fazemos esse trabalho ao apoiar uma rede global de ativistas comprometidos com a resiliência digital e por meio da colaboração com parceiros em ferramentas e recursos como este manual. Para saber mais sobre o trabalho que fazemos, acesse nosso **site**, siga nossa página no **Twitter** ou entre em contato diretamente pelo e-mail **cyberhandbook@ndi.org**. Estamos à disposição para ouvi-lo e esclarecer dúvidas sobre nosso time e nosso trabalho em segurança cibernética, tecnologia e democracia.

A quem se destina este manual?

Este manual foi preparado com um objetivo simples em mente: ajudar organizações da sociedade civil a desenvolver um plano de segurança cibernética compreensível e implementável.

À medida que o mundo migra cada vez mais para a modalidade online, a segurança cibernética deixa de ser apenas uma palavra da moda, e passa a ser vista como um conceito crítico para o sucesso de uma organização e a segurança de um time. Em especial, para organizações da sociedade civil nos espaços de democracia, advocacia, prestação de contas e direitos humanos, a segurança da informação (tanto online quanto offline) é um desafio que requer foco, investimento e vigilância.

Sua organização provavelmente será, se já não tiver sido, alvo de um ataque de segurança cibernética. A intenção aqui não é alarmar, mas sim falar de um fato que é realidade até mesmo para as organizações que não se consideram alvos de fato.

Em um ano médio, o Center for Strategic and International Studies, que mantém uma lista atualizada do que consideram ser "incidentes cibernéticos significativos", cataloga centenas de ataques cibernéticos graves, muitos dos quais têm como alvo dezenas, senão centenas, de organizações simultaneamente. Além desses ataques denunciados, a cada ano, provavelmente há centenas de outros ataques menores que não são detectados ou relatados, muitos deles direcionados a organizações da sociedade civil que trabalham para apoiar a democracia, a responsabilidade e os direitos humanos. Muitas vezes, organizações que representam mulheres ou outros grupos marginalizados são particularmente visadas.

Ataques cibernéticos como esses têm consequências significativas. Se o objetivo é ter acesso ao seu dinheiro, reprimir sua voz, atrapalhar suas operações organizacionais, manchar sua reputação ou até mesmo roubar informações que podem causar danos psicológicos ou físicos aos seus parceiros ou funcionários, essas ameaças precisam ser levadas a sério. A boa notícia é que você não precisa se tornar um codificador ou tecnólogo para defender a si mesmo e sua organização contra ameaças desse tipo. No entanto, você precisa estar preparado para investir esforço, energia e tempo no desenvolvimento e implementação de um plano de segurança organizacional que seja forte. Se você nunca pensou em segurança cibernética na sua organização, não teve tempo de se concentrar nela, ou conhece algumas noções básicas sobre o tema, mas acha que sua organização poderia melhorar sua própria segurança cibernética, este manual foi feito para você. Independentemente de sua origem, este manual tem como objetivo fornecer à sua organização as informações essenciais necessárias para implementar um plano de segurança sólido. Um plano que ultrapasse o simples ato de colocar palavras no papel e possibilita que as melhores práticas sejam colocadas em ação.

O que é um plano de segurança e por que minha organização deveria adotar um?

Um plano de segurança é o conjunto de políticas, procedimentos e instruções escritas que foi definido por sua organização para alcançar o nível de segurança que você e seu time consideram adequados para proteger seus colaboradores, parceiros e informações.

Um plano de segurança organizacional bem elaborado e atualizado reforça a segurança e eficácia de uma organização, proporcionando a tranquilidade necessária para que os colaboradores se concentrem no importante trabalho diário que precisam desenvolver. Sem pensar em um plano abrangente, é muito fácil não enxergar certos tipos de ameaças, mantendo foco excessivo em determinado risco ou ignorando a segurança cibernética até que uma crise aconteça. Quando você começa a desenvolver um plano de segurança, há algumas perguntas importantes para fazer a si mesmo que formam um processo conhecido como **avaliação de risco.** Responder a essas perguntas ajuda sua organização a entender as ameaças exclusivas enfrentadas. Além disso, com esse questionamento, você consegue dar um passo para trás e pensar de forma abrangente sobre o que precisa de proteção, e contra quem. Avaliadores treinados, auxiliados por sistemas como a estrutura de auditoria SAFETAG da Internews, podem ajudar a conduzir sua organização nesse processo. É válido ter acesso a esse nível de conhecimento profissional, porém, mesmo que você não possa passar por uma avaliação completa, procure se reunir com sua organização para considerar cuidadosamente as questões-chave a seguir:

1 Quais ativos sua organização possui e o que você deseja proteger?

Você pode começar a responder a essas perguntas **criando um catálogo de todos os ativos da sua organização**. Informações como mensagens, e-mails, contatos, documentos, calendários e locais são todos ativos possíveis. Telefones, computadores e outros dispositivos podem ser ativos. Além disso, pessoas, conexões e relacionamentos também podem ser ativos. Faça uma **lista de seus ativos** e tente catalogá-los em ordem de importância para a organização, onde você os mantém (talvez vários locais digitais ou físicos) e o que impede que outras pessoas os acessem, danifiquem ou interfiram neles. Tenha em mente que nem tudo tem a mesma importância. Se alguns dos dados da organização são uma questão de registro público ou informações que você já publica, não são segredos que você precisa proteger.

2 Quem são seus adversários e quais são suas capacidades e motivações?

"Adversário" é um termo comumente usado em segurança organizacional. Em termos simples, adversários são atores (indivíduos ou grupos) que estão interessados em atingir sua organização, atrapalhar seu trabalho e obter acesso ou destruir suas informações: os criminosos. Golpistas financeiros, concorrentes, autoridades ou governos locais ou nacionais, ou hackers com motivação política ou ideológica são exemplos de possíveis adversários. É importante fazer uma lista de seus adversários e pensar criticamente sobre quem pode querer gerar um impacto negativo na sua organização e sua equipe. Embora seja fácil imaginar atores externos (como um governo estrangeiro ou um grupo político específico) como adversários, lembre-se também de que os adversários podem ser pessoas que você conhece, como funcionários insatisfeitos, ex-funcionários e familiares ou parceiros que não desejam oferecer apoio. Diferentes adversários representam ameaças distintas e possuem recursos e capacidades diferentes para interferir nas suas operações e obter acesso ou destruir suas informações.

Por exemplo, os governos costumam dispor de elevado capital e recursos poderosos, incluindo a capacidade de desativar a Internet ou usar tecnologia de vigilância onerosa; as redes móveis e os provedores de Internet provavelmente têm acesso a registros de chamadas e históricos de navegação; hackers habilidosos em redes Wi-Fi públicas têm a capacidade de interceptar comunicações ou transações financeiras mal protegidas. Você pode até se tornar seu próprio adversário, por exemplo, ao excluir acidentalmente arquivos importantes ou enviar mensagens privadas para a pessoa errada.

É provável que os motivos dos adversários sejam diferentes de acordo com as capacidades, interesses e estratégias que possuem. Eles estão interessados em descreditar sua organização? Talvez eles tenham a intenção de silenciar sua mensagem? Ou talvez eles vejam sua organização como concorrente e queiram ganhar vantagem? É importante entender a motivação de um adversário visto que isso pode ajudar sua organização a avaliar melhor as ameaças que ele representa.

3 Quais ameaças sua organização enfrenta? Em que medida essas ameaças são plausíveis e de alto impacto?

Ao identificar possíveis ameaças, é provável que você acabe com uma longa lista, o que pode ser avassalador. Você pode sentir que qualquer esforço seria inútil ou não saber por onde começar. Para ajudar a capacitar sua organização a dar os próximos passos produtivos, é útil analisar cada ameaça com base em dois fatores: a probabilidade de que a ameaça possa acontecer; e o impacto que ela poderia causar.

Para medir a probabilidade de uma ameaça (talvez "baixa, média ou alta", com base nas chances de determinado evento provavelmente não acontecer, provavelmente acontecer ou acontecer com frequência), você pode usar informações que conhece sobre a capacidade e a motivação de seus adversários, análises de incidentes de segurança anteriores, experiências de outras organizações semelhantes e, claro, a presença de quaisquer estratégias de mitigação existentes que sua organização tenha implementado.

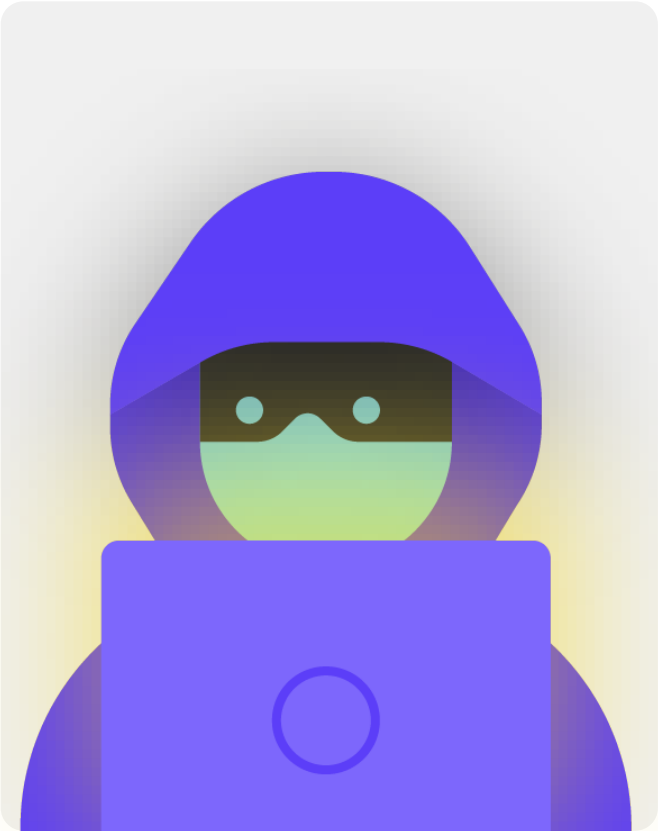
Para medir o impacto de uma ameaça, pense em como as coisas seriam se a ameaça realmente ocorresse. Faça perguntas como "Como a ameaça nos prejudicou como organização e como pessoas, física e mentalmente?", "Qual a duração do efeito?", "A ameaça dá origem a outras situações prejudiciais?" e "Como ela dificulta nossa capacidade de atingir nossos objetivos organizacionais agora e no futuro?" Ao responder a essas perguntas, considere se a ameaça é de baixo, médio ou alto impacto.

Depois de categorizar suas ameaças por probabilidade e impacto, comece a traçar um plano de ação mais informado. Ao se concentrar nas ameaças com maior probabilidade de acontecer E que terão impactos negativos significativos, você canalizará seus recursos limitados da maneira mais eficiente e eficaz possível.

Seu objetivo é sempre mitigar o máximo de risco possível, mas ninguém – nem o governo ou companhia com mais recursos do mundo – pode eliminar o risco por completo. E está tudo bem: você pode fazer bastante para proteger a si mesmo, seus colegas e sua organização ao cuidar das ameaças mais significativas.



Para ajudá-lo a gerenciar esse processo de avaliação de risco, considere usar uma planilha, como esta desenvolvida pela Electronic Frontier Foundation. Lembre-se de que as informações que você desenvolve como parte desse processo (como uma lista de seus adversários e as ameaças que eles representam) podem ser confidenciais, por isso é importante mantê-las em segurança.



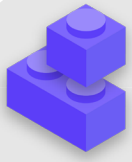
Como criar um plano de segurança cibernética organizacional

Embora o plano de segurança de cada organização pareça um pouco diferente com base em sua avaliação de risco e dinâmica organizacional, certos conceitos básicos são quase universais.

Este manual aborda esses conceitos essenciais de uma maneira que ajude sua organização a criar um plano de segurança concreto com base em soluções práticas e aplicativos do mundo real.

O manual procura oferecer opções e sugestões gratuitas ou de custo muito baixo. Lembre-se de que o custo mais significativo associado à implementação de um plano de segurança eficaz será o tempo que você e sua organização precisam para conversar, aprender e implementar seu novo plano. No entanto, considerando os riscos que sua organização provavelmente enfrentará, esse investimento valerá a pena.

Em cada seção, você encontrará uma explicação de um tópico-chave que sua organização e sua equipe devem conhecer: o que é e por que é importante. Cada tópico é combinado com estratégias, abordagens e ferramentas recomendadas que são essenciais para limitar seu risco, além de dicas e links para recursos adicionais que podem ajudá-lo a implementar essas recomendações em sua organização.



Kit básico do plano de segurança

Para ajudar sua organização a processar as lições do manual e transformá-las em um plano real, use este kit básico. Você pode imprimir o kit ou preenchê-lo digitalmente enquanto lê o manual online. Ao fazer anotações e começar a atualizar ou elaborar seu plano de segurança, certifique-se de consultar os "Componentes básicos do plano de segurança" detalhados em cada seção. Nenhum plano de segurança está completo sem, no mínimo, abordar esses elementos essenciais.



Aproveite outros recursos que também podem ajudá-lo a criar e implementar seu plano. Como uma organização da sociedade civil, o aplicativo gratuito **SOAP** (Securing Organizations with Automated Policymaking) pode ajudar a simplificar e automatizar a criação do seu plano de segurança.

Também faça uso de recursos de treinamento gratuitos, como o **Planejador de segurança** da Consumer Reports, o **aplicativo Umbrella da Security First**, o **Projeto Totem** da Free Press Unlimited e Greenhost, e o **Kit de ferramentas de segurança cibernética para organizações com uma missão social** da Global Cyber Alliance, que abrangem recursos em muitas das práticas recomendadas mencionadas neste manual e links que direcionam a dezenas de ferramentas de treinamento para ajudá-lo a implementar inúmeros princípios básicos.



Desenvolvimento de uma cultura de segurança

Desenvolvimento de uma cultura de segurança

Uma base forte: Como proteger contas e dispositivos

Comunicação e armazenamento de dados com segurança

Como estar seguro na Internet

Proteção da segurança física

O que fazer diante de imprevistos

Segurança tem tudo a ver com pessoas e, para proteger sua organização, você precisa garantir que todos os envolvidos levem a segurança cibernética a sério. Transformar a cultura é difícil, mas algumas etapas simples e conversas importantes podem ser fundamentais para criar uma atmosfera que aumentará a resiliência de sua equipe e organização diante das ameaças de segurança. Uma das etapas mais simples, mas também mais importantes a serem tomadas para construir essa cultura de segurança organizacional, é comunicá-la dentro de sua organização e ter líderes que sejam um exemplo de boa conduta.

Integre a segurança em sua estrutura operacional regular

Conforme descrito em detalhes no Guia de segurança holística da Tactical Tech, é essencial criar espaços regulares e seguros para falar sobre os diferentes aspectos da segurança.

Dessa forma, se os membros do time estiverem preocupados com a segurança, ficarão menos ansiosos diante da ideia de parecerem paranoicos ou desperdiçarem o tempo de outras pessoas. **Agendar conversas regulares sobre segurança** também normaliza a frequência de interação e reflexão sobre assuntos relacionados à segurança, para que os problemas não sejam esquecidos e os membros do time tenham maior probabilidade de trazer pelo menos uma conscientização passiva de segurança para seu trabalho contínuo. As conversas não precisam acontecer toda semana, mas lembre-se delas de forma recorrente. Essas discussões não devem apenas deixar espaço para tópicos de segurança técnica, mas também devem incluir questões que afetam o conforto e a segurança da equipe, como conflitos na comunidade, assédio online (e offline) ou problemas com o uso e implementação de ferramentas digitais. As conversas podem até incluir tópicos como hábitos de compartilhamento de informações offline e as formas como a equipe protege ou não as informações fora do trabalho. Afinal, é importante lembrar que a segurança de uma organização é tão forte quanto seu elo mais fraco. Uma maneira de conseguir um engajamento consistente é adicionar segurança à agenda de uma reunião regular. Também é interessante alternar a responsabilidade de organizar e facilitar uma discussão sobre segurança entre os membros da organização, o que pode ajudar a desenvolver a ideia de que a segurança é responsabilidade de todos e não apenas de alguns poucos selecionados ou da "Time de TI". À medida que você começa a formalizar a discussão sobre segurança, a equipe provavelmente se sentirá mais à vontade para discutir essas questões importantes entre si, bem como em ambientes menos formais.

Também é importante incorporar elementos de segurança ao funcionamento normal da organização, como durante a integração de funcionários, e pensar em cortar o acesso aos sistemas durante a demissão. A segurança não deve ser "mais uma preocupação", mas sim uma ***parte integral de sua estratégia e operações.***

Lembre-se de que todos os planos de segurança devem ser considerados documentos vivos e devem ser reavaliados e discutidos regularmente, sobretudo quando novos funcionários ou voluntários ingressam na organização ou quando o contexto de segurança sofre mudanças.

Plan to revisit your strategy and make updates annually, or if there are major changes in strategy, tools, or the threats you face.

Obtenha adesão organizacional

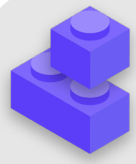
Parte de uma cultura de segurança bem-sucedida também é garantir a adesão de toda a sua organização ao seu plano de segurança.

Fundamentalmente, essa iniciativa deve incluir apoio e orientação forte e vocal dos líderes organizacionais que, em muitos casos, serão os que tomarão a decisão final de alocar tempo, recursos e energia para desenvolver e implementar um plano de segurança eficaz. Se eles não levarem a questão a sério, ninguém mais o fará. Para alcançar essa adesão em toda a organização, pense cuidadosamente sobre quando e como apresentar seu plano, faça-o com clareza, certifique-se de que a liderança reforce as mensagens e guie todos os elementos e etapas do plano para que não haja mistério ou confusão sobre o que você está tentando alcançar. Muitos doadores agora exigem que os donatários mantenham uma segurança forte, portanto, enfatizar essa necessidade para a equipe também é uma boa maneira de criar adesão organizacional mais profunda. Ao falar sobre segurança, evite táticas de susto. Às vezes, as ameaças que sua organização e sua equipe enfrentam podem ser assustadoras, mas tente se concentrar em compartilhar fatos e criar um espaço calmo para perguntas e preocupações. Fazer com que os perigos pareçam muito ameaçadores pode fazer com que as pessoas considerem você uma pessoa sensacionalista ou simplesmente desistam, pensando que nada do que fazem importa, e nada disso é verdade.

Estabeleça um plano de treinamento

Depois de desenvolver e se comprometer com um plano, pense em como você treinará todos os funcionários (e voluntários) sobre essas novas práticas recomendadas.

Exigir treinamento regular – e tornar obrigatória a participação no treinamento, contabilizando-a nas avaliações de desempenho da equipe – pode ser uma tática útil. Evite criar consequências rígidas e negativas para os funcionários que têm dificuldades com os conceitos de segurança. Lembre-se de que alguns funcionários podem se adaptar e aprender sobre tecnologia de maneira diferente de outros, com base em níveis variados de familiaridade com ferramentas digitais e a Internet. O medo do fracasso só desincentiva ainda mais a equipe de relatar problemas ou procurar ajuda. No entanto, a criação de responsabilidade positiva e recompensas para o treinamento bem-sucedido e a adoção de políticas podem ajudar a incentivar a melhoria em toda a organização. É possível encontrar suporte valioso adicional por meio de redes de treinamento de segurança digital locais ou internacionais e recursos de treinamento gratuitos, como o aplicativo Umbrella da Security First, o Projeto Totem da Free Press Unlimited e Greenhost, e o Portal educativo da Global Cyber Alliance.



Desenvolvimento de uma cultura de segurança

- **Agende conversas e treinamentos regulares sobre segurança e seu plano de segurança.**
- **Envolva todos; distribua a responsabilidade pela implementação do seu plano de segurança em toda a organização.**
- **Garanta que a liderança modele um bom comportamento de segurança e um compromisso com seu plano.**
- **Evite táticas de medo ou punição; recompense a melhoria obtida e crie um espaço confortável para a equipe relatar problemas e procurar ajuda.**
- **Atualize seu plano de segurança anualmente ou após grandes mudanças na organização.**



Uma base forte: Como proteger contas e dispositivos

Por que o foco em contas e dispositivos? Porque formam a base de tudo o que sua organização faz digitalmente.

É muito provável que você acesse informações confidenciais, se comunique interna e externamente, e salve dados privados. Se não estiverem em segurança, todos esses dados e muito mais podem ser colocados em risco. Por exemplo, se os hackers estiverem observando suas teclas ou ouvindo seu microfone, as conversas privadas com colegas serão capturadas, independentemente da segurança de seus aplicativos de mensagens. Ou, se um adversário obtiver acesso às contas de mídia social de sua organização, poderá facilmente prejudicar sua reputação e credibilidade, sabotando o sucesso de seu trabalho. Portanto, como organização, é essencial, garantir que todos estejam realizando algumas etapas simples, mas eficazes, para manter seus dispositivos e contas seguros. É importante observar que essas recomendações também incluem contas e dispositivos pessoais, pois geralmente são alvos fáceis para os adversários. Os hackers terão prazer em perseguir o alvo mais fácil e invadir uma conta pessoal ou um computador doméstico se seu time estiver usando esses recursos para se comunicar e acessar informações importantes.

Contas seguras e sociedade civil

A invasão amplamente divulgada da SolarWinds, revelada no final de 2020 e que comprometeu mais de 250 organizações, incluindo a maioria dos departamentos do governo dos Estados Unidos, fornecedores de tecnologia como Microsoft, Cisco e ONGs, aconteceu quando hackers adivinharam senhas fracas usadas em contas importantes de administrador. No geral, cerca de 80% de todas as violações relacionadas a hackers ocorrem devido a senhas fracas ou reutilizadas.

Com a crescente prevalência de violações de senha como essa e o acesso mais fácil para todos os tipos de adversários a ferramentas sofisticadas de hacking de senhas, as melhores práticas para criação de senhas e a autenticação de dois fatores são itens essenciais de segurança para organizações da sociedade civil. Um exemplo de contas da sociedade civil sob ataque foi relatado pelo Facebook em 2020. De acordo com seu relatório, grupos de hackers em Bangladesh atacaram contas de ativistas locais da sociedade civil, jornalistas e minorias religiosas. Infelizmente, os hackers conseguiram comprometer algumas dessas contas do Facebook, incluindo um administrador da página do Facebook de um grupo local. Com acesso à conta de administrador, os hackers removeram os administradores restantes, assumiram e desativaram a página, impedindo que o grupo compartilhasse informações importantes e se comunicasse com seu público. A investigação do Facebook descobriu que as contas provavelmente foram comprometidas por vários meios, incluindo abuso de seu processo de recuperação de conta. Se todas as contas estivessem usando autenticação de dois fatores, esses ataques teriam sido muito mais difíceis para os hackers executarem efetivamente.



Contas seguras: Senhas e autenticação de dois fatores

No mundo de hoje, é provável que sua organização e sua equipe tenham dezenas, senão centenas, de contas que, se violadas, podem expor informações confidenciais ou até mesmo prejudicar indivíduos em risco.

Pense nas diferentes contas que a equipe individual e a organização como um todo podem ter: e-mail, aplicativos de bate-papo, mídia social, banco online, armazenamento de dados em nuvem, além de lojas de roupas, restaurantes locais, jornais e muitos outros sites ou aplicativos que você acessa. Uma segurança reforçada no mundo de hoje exige uma abordagem diligente para proteger todas essas contas contra ataques, o que começa com a garantia de uma boa higiene de senha e o uso de autenticação de dois fatores em toda a organização.

O QUE FAZ QUE UMA SENHA SEJA BOA?

Há três aspectos que fazem uma senha ser boa e forte: comprimento, aleatoriedade e exclusividade.

COMPRIMENTO	Quanto mais longa for a senha, mais difícil será para um adversário adivinhá-la. Hoje em dia, a maioria dos hacks de senha são feitos por programas de computador, e esses programas nefastos não demoram muito para decifrar uma senha curta. Por isso, é essencial que suas senhas tenham no mínimo 16 caracteres, ou no mínimo cinco palavras, e de preferência mais longas.
ALEATORIEDADE	Mesmo que uma senha seja longa, não é considerada boa se for uma informação a seu respeito que o adversário possa adivinhar facilmente. Evite incluir informações como seu aniversário, cidade natal, atividades favoritas ou outros fatos que alguém possa descobrir sobre você em uma pesquisa rápida na Internet.
SINGULARIDADE	Talvez a "pior prática" de senha mais comum seja usar a mesma senha para vários sites. Repetir senhas é um grande problema porque indica que, quando apenas uma dessas contas é comprometida, qualquer outra conta que use essa mesma senha também fica vulnerável. Se você usar a mesma senha em vários sites, o impacto de um erro ou violação de dados é muito maior. Embora não se importe com sua senha da biblioteca local, se ela for hackeada e você usar a mesma senha em uma conta mais confidencial, informações importantes poderão ser roubadas.



Uma maneira fácil de atingir esses objetivos de comprimento, aleatoriedade e singularidade é escolher três ou quatro palavras comuns, mas aleatórias. Por exemplo, sua senha pode ser "flor lâmpada urso verde", que é fácil de lembrar, mas difícil de adivinhar. Você pode dar uma olhada neste site da Better Buys para ver uma estimativa da rapidez com que senhas ruins podem ser hackeadas.

USE UM GERENCIADOR DE SENHAS PARA AJUDAR

Agora você sabe que é importante que todos na organização usem uma senha longa, aleatória e diferente para cada uma de suas contas pessoais e organizacionais, mas como realmente fazer isso? Memorizar uma boa senha para dezenas (se não centenas) de contas é impossível, então todos precisam contar com um truque. A maneira errada de fazer isso é reutilizar senhas. Felizmente, podemos recorrer a gerenciadores de senhas digitais para tornar nossas vidas muito mais fáceis (e nossas práticas de senha muito mais seguras). Esses aplicativos, muitos dos quais podem ser acessados por computador ou dispositivo móvel, são capazes de criar, armazenar e gerenciar senhas para você e toda a sua organização. Adotar um gerenciador de senhas seguro significa que você só terá que se lembrar de uma senha muito forte e longa chamada senha primária (historicamente chamada de senha "mestre"), enquanto pode obter os benefícios de segurança de usar senhas boas e exclusivas em todas as suas contas. Você usará essa senha principal (e, idealmente, um segundo fator de autenticação (2FA) que será discutido na próxima seção) para abrir seu gerenciador de senhas e desbloquear o acesso a todas as suas outras senhas. Os gerenciadores de senhas também podem ser compartilhados em várias contas para facilitar o compartilhamento seguro de senhas em toda a organização.

Por que precisamos usar algo novo? Não podemos simplesmente anotá-las em um papel ou em uma planilha no computador?

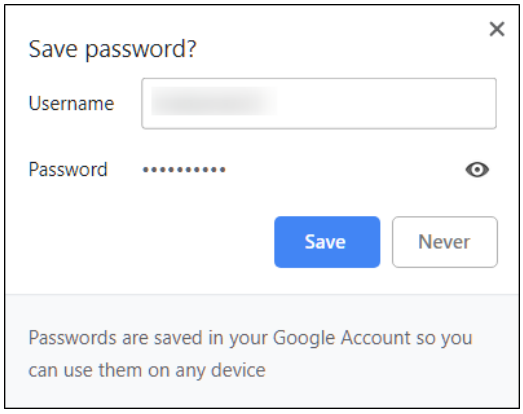
Infelizmente, existem muitas abordagens comuns para gerenciar senhas que não são seguras. Armazenar senhas em folhas de papel (a menos que você as mantenha trancadas em um cofre) pode expô-las a roubo físico, olhares indiscretos e conveniência para perda e danos. Salvar senhas em um documento em seu computador facilita significativamente o acesso para um hacker – ou para alguém que rouba seu computador e, além de ter acesso ao seu dispositivo, também terá a todas as suas contas. Usar um bom gerenciador de senhas é tão fácil quanto criar um documento desses, mas é uma alternativa muito mais segura.

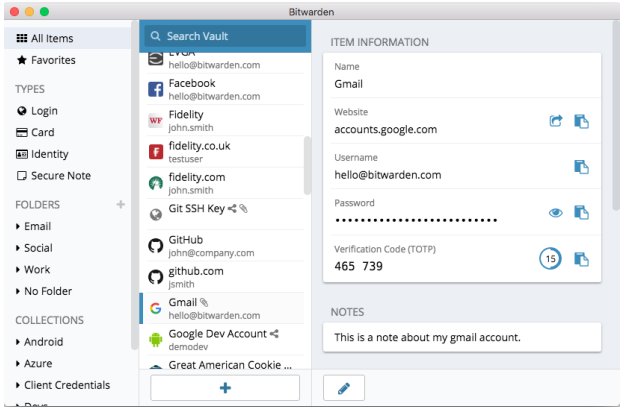
Por que devemos confiar em um gerenciador de senhas?

Os gerenciadores de senhas de qualidade fazem esforços extraordinários (e empregam excelentes times de segurança) para manter a segurança de seus sistemas. Bons aplicativos de gerenciamento de senhas (alguns são recomendados abaixo) também são configurados para que não tenham a capacidade de "desbloquear" suas contas. Isso significa que, na maioria dos casos, mesmo que tenham sido hackeados ou obrigados legalmente a entregar informações, não poderão perder ou revelar suas senhas. Também é importante lembrar que é infinitamente mais provável que um adversário adivinhe uma de suas senhas fracas ou repetidas, ou se depare com a senha em uma violação de dados públicos, do que um bom gerenciador de senhas enfrentar uma invasão em seus sistemas de segurança. É importante ser cético, e você definitivamente não deve confiar cegamente em todos os softwares e aplicativos, mas gerenciadores de senhas respeitáveis têm todos os incentivos certos para agir com cuidado.



Em vez de usar seu navegador (como o Chrome, mostrado à esquerda) para salvar suas senhas, use um gerenciador de senhas dedicado (como o Bitwarden, mostrado à direita). Os gerenciadores de senhas têm recursos que tornam a vida mais segura e conveniente para sua organização.





E quanto ao armazenamento de senhas no navegador?

Salvar senhas em seu navegador não é o mesmo que usar um gerenciador de senhas seguro. Resumindo, você não deve usar o Chrome, Firefox, Safari ou qualquer outro navegador como seu gerenciador de senhas. Embora seja definitivamente uma melhoria em relação a anotá-las em papel ou salvá-las em uma planilha, os recursos básicos de salvamento de senha do seu navegador de Internet deixam algo a desejar do ponto de vista da segurança. Essas deficiências também impedem que você se beneficie de grande parte da conveniência que um bom gerenciador de senhas proporciona. Ao perder essa conveniência, é mais provável que as pessoas de toda a sua organização continuem com suas práticas ruins de criação e compartilhamento de senhas.

Por exemplo, ao contrário dos gerenciadores de senhas dedicados, os recursos integrados "salvar esta senha" ou "lembrar esta senha" dos navegadores não fornecem compatibilidade móvel simples, funcionalidade entre navegadores e ferramentas de auditoria e geração de senhas fortes. Esses recursos são uma grande parte do que torna um gerenciador de senhas dedicado tão útil e benéfico para a segurança da sua organização. Os gerenciadores de senhas também abrangem recursos específicos da organização (como compartilhamento de senhas) que fornecem não apenas valor de segurança individual, mas valor à sua organização como um todo. Se você estiver salvando senhas com seu navegador (intencionalmente ou não), reserve um momento para removê-las.

Qual gerenciador de senhas devemos usar?

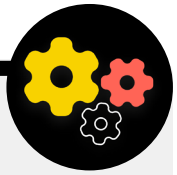
Existem muitas ferramentas de gerenciamento de senhas excelentes que podem ser configuradas em menos de 30 minutos. Se você estiver procurando uma opção online confiável para sua organização que possa ser acessada por pessoas de vários dispositivos a qualquer momento, 1Password (a partir de US$ 2,99 por usuário ao mês) ou o Bitwarden, que é gratuito e de código aberto, são bastante compatíveis e recomendados. Uma opção online, como o Bitwarden, pode ser uma ótima escolha

tanto pela segurança quanto pela praticidade. O Bitwarden, por exemplo, pode ajudá-lo a criar senhas fortes e exclusivas e acessar senhas de vários dispositivos por meio de extensões de navegador e um aplicativo móvel. Com a versão paga (US$ 10 por um ano inteiro), Bitwarden também fornece relatórios sobre senhas reutilizadas, fracas e possivelmente violadas para ajudá-lo a ficar por dentro das informações. Depois de configurar sua senha principal (conhecida como senha mestra), você também deve ativar a autenticação de dois fatores para manter o cofre do gerenciador de senhas o mais seguro possível.

Também é essencial **praticar uma boa segurança ao usar seu gerenciador de senhas.** Por exemplo, se você usar a extensão do navegador do seu gerenciador de senhas ou efetuar login no Bitwarden (ou qualquer outro gerenciador de senhas) em um dispositivo, lembre-se de se desconectar após o uso se estiver compartilhando esse dispositivo ou acreditar que pode estar em maior risco de roubo do dispositivo físico. Também é necessário se desconectar do seu gerenciador de senhas se deixar o computador ou dispositivo móvel sem vigilância. Se estiver compartilhando senhas em sua organização, também revogue o acesso às senhas (e altere as próprias senhas) quando as pessoas deixarem a organização. Você não quer que um ex-funcionário mantenha o acesso à senha do Facebook da sua organização, por exemplo.

E se alguém esquecer sua senha principal?

É fundamental lembrar sua senha principal. Bons sistemas de gerenciamento de senhas, como os recomendados acima, não lembram a senha principal para você ou liberam a redefinição diretamente por e-mail, como acontece com alguns sites. Esse é um ótimo recurso de segurança, mas também torna essencial memorizar sua senha principal ao configurar seu gerenciador de senhas pela primeira vez. Para facilitar, considere configurar um lembrete diário para recuperar sua senha principal ao criar uma conta de gerenciador de senhas pela primeira vez.



Como usar um gerenciador de senhas para sua organização

Você pode fortalecer as práticas de senha de toda a sua organização e garantir que todos os funcionários individuais tenham acesso (e usem) um gerenciador de senhas ao implementar um em toda a organização. Em vez de cada membro do time configurar seu próprio, considere investir em um plano de "time" ou "comercial". Por exemplo, o plano de "organização de times" do Bitwarden tem o custo mensal de US$ 3 por usuário. Com ele (ou outros planos de time de gerenciadores de senhas como o 1Password), você tem a capacidade de gerenciar todas as senhas compartilhadas em toda a organização. Os recursos de um gerenciador de senhas para toda a organização não apenas oferecem maior segurança, mas também conveniência para o pessoal.

É possível compartilhar credenciais com segurança no próprio gerenciador de senhas para diferentes contas de usuário. O Bitwarden, por exemplo, também fornece um recurso conveniente de compartilhamento de arquivos e texto criptografado de ponta a ponta em seu plano de time, chamado "Bitwarden Send". Ambos os recursos proporcionam à sua organização mais controle sobre quem pode ver e compartilhar quais senhas, além de fornecer uma opção mais segura para compartilhar credenciais para contas de time ou de grupo. Se você configurar um gerenciador de senhas para toda a organização, certifique-se de que alguém seja especificamente responsável por remover as contas do time e alterar as senhas compartilhadas quando alguém sair do time.

O QUE É A AUTENTICAÇÃO DE DOIS FATORES?

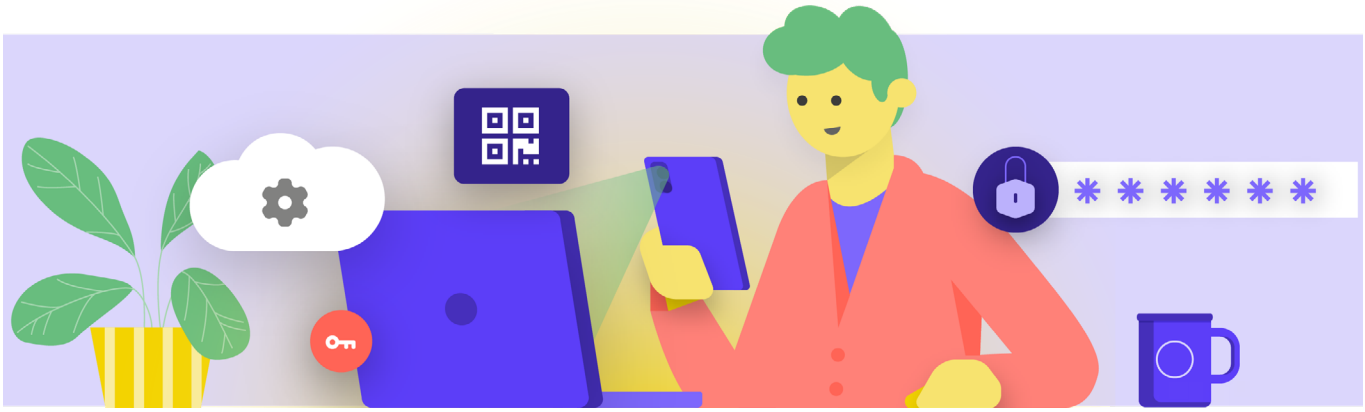
Por melhor que seja a higiene de suas senhas, é bastante comum hackers conseguirem burlá-las. Manter suas contas protegidas contra agentes de ameaças comuns no mundo de hoje requer outra camada de proteção. É diante dessa necessidade que a autenticação multifator ou de dois fatores entra em ação – conhecida como MFA ou 2FA. Há muitos guias e recursos excelentes que explicam a autenticação de dois fatores, incluindo o artigo Autenticação de dois fatores para iniciantes de Martin Shelton e o Guia de campo inicial de segurança cibernética durante eleições do Center for Democracy & Technology. Esta seção faz muitas referências a esses dois recursos para ajudar a explicar por que é tão importante implementar a autenticação de dois fatores (2FA) em toda a sua organização. Resumindo, a 2FA fortalece a segurança da conta ao exigir uma segunda informação – algo mais do que apenas uma senha – para obter o acesso. A segunda informação costuma ser algo que você possui, como um código de um aplicativo em seu telefone ou um token ou chave física. Esta segunda informação atua como uma segunda camada de defesa. Se um hacker rouba sua senha ou obtém acesso a ela por meio de uma divulgação de senhas feita por uma grande violação de dados, a 2FA eficaz pode impedir que acessem sua conta (e, portanto, que invadam suas informações privadas e confidenciais). Garantir que todos na organização implementem a 2FA em suas contas é extremamente importante.

COMO PODEMOS CONFIGURAR A AUTENTICAÇÃO DE DOIS FATORES?

Existem três métodos comuns para a 2FA: chaves de segurança, aplicativos de autenticação e códigos SMS únicos.

Chaves de segurança

As chaves de segurança são a melhor opção, em parte porque são quase totalmente à prova de phishing. Essas "chaves" são tokens de hardware (pense em mini drives USB) que podem ser anexados ao seu chaveiro (ou permanecer no seu computador) para facilitar o acesso e a segurança. Quando chegar a hora de usar a chave para desbloquear determinada conta, basta inseri-la no dispositivo e tocá-la fisicamente quando for solicitado durante o login. Há uma grande variedade de modelos que você pode adquirir online (de US$ 20 a US$ 50), incluindo as altamente conceituadas YubiKeys. O Wirecutter do New York Times apresenta um guia útil com algumas recomendações sobre quais chaves comprar. Lembre-se de que a mesma chave de segurança pode ser usada para quantas contas você desejar. Embora as chaves de segurança sejam caras para muitas organizações, iniciativas como o Programa de proteção avançada do Google ou o AccountGuard da Microsoft fornecem essas chaves gratuitamente para alguns grupos de risco qualificados. Entre em contato com as pessoas que lhe entregaram o manual para ver se conseguem conectá-lo a esses programas ou entre em contato com cyberhandbook@ndi.org.



Aplicativos de autenticação

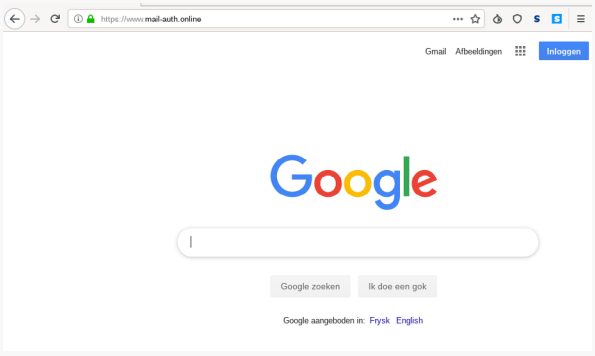
A **segunda melhor opção para a 2FA são os aplicativos de autenticação.** Esses serviços permitem que você receba um código de login temporário de dois fatores por meio de um aplicativo móvel ou notificação por push em seu smartphone. Algumas opções populares e confiáveis incluem Google Authenticator, Authy e Duo Mobile. Os aplicativos autenticadores também são ótimos porque funcionam quando você não tem acesso à sua rede celular e são gratuitos para uso individual. No entanto, os aplicativos autenticadores são mais suscetíveis a phishing do que as chaves de segurança, afinal, os usuários podem ser induzidos a inserir códigos de segurança de um aplicativo de autenticação em um site falso. Tome cuidado para inserir códigos de login apenas em sites legítimos. E não "aceite" notificações push de login, a menos que tenha certeza de que foi você quem fez a solicitação de login. Ao usar um aplicativo autenticador, também é essencial estar preparado com códigos de backup (discutidos abaixo) caso seu telefone seja perdido ou roubado.

Códigos por SMS

A forma menos segura, mas infelizmente ainda mais comum de 2FA, são os códigos enviados via SMS. Como o SMS pode ser interceptado e os números de telefone podem ser falsificados ou hackeados por meio de sua operadora de celular, o SMS é insuficiente como método para solicitar códigos 2FA. É melhor do que usar apenas uma senha, mas aplicativos autenticadores ou uma chave de segurança física são recomendados sempre que possível. Um adversário pode ter acesso a códigos 2FA por SMS, bastando apenas ligar para a companhia telefônica e trocar seu cartão SIM. Quando estiver pronto para ativar a 2FA em todas as várias contas da sua organização, use este site (https://2fa.directory/) para procurar rapidamente informações e instruções referentes a serviços específicos (como Gmail, Office 365, Facebook, Twitter etc.) e para ver quais serviços permitem quais tipos de 2FA.

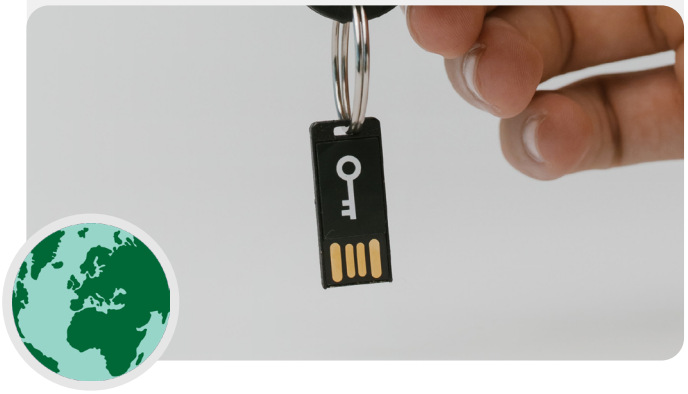
2FA e sociedade civil

De acordo com um recente relatório da Amnesty International, hackers que miravam em defensores de direitos humanos no Uzbequistão usaram ataques de phishing para induzir os usuários a compartilhar senhas *e* códigos de autenticação de dois fatores em suas contas de e-mail por meio de páginas de login falsas do Gmail. Esses ataques consistem em uma maneira cada vez mais comum de "contornar" a autenticação de dois fatores. É importante – mesmo com a 2FA em vigor – ter cuidado com relação a onde você digita seus códigos. Uma solução ainda melhor é eliminar esse risco ao adotar chaves de segurança físicas.



Chaves de segurança no mundo real

Ao fornecer chaves de segurança física para autenticação de dois fatores a todos os mais de 85.000 funcionários, o Google (uma organização de alto risco e altamente segmentada) **eliminou efetivamente qualquer ataque de phishing** bem-sucedido contra a organização. Este caso mostra como as chaves de segurança podem ser eficazes até mesmo para as organizações mais vulneráveis.



E SE ALGUÉM PERDER UM DISPOSITIVO COM 2FA?

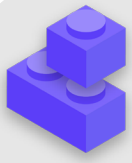
Se estiver usando uma chave de segurança, trate-a da mesma maneira que trataria uma chave de sua casa ou apartamento, se tiver uma. Resumindo, não a perca. Assim como as chaves de sua casa, é sempre viável ter uma chave reserva registrada em sua conta que permaneça trancada em um local seguro (como um cofre em casa ou contêiner protegido) para casos de perda ou roubo. Como alternativa, crie códigos de backup para contas que permitem essa função. Você deve manter esses códigos salvos em um local extremamente seguro, como seu gerenciador de senhas ou um cofre físico. Esses códigos de backup podem ser gerados nas configurações de 2FA da maioria dos sites (o mesmo local onde você habilite a 2FA primeiro) e podem atuar como uma chave de backup em caso de emergência. O acidente mais comum relacionado à 2FA ocorre quando as pessoas substituem ou perdem telefones que usam para aplicativos de autenticação. Se estiver usando o Google Authenticator, você não terá sorte se seu telefone for roubado, a menos que salve os códigos de backup gerados quando conectar uma conta ao Google Authenticator. Portanto, se estiver usando o Google Authenticator como um aplicativo 2FA, salve os códigos de backup de todas as contas que você conectar em um local seguro. Se estiver usando Authy ou Duo, ambos os aplicativos têm recursos de backup integrados com configurações de segurança fortes que podem ser ativadas. Se escolher um desses aplicativos, é possível configurar essas opções de backup em caso de invasão, perda ou roubo do dispositivo. Veja as instruções do Authy **aqui** e as do Duo **aqui**. Certifique-se de que todos em sua organização estejam cientes dessas etapas quando começarem a habilitar a 2FA em todas as suas contas.



Aplicação da 2FA em toda a sua organização

Se sua organização fornecer contas de e-mail para todos os funcionários por meio do Google Workspace (anteriormente conhecido como GSuite) ou Microsoft 365 usando seu próprio domínio (por exemplo, @ndi.org), você poderá executar a 2FA e configurações fortes de segurança em todas as contas. Essa execução não apenas ajuda a proteger essas contas, mas também atua como uma maneira de introduzir e normalizar a 2FA para sua equipe, que também se sentirá mais à vontade para utilizá-la nas contas pessoais. Como administrador do Google Workspace, você pode seguir **essas instruções** para aplicar a 2FA em seu domínio. É possível fazer algo semelhante no Microsoft 365 ao seguir **essas etapas** como administrador de domínio.

Considere também inscrever as contas da sua organização no **Programa de proteção avançada** (Google) ou **AccountGuard** (Microsoft) para aplicar controles de segurança adicionais e exigir chaves de segurança físicas para autenticação de dois fatores.



Contas seguras

- **Exija senhas fortes para todas as contas organizacionais e incentive o mesmo para as contas pessoais dos funcionários e voluntários.**
- **Implemente um gerenciador de senhas confiável para a organização (e incentive seu uso também na vida pessoal da equipe).**
  - Exija uma senha principal forte e 2FA para todas as contas do gerenciador de senhas.
  - Relembre todos de se desconectarem de um gerenciador de senhas em dispositivos compartilhados ou quando houver maior risco de roubo ou confisco de dispositivos.
- **Altere as senhas compartilhadas quando os funcionários deixarem a organização.**
- **Somente compartilhe senhas com segurança, como por meio do gerenciador de senhas da sua organização ou de aplicativos criptografados de ponta a ponta.**
- **Exija 2FA em todas as contas organizacionais e incentive a equipe a configurar a 2FA em todas as contas pessoais também.**
  - Se possível, forneça chaves de segurança físicas a todos os funcionários.
  - Se as chaves de segurança não estiverem em seu orçamento, incentive o uso de aplicativos autenticadores em vez de SMS ou chamadas telefônicas para 2FA.
- **Realize treinamentos com regularidade para garantir que a equipe esteja ciente das práticas recomendadas de senha e 2FA, incluindo o que torna uma senha forte e a importância de nunca reutilizar senhas, aceitar apenas solicitações legítimas de 2FA e gerar códigos 2FA de backup.**

Dispositivos seguros

Além das contas, é essencial manter todos os dispositivos – computadores, telefones, USBs, discos rígidos externos etc. – devidamente protegidos.

Essa proteção começa com o cuidado com o tipo de dispositivos que sua organização e sua equipe compram e utilizam. Qualquer fornecedor ou fabricante que você selecionar deve ter um histórico comprovado de adesão aos padrões globais em relação ao desenvolvimento seguro de dispositivos de hardware (como telefones e computadores). Todos os dispositivos que você adquirir devem ser fabricados por companhias confiáveis que não tenham sido incentivadas a entregar dados e informações a um adversário em potencial. É importante observar que o governo chinês exige que as companhias chinesas forneçam dados ao governo central. Portanto, apesar da presença onipresente e econômica de smartphones como Huawei ou ZTE, eles devem ser evitados. Embora o custo mais baixo de hardware possa ser bastante atrativo para uma organização, os possíveis riscos de segurança às organizações que defendem a democracia, os direitos humanos ou a responsabilidade devem fazer com que outras opções de dispositivos sejam priorizadas, pois esse acesso aos dados ajudou a facilitar o direcionamento da mira do governo chinês e de outros governos para certos indivíduos e comunidades. Seus adversários podem comprometer a segurança de seus dispositivos, e tudo o que você faz a partir deles, quando obtêm acesso físico ou acesso "remoto" ao seu dispositivo.

A segurança dos dispositivos e a sociedade civil

Alguns dos malwares mais avançados do mundo foram desenvolvidos e implantados globalmente para atingir organizações da sociedade civil e defensores dos direitos humanos. Na Índia, por exemplo, a Anistia Internacional relatou que pelo menos nove defensores de direitos humanos foram atacados em 2020 por spyware (um tipo de software malicioso) em seus dispositivos móveis e computadores. O spyware foi transmitido através de uma série de e-mails de phishing com links para arquivos infectados compartilhados pelo Firefox Send (um programa de compartilhamento de arquivos descontinuado). Os dispositivos dos alvos que abriram os arquivos foram infectados com software que gravava áudio, interceptava teclas e mensagens, e os colocava sob total vigilância dos invasores. Esses ataques, que são frequentemente direcionados a grupos da sociedade civil e sua equipe individual, infelizmente são uma maneira comum de invasores obterem acesso "remoto" a um dispositivo.



ACESSO AOS DISPOSITIVOS FÍSICOS POR PERDA OU ROUBO

Para evitar comprometimento físico, é essencial manter seus dispositivos fisicamente seguros. Resumindo, não facilite para um adversário roubar ou mesmo tirar temporariamente seu dispositivo de você. Mantenha os dispositivos trancados quando forem deixados em casa ou no escritório. Ou, se achar que é mais seguro, carregue-os consigo. Obviamente, isso significa que parte da segurança do dispositivo é a segurança física dos seus espaços de trabalho (seja em um ambiente de escritório ou em casa). Você precisará instalar fechaduras fortes, câmeras de segurança ou outros sistemas de monitoramento, principalmente se sua organização estiver em alto risco. Lembre os funcionários de que devem tratar os dispositivos da mesma forma que tratariam uma grande pilha de dinheiro, ou seja, não os deixando espalhados sem vigilância ou desprotegidos.

E se um dispositivo for roubado?

Para limitar o impacto se alguém conseguir roubar um dispositivo – ou mesmo se apenas obtiver acesso a ele por um curto período de tempo – certifique-se de **obrigar o uso de senhas ou códigos de acesso fortes nos computadores e telefones de todos.** As mesmas dicas de senha da seção Senhas deste manual se aplicam a uma senha forte para um computador ou laptop. Quando se trata de bloquear seu telefone, use códigos com pelo menos seis a oito dígitos e evite usar o "deslizamento padrão" para desbloquear a tela. Para obter dicas adicionais sobre bloqueios de tela, confira o Kit de desintoxicação de dados da Tactical Tech. O uso de senhas fortes no dispositivo dificulta consideravelmente o acesso rápido de um adversário às informações do seu dispositivo em caso de roubo ou confisco. Com uma senha forte em vigor, ativar o Face ID ou o desbloqueio por impressão digital pode ser interessante. Porém, certifique-se de desativá-los (enquanto mantém sua senha forte ativada) antes de qualquer atividade de alto risco, como protestos ou travessias de fronteira, caso você e sua equipe estejam preocupados com o confisco de dispositivos por parte das autoridades. Se algum dispositivo emitido pela organização tiver um recurso "Find my Device", como o Find My iPhone do iPhone e o Find My Device do Android, considere exigir que a equipe o ative. Incentive a equipe a usar esses recursos também em dispositivos pessoais. Com esses recursos ativados, o proprietário do dispositivo (ou um contato confiável) pode localizar o dispositivo ou limpar remotamente seu conteúdo caso seja roubado, perdido ou confiscado. Para iPhones, você também pode configurar o dispositivo para realizar automaticamente uma autolimpeza depois de várias tentativas de login com falha. Esses recursos de gerenciamento de dispositivos tornam-se extremamente importantes para uma organização quando um dispositivo com informações confidenciais é perdido ou cai em mãos erradas.

E a criptografia dos dispositivos?

É importante usar criptografia, embaralhando os dados para que fiquem ilegíveis e inutilizáveis em todos os dispositivos, principalmente em computadores e smartphones. Você deve configurar todos os dispositivos em sua organização com algo conhecido como **criptografia de disco completo**, se possível. A criptografia de disco completo significa que a totalidade de um dispositivo é criptografada para que um adversário, se o roubar fisicamente, não consiga extrair o conteúdo do seu interior sem saber a senha ou chave usada para criptografá-lo. Muitos smartphones e computadores modernos oferecem criptografia de disco completo. Dispositivos da Apple, como iPhones e iPads, de forma bastante conveniente ativam a criptografia de disco completo quando você define uma senha normal do dispositivo. Os computadores Apple que usam macOS fornecem um recurso chamado FileVault, que pode ser ativado para criptografia de disco completo. Os computadores Windows que executam licenças profissionais, corporativas ou educacionais oferecem um recurso chamado BitLocker, que pode ser ativado para criptografia de disco completo. Você pode ativar o BitLocker seguindo essas instruções da Microsoft, que talvez precisem ser habilitadas primeiro pelo administrador da sua organização. Se a equipe tiver apenas uma licença doméstica para seus computadores Windows, o BitLocker não estará disponível. No entanto, ainda podem ativar a criptografia de disco completo acessando "Atualização e segurança" > "Criptografia do dispositivo" nas configurações do sistema operacional Windows.

Os dispositivos Android, a partir da versão 9.0 e posterior, são fornecidos com a criptografia baseada em arquivo ativada por padrão. A criptografia baseada em arquivo do Android opera de maneira diferente da criptografia de disco completo, mas ainda oferece segurança forte. Se você estiver usando um telefone Android relativamente novo e tiver definido uma senha, a criptografia baseada em arquivo deve ser ativada. No entanto, é uma boa ideia verificar suas configurações apenas para ter certeza, principalmente se o seu telefone tiver mais de dois anos. Para verificar, vá para Configurações > Segurança no seu dispositivo Android. Dentro das configurações de segurança, você deve ver uma subseção para "criptografia" ou "criptografia e credenciais", que indicará se seu telefone está criptografado e, caso contrário, permitirá que você ative a criptografia.

Para computadores (seja Windows ou Mac), é particularmente importante armazenar todas as chaves de criptografia (chamadas de chaves de recuperação) em um local seguro. Essas "chaves de recuperação" são, na maioria dos casos, senhas ou frases secretas essencialmente longas. Caso esqueça a senha normal do dispositivo ou algo inesperado aconteça (como falha do dispositivo), as chaves de recuperação são a única maneira de recuperar seus dados criptografados e, se necessário, movê-los para um novo dispositivo. Portanto, ao ativar a criptografia de disco completo, salve essas chaves ou senhas em um local seguro, como uma conta de nuvem segura ou o gerenciador de senhas da sua organização.

ACESSO REMOTO AO DISPOSITIVO – TAMBÉM CONHECIDO COMO HACKING

Além de manter os dispositivos fisicamente seguros, é importante mantê-los livres de malware. O Security-in-a-Box da Tactical Tech fornece uma descrição útil do que é malware e por que é importante evitá-lo, o que é adaptado ligeiramente no restante desta seção.

Entenda e evite o malware

Há muitas maneiras de classificar malware (que é um termo cujo significado é software malicioso). Vírus, spyware, worms, trojans, rootkits, ransomware e cryptojackers são todos tipos de malware. Alguns tipos de malware se espalham pela Internet por e-mail, mensagens de texto, páginas da web maliciosas e outros meios. Alguns se espalham por dispositivos como cartões de memória USB que são usados para trocar e roubar dados. E, enquanto alguns malwares exigem que um alvo desavisado cometa um erro, outros podem infectar silenciosamente sistemas vulneráveis sem que cometa qualquer erro.

Além do malware geral, que é amplamente divulgado e destinado ao público em geral, o malware direcionado costuma ser usado para interferir ou espionar determinado indivíduo, organização ou rede. Criminosos comuns usam essas técnicas, assim como os serviços militares e de inteligência, terroristas, assediadores virtuais, cônjuges abusivos e agentes políticos suspeitos.

Seja qual for o nome, independentemente da forma como é distribuído, o malware é capaz de arruinar computadores, roubar e destruir dados, falir organizações, invadir a privacidade e colocar os usuários em risco. Em síntese, o malware é realmente perigoso. No entanto, há algumas etapas simples que podem ser adotadas por sua organização para se proteger contra essa ameaça comum.

Uma ferramenta antimalware nos protegerá?

Infelizmente, as ferramentas antimalware não são uma solução completa. No entanto, é uma boa ideia usar algumas ferramentas básicas e gratuitas como ponto de partida. Com novos riscos no mundo real que surgem com tanta frequência, o malware muda tão rapidamente que confiar em qualquer ferramenta desse tipo não pode ser sua única defesa.

Se você estiver usando o Windows, dê uma olhada no Windows Defender integrado. Computadores Mac e Linux não vêm com software antimalware integrado, nem dispositivos Android e iOS. Você pode instalar uma ferramenta confiável e gratuita como o Bitdefender ou Malwarebytes para esses dispositivos (e computadores Windows também). **Contudo, não confie nesse recurso como sua única linha de defesa,** pois eles certamente deixarão passar alguns dos novos ataques mais direcionados e perigosos.

Além disso, seja cauteloso ao baixar ferramentas antimalware ou antivírus respeitáveis apenas de fontes legítimas (como os sites vinculados acima). Infelizmente, existem muitas versões falsas ou comprometidas de ferramentas antimalware que mais prejudicam do que beneficiam.

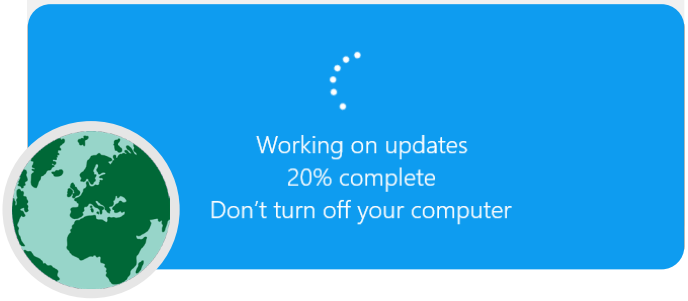
Na medida em que você usa o Bitdefender ou outra ferramenta antimalware em sua organização, certifique-se de não executar duas delas ao mesmo tempo. Muitas identificam o comportamento do outro programa antimalware como suspeito e o impedem de ser executado, o que compromete o funcionamento de ambas. O Bitdefender ou outros programas antimalware respeitáveis podem ser atualizados gratuitamente, e o Windows Defender integrado recebe atualizações junto com seu computador. Certifique-se de que seu software antimalware se atualize regularmente (algumas versões de teste de software comercial que acompanham um computador serão desativadas após o término do período de avaliação, tornando-o mais perigoso do que útil). Novos malwares são criados e distribuídos todos os dias, e seu computador rapidamente se tornará ainda mais vulnerável se você não acompanhar as novas definições de malware e técnicas antimalware. Se possível, configure seu software para instalar atualizações automaticamente. Se sua ferramenta antimalware tiver um recurso opcional "sempre ativado", é recomendado habilitá-lo e considerar verificar ocasionalmente todos os arquivos em seu computador.

Mantenha os dispositivos atualizados

As atualizações são essenciais. Use a versão mais recente de qualquer sistema operacional executado em um dispositivo (Windows, Mac, Android, iOS etc.) e mantenha esse sistema operacional atualizado. Mantenha outros softwares, navegadores e plug-ins de navegador atualizados também. Instale as atualizações assim que estiverem disponíveis, de preferência ativando as atualizações automáticas. Quanto mais atualizado for o sistema operacional de um dispositivo, menos vulnerabilidades você terá. Pense nas atualizações como um band-aid colocado em um corte aberto: elas selam vulnerabilidades e reduzem significativamente as chances de você ser infectado. Além disso, desinstale o software que você não usa mais. Softwares desatualizados costumam apresentar problemas de segurança e você pode ter instalado uma ferramenta que não está mais sendo atualizada pelo desenvolvedor, deixando-a mais vulnerável a hackers.

Malware no mundo real: As atualizações são essenciais

Em 2017, os ataques do ransomware WannaCry infectaram milhões de dispositivos em todo o mundo e causaram o fechamento de hospitais, entidades governamentais, grandes e pequenas organizações e companhias em dezenas de países. Por que o ataque foi tão eficaz? Por causa de sistemas operacionais Windows desatualizados, "sem patches", muitos dos quais foram inicialmente pirateados. Grande parte dos danos – humanos e financeiros – poderia ter sido evitada com melhores práticas de atualização automatizada e o uso de sistemas operacionais legítimos.



Tenha cuidado com os USBs

Tenha cuidado ao abrir arquivos enviados a você como anexos, por meio de links de download ou por qualquer outro meio. Além disso, **pense duas vezes antes de inserir mídias removíveis, como pen drives**, cartões de memória flash, DVDs e CDs em seu computador, visto que podem ser um vetor de malware. USBs que foram compartilhados por certo tempo são muito propensos a conter vírus. Para opções alternativas de compartilhamento de arquivos com segurança em toda a sua organização, dê uma olhada na seção Compartilhamento de arquivos do manual.

Seja cauteloso também com os outros dispositivos aos quais você se conecta por meio de Bluetooth. Não há problema em sincronizar seu telefone ou computador com um alto-falante Bluetooth conhecido e confiável para reproduzir sua música favorita, mas tenha cuidado ao vincular ou aceitar solicitações de qualquer dispositivo desconhecido. Permita apenas conexões com dispositivos confiáveis e lembre-se de desligar o Bluetooth quando não estiver em uso.

Seja inteligente ao navegar

Nunca aceite e execute aplicativos provenientes de sites que você não conhece e nos quais não confia. Em vez de aceitar uma "atualização" oferecida em uma janela pop-up do navegador, por exemplo, verifique se há atualizações no site oficial do aplicativo relevante. Conforme discutido na seção Phishing do manual, é essencial ficar alerta ao navegar em sites. Verifique o destino de um link (ao passar o mouse sobre ele) antes de clicar, confira o endereço do site ao seguir o link e avalie se parece adequado antes de inserir informações confidenciais, como sua senha. Não clique em mensagens de erro ou avisos e observe as janelas do navegador que aparecem automaticamente. Leia-as com atenção em vez de apenas clicar em "Sim" ou "OK".

E os smartphones?

Assim como nos computadores, mantenha o sistema operacional e os aplicativos móveis atualizados, e ative as atualizações automáticas. Instale programas somente a partir de fontes oficiais ou confiáveis, como a Play Store do Google e a App Store da Apple (ou F-droid, uma loja de aplicativos gratuita e de código aberto para Android). Os aplicativos podem conter malware e continuar apresentando um funcionamento normal, e você nem sempre saberá se algum deles é malicioso. Certifique-se também de baixar a versão legítima de um aplicativo. Especialmente em dispositivo Android, existem versões "falsas" de aplicativos populares. Portanto, certifique-se de que o aplicativo tenha sido criado pela companhia ou desenvolvedor adequado, tenha boas críticas e o número esperado de downloads (por exemplo, uma versão falsa do WhatsApp pode ter apenas alguns milhares de downloads, enquanto a versão real tem mais de 5 bilhões). Preste atenção às permissões que seus aplicativos solicitam. Se parecerem excessivas (como uma calculadora exigindo acesso à sua câmera ou Angry Birds solicitando acesso à sua localização, por exemplo), negue a solicitação ou desinstale o aplicativo. Desinstalar aplicativos que você não usa mais também pode ajudar a proteger seu smartphone ou tablet. Às vezes, desenvolvedores vendem a propriedade de seus aplicativos para outras pessoas. Esses novos proprietários podem tentar lucrar adicionando código malicioso.

Malware no mundo real: Aplicativos móveis maliciosos

Há anos, hackers de vários países usam aplicativos falsos na Google Play Store para disseminar malware. Um caso específico direcionado a usuários no Vietnã veio à tona em abril de 2020. Essa campanha de espionagem usava aplicativos falsos, que supostamente ajudavam os usuários a encontrar pubs próximos ou procurar informações sobre igrejas locais. Uma vez instalados inadvertidamente por usuários do Android, os aplicativos maliciosos coletavam registros de chamadas, dados de localização e informações sobre contatos e mensagens de texto. Este é apenas um dos muitos motivos para ter cuidado com os aplicativos baixados em seus dispositivos.



Economize dinheiro e aumente a segurança do dispositivo com o Tails para sua organização

Uma opção muito segura que requer um pouco de habilidade técnica para configurar é o sistema operacional Tails. Este sistema operacional portátil é de uso gratuito e você pode inicializá-lo diretamente de um USB, ignorando a necessidade de depender de sistemas operacionais Windows ou Mac licenciados. O Tails também é uma boa opção para aqueles com risco extremamente alto, pois incorpora uma ampla variedade de recursos de aprimoramento de privacidade. Esses recursos incluem a integração do Tor (discutido abaixo) para proteger seu tráfego na web e a limpeza completa da memória toda vez que você desliga o sistema operacional. Basicamente, esses recursos permitem que você comece do zero toda vez que reiniciar o computador. O Tails também possui um modo de persistência, que permite salvar arquivos e configurações importantes em várias sessões, se desejado.

Outra opção para um sistema operacional gratuito e seguro é o Qubes OS. Embora não seja a opção mais simples para usuários não técnicos, o Qubes foi projetado para limitar a ameaça de malware e é outra opção a ser considerada para usuários mais avançados e de alto risco em sua organização, principalmente se os custos de licenciamento forem um desafio.

E se não pudermos pagar por software legal?

Pode ser oneroso comprar versões licenciadas de software popular como o Microsoft Office (Word, Powerpoint, Excel) para toda a sua organização, mas um orçamento limitado não é desculpa para baixar versões piratas de software ou deixar de mantê-las atualizadas. Essa não é uma questão de moralidade, é uma questão de segurança. O software pirata costuma estar infectado por malware e, muitas vezes, não pode ser corrigido diante de falhas de segurança. Se não puder comprar o software que sua organização precisa, há uma grande variedade de excelentes softwares gratuitos e de código aberto, como LibreOffice (um substituto para aplicativos padrão do Microsoft Office) ou GIMP (um substituto para Photoshop) que podem atender às suas necessidades. Considere também se registrar por meio da Tech Soup, uma organização que oferece grandes descontos em softwares populares para organizações sem fins lucrativos. Mesmo que você possa pagar por software e aplicativos legítimos, seu dispositivo ainda estará em risco se o sistema operacional subjacente não for legítimo. Portanto, se sua organização não puder cobrir o pagamento de licenças do Windows, considere alternativas mais econômicas, como Chromebooks, que são uma opção excelente e que fornece fácil proteção se sua organização trabalha principalmente na nuvem. Se você estiver usando o Google Docs ou o Microsoft 365, não precisará de muitos aplicativos de desktop – os editores gratuitos de documentos e planilhas no navegador são mais do que suficientes para praticamente qualquer uso. Outra opção, se você tiver funcionários com habilidades técnicas, é instalar um sistema operacional gratuito baseado em Linux (uma alternativa de código aberto aos sistemas operacionais Windows e Mac) em cada computador. Uma opção Linux popular e bastante intuitiva é o Ubuntu. Independentemente do sistema operacional escolhido, certifique-se de que alguém na organização seja responsável por realizar verificações regulares com a equipe para garantir que as atualizações mais recentes tenham sido instaladas.

Ao escolher uma nova ferramenta ou sistema, considere como sua organização pode apoiá-lo técnica e financeiramente a longo prazo. Faça a si mesmo perguntas como: Você pode pagar e reter a equipe necessária para manter a ferramenta ou sistema com segurança? Você pode pagar por assinaturas recorrentes? Você tem acesso a descontos de grupos como o Tech Soup mencionado acima? Responder a essas perguntas pode ajudar a garantir que suas estratégias de software e tecnologia sejam mais bem-sucedidas ao longo do tempo.



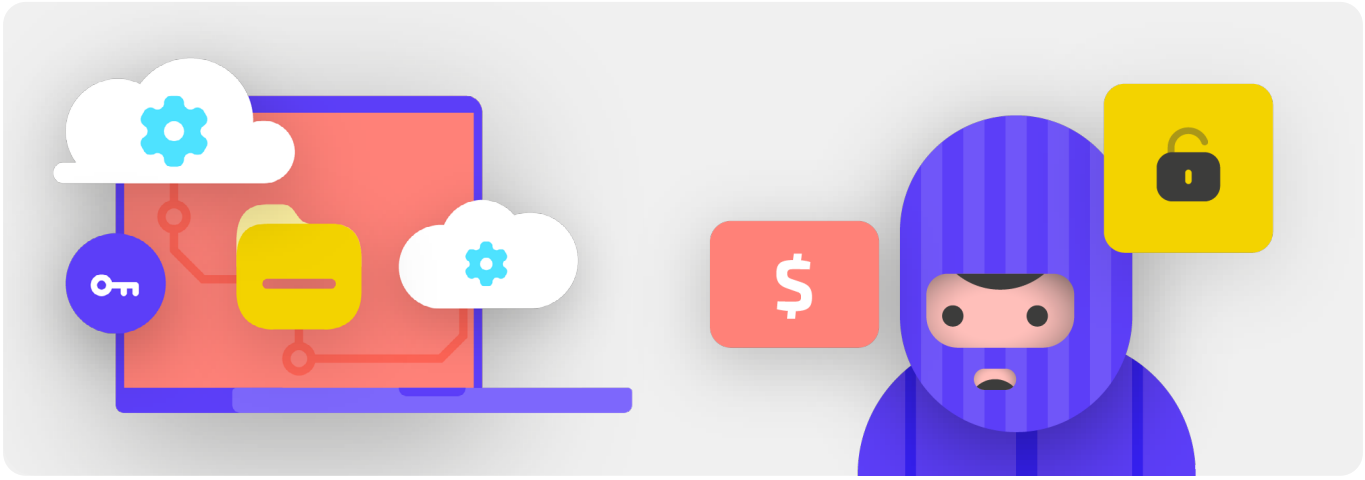
Como manter a segurança dos dispositivos

- **Capacite a equipe quanto aos riscos de malware e as melhores práticas para evitá-lo.**
  - Forneça políticas sobre como conectar dispositivos externos, clicar em links, baixar arquivos, aplicativos e verificar permissões de software e aplicativos.
- **Decrete que dispositivos, software e aplicativos devem ser mantidos totalmente atualizados.**
  - Ative as atualizações automáticas sempre que possível.
- **Certifique-se de que todos os dispositivos estejam usando software licenciado.**
  - Se o custo for proibitivo, migre para uma alternativa sem custo.
- **Exija proteção por senha de todos os dispositivos organizacionais, incluindo dispositivos móveis pessoais usados para comunicações relacionadas ao trabalho.**
- **Habilite a criptografia de disco completo em dispositivos.**
- **Relembre frequentemente a equipe de manter seus dispositivos fisicamente seguros – e gerencie a segurança do seu escritório com travas e formas adequadas de proteger os computadores.**
- **Não compartilhe arquivos usando USBs nem conecte USBs em seus computadores.**
  - Use opções alternativas de compartilhamento seguro de arquivos.

Phishing: Uma ameaça comum a dispositivos e contas

O phishing é o ataque mais comum e eficaz contra organizações em todo o mundo. A técnica é usada pelos militares mais sofisticados dos estados-nação, bem como por fraudadores triviais.

Para simplificar, um ataque de phishing acontece quando um adversário tenta induzi-lo a compartilhar informações que podem ser usadas contra você ou sua organização. O phishing pode acontecer por meio de e-mails, mensagens de texto/SMS (geralmente chamados de phishing por SMS ou "smishing"), aplicativos de mensagens como WhatsApp, mensagens ou postagens de mídia social ou chamadas telefônicas (geralmente chamadas de phishing de voz ou "vishing"). As mensagens de phishing podem tentar fazer com que você digite informações confidenciais (como senhas) em um site falso para obter acesso a uma conta, solicitar que você compartilhe informações privadas (como um número de cartão de crédito) por voz ou texto ou convencê-lo a baixar malware (software malicioso) que pode infectar seu dispositivo. Para um exemplo não técnico, milhões de pessoas recebem chamadas telefônicas falsas e automatizadas diariamente, com a informação de que sua conta bancária foi comprometida ou que sua identidade foi roubada – todas projetadas para enganar pessoas desprevenidas a compartilhar informações confidenciais.



COMO PODEMOS IDENTIFICAR O PHISHING?

O phishing pode parecer sinistro e impossível de detectar, mas existem algumas etapas simples que todos em sua organização podem seguir para se proteger contra a maioria dos ataques. As dicas de defesa contra phishing a seguir são modificadas e estendidas a partir do guia de phishing detalhado desenvolvido pela Freedom of the Press Foundation e devem ser compartilhadas com sua organização (e outros contatos), além de integradas ao seu plano de segurança:

Às vezes, o campo "de" pode estar mentindo para você

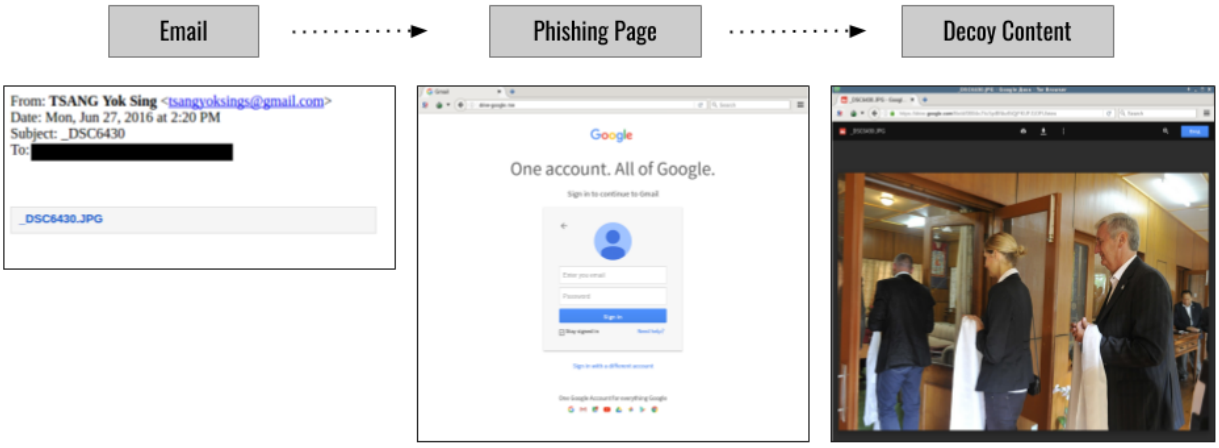
Esteja ciente de que o campo "de" em seus e-mails pode ter sido falsificado ou forjado para enganá-lo. É comum que os phishers configurem um endereço de e-mail que se parece muito com um endereço de e-mail legítimo com o qual você está familiarizado, digitado com alguns erros para enganá-lo. Por exemplo, você pode receber um e-mail de alguém com o endereço "john@gooogle.com"" em vez de "john@google.com". Observe os Os extras em "google". Você também pode conhecer alguém com um endereço de e-mail "john@gmail.com", mas receber um e-mail de phishing de um falsificador que configurou "johm@gmail.com" – sendo que a única diferença é uma sutil mudança de letras no final. Sempre verifique se você sabe o endereço de envio de um e-mail antes de continuar. Um conceito semelhante se aplica ao phishing por meio de mensagens de texto, chamadas ou aplicativos de mensagens. Se você receber uma mensagem de um número desconhecido, pense duas vezes antes de responder ou interagir com a mensagem.



O phishing e a sociedade civil

Ataques de phishing sofisticados e personalizados visam grupos da sociedade civil em todo o mundo diariamente.

Um exemplo de tal ataque é destacado no relatório do The Citizen Lab 2018, Espionagem com pouco orçamento: Dentro de uma operação de phishing com alvos na Comunidade Tibetana. Este ataque de phishing bastante econômico e simples, mas incrivelmente eficaz, foi direcionado a defensores dos direitos humanos tibetanos e outros ativistas. O ataque começou com um e-mail de phishing (mostrado à esquerda) de um endereço padrão do Gmail que continha apenas um link de arquivo de imagem. Quando clicado, o link direcionava o alvo a uma página falsa de login de e-mail do Google (mostrada no meio) que foi usada para roubar credenciais da conta. Se as vítimas fornecessem credenciais para a página falsa, suas contas estariam facilmente comprometidas. Depois de fornecer seu nome de usuário e senha ao site falso, as vítimas seriam redirecionadas para uma imagem (mostrada à direita) que exibe os delegados em uma reunião tibetana. A imagem foi incluída como um chamariz para fazer os alvos de phishing acreditarem que realmente acessaram sua conta real do Google e reduzir quaisquer possíveis suspeitas sobre a verdadeira natureza maliciosa do e-mail.



Cuidado com os anexos

Os anexos podem conter malware e vírus, e geralmente acompanham e-mails de phishing. **A melhor maneira de evitar malware de anexos é nunca os baixar.** Como regra, não abra nenhum anexo imediatamente, especialmente se vierem de pessoas que você não conhece. Se possível, solicite que a pessoa que lhe enviou o documento copie e cole o texto em um e-mail ou compartilhe o documento por meio de um serviço como o Google Drive ou o Microsoft OneDrive, que realizam verificação de vírus integrada na maioria dos documentos carregados em suas plataformas. Crie uma cultura organizacional onde anexos são desencorajados. Se você realmente precisar abrir um anexo, abra-o somente em um ambiente seguro (consulte a seção Avançado abaixo) onde o malware em potencial não pode ser implantado no seu dispositivo.

Se você usa o Gmail e recebe um anexo em determinado e-mail, ao invés de baixar e abri-lo em seu computador, basta clicar no arquivo anexado e lê-lo em "pré-visualizar" no seu navegador. Esta etapa permite que você visualize o texto e o conteúdo de um arquivo sem baixá-lo e sem permitir o carregamento de um possível malware em seu computador. É uma alternativa que funciona bem para documentos do Word, PDFs e até mesmo apresentações de slides. Se você precisar editar o documento, considere abrir o arquivo em um programa de nuvem, como o Google Drive, e convertê-lo em um Google Doc ou Google Slides.

Se você usa o Outlook, também pode visualizar anexos sem baixá-los a partir do cliente web do Outlook. Se precisar editar o anexo, considere abri-lo no OneDrive, se o recurso estiver disponível para você. Se você usa o Yahoo Mail, o mesmo conceito se aplica. Não baixe anexos, prefira visualizá-los no navegador de Internet.

Não importa quais ferramentas você tem à sua disposição, a melhor abordagem é simplesmente nunca baixar anexos desconhecidos ou pouco confiáveis e, independentemente da importância de um anexo, nunca abrir algo com um tipo de arquivo você não reconhece ou não tem intenção de usar.



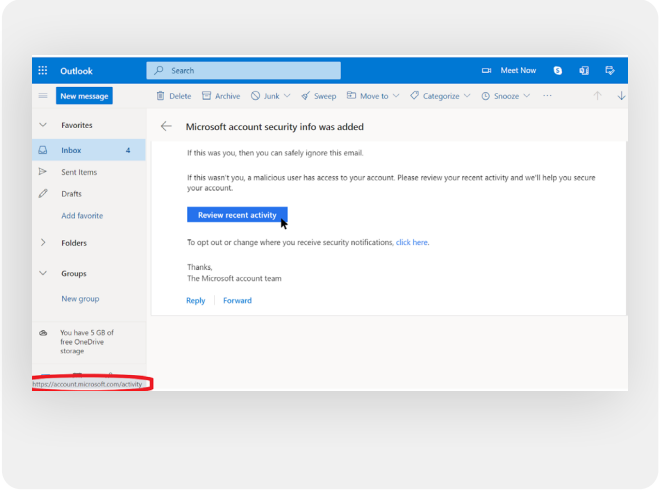
Defesa contra phishing para sua organização

Se sua organização usa o Microsoft 365 corporativo para e-mail e outros aplicativos, seu administrador de domínio deve configurar a política de anexos seguros para se proteger contra anexos perigosos. Se estiver usando o Google Workspace empresarial (anteriormente conhecido como GSuite), há uma opção igualmente eficaz que seu administrador deve configurar chamada Google Security Sandbox. Usuários individuais mais avançados podem considerar a configuração de programas sofisticados de sandbox, como Dangerzone, ou, para aqueles com a versão Pro ou Enterprise do Windows 10, há o Windows Sandbox. Outra opção avançada que pode ser implementada em toda a sua organização é um serviço de filtragem de sistema de nomes de domínio (DNS) seguro. As organizações podem usar essa tecnologia para impedir que a equipe acesse ou interaja acidentalmente com conteúdo malicioso, fornecendo uma camada adicional de proteção contra phishing. Novos serviços, como o Gateway da Couldflare, fornecem esses recursos para organizações sem exigir grandes somas de dinheiro (o Gateway, por exemplo, é gratuito para até 50 usuários). Ferramentas gratuitas adicionais, incluindo Quad9 do kit de ferramentas da Global Cyber Alliance, ajudam a impedir que você acesse sites conhecidos que contenham vírus ou outros malwares e possam ser implementados em menos de cinco minutos.

Clique com cautela

Desconfie de links em e-mails ou outras mensagens de texto. Os links podem estar disfarçados para baixar arquivos maliciosos ou direcioná-lo a sites falsos que podem solicitar o fornecimento de senhas ou outras informações confidenciais. Quando estiver em um computador, há um truque simples para garantir que um link em um e-mail ou mensagem realmente o direcione para onde deveria: Use o mouse para passar o cursor sobre qualquer link antes de clicar e, em seguida, olhe na parte inferior da janela do navegador para conferir o URL real (veja a imagem abaixo).

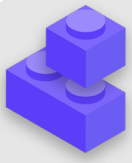
É mais difícil verificar links em um e-mail no dispositivo móvel sem clicar neles acidentalmente, portanto, tenha cuidado. Na maioria dos smartphones, você pode verificar o destino de um link ao pressionar por bastante tempo (mantendo pressionado) um link até que o URL completo apareça.
Em phishing via SMS e aplicativos de mensagens, links encurtados são uma prática muito comum usada para disfarçar o destino de um URL. Se você vir um link curto (por exemplo, bit.ly ou tinyurl.com) em vez do URL completo, não clique nele. Se o link for importante, copie-o em um expansor de URL, como https://www.expandurl.net/, para ver o destino real do URL encurtado. Além disso, não clique em links para sites que você não conhece. Em caso de dúvida, faça uma busca pelo site, com o nome do site entre aspas (ex: "www.badwebsite.com") para ver se é um site legítimo. Você também pode executar links potencialmente suspeitos por meio do verificador de URL VirusTotal. Esta não é uma opção 100% precisa, mas é uma boa precaução a ser tomada.



Por fim, se você clicar em qualquer link de uma mensagem e for solicitado a fazer login em algo, não o faça a menos que tenha 100% de certeza de que o e-mail é legítimo e o direciona para o site correto. Muitos ataques de phishing fornecem links que o direcionam a páginas de login falsas do Gmail, Facebook ou outros sites populares. Não caia nesse golpe. Sempre há a opção de abrir um novo navegador e acessar diretamente sites como Gmail.com, Facebook.com etc., se quiser ou precisar fazer login. Assim, você também será direcionado ao conteúdo com segurança – se ele for legítimo, para começar.

O que devemos fazer quando recebemos uma mensagem de phishing?

Se alguém em sua organização receber um anexo, link, imagem ou mensagem não solicitada ou chamada suspeita, é importante que informe imediatamente o responsável pela segurança de TI da sua organização. Se não houver um indivíduo nessa função, a identificação deverá ser feita como parte do desenvolvimento de seu plano de segurança. A equipe também pode denunciar o e-mail como spam ou phishing diretamente no Gmail ou Outlook. É crucial ter um plano que indique o que funcionários ou voluntários devem fazer se ou quando receberem uma possível mensagem de phishing. Além disso, recomendamos seguir essas práticas recomendadas de phishing: não clicar em links suspeitos, evitar anexos e verificar o endereço em "de", além de compartilhá-las com outras pessoas com quem você trabalha, de preferência por meio de um canal de comunicação amplamente utilizado. Agindo dessa forma, você está se preocupando com as pessoas com quem se comunica, além de incentivar uma cultura em suas redes de que está alerta e ciente dos perigos do phishing. Sua segurança depende das organizações nas quais você confia e vice-versa. As melhores práticas protegem a todos.
Além de compartilhar as dicas acima com todos os funcionários e voluntários, você também pode praticar a identificação de phishing com o Teste de phishing do Google. Também recomendamos enfaticamente a criação de treinamento regular de phishing com a equipe para testar a conscientização e manter as pessoas vigilantes. Esse treinamento pode ser formalizado como parte de reuniões organizacionais regulares ou conduzido de forma mais informal. O importante é que todos na organização se sintam à vontade para fazer perguntas sobre phishing, denunciar phishing (mesmo que sintam que podem ter cometido um erro, como clicar em um link), e que todos tenham o poder de ajudar a defender sua organização contra essa ameaça de alto impacto e alta probabilidade.



Phishing

- **Treine regularmente a equipe sobre o que é phishing, como identificá-lo e se defender dele, incluindo phishing em mensagens de texto, aplicativos de mensagens e telefonemas, não apenas em e-mail.**
- **Relembre frequentemente a equipe das melhores práticas, como:**
  - Não baixar anexos desconhecidos ou potencialmente suspeitos.
  - Verificar o URL de um link antes de clicar. Não clicar em links desconhecidos ou potencialmente suspeitos.
  - Não fornecer informações confidenciais ou privadas por e-mail, texto ou telefonema para endereços ou pessoas desconhecidas ou não confirmadas.
- **Incentive a denúncia de phishing.**
  - Estabeleça um mecanismo de denúncia e uma pessoa responsável para questões de phishing em sua organização.
  - Recompense o ato de denunciar e não penalize por falhas.



Comunicação e armazenamento de dados com segurança

Comunicações e compartilhamento de dados

Para tomar as melhores decisões para sua organização sobre como se comunicar, é fundamental entender os diferentes tipos de proteção que nossas comunicações podem ter e por que essa proteção é relevante.

Um dos elementos mais importantes da segurança das comunicações diz respeito a mantê-las privadas, o que atualmente é uma questão amplamente tratada pela criptografia. Sem criptografia adequada, as comunicações internas podem ser vistas por qualquer número de adversários. Comunicações sem proteção podem expor informações e mensagens confidenciais ou embaraçosas, revelar senhas ou outros dados privados e, possivelmente, colocar sua equipe e organização em risco, dependendo da natureza de suas comunicações e do conteúdo que você compartilha.

Comunicações seguras e sociedade civil

Milhares de ativistas e organizações que abordam a democracia e os direitos humanos contam com canais de comunicação seguros diariamente para manter a confidencialidade das conversas em ambientes políticos desafiadores. Sem essas práticas de segurança, mensagens confidenciais podem ser interceptadas e usadas pelas autoridades para atingir ativistas e dispersar protestos. Um exemplo notório e bem documentado disso ocorreu após as eleições de 2010 na Bielorrússia. Conforme detalhado neste relatório da Amnesty International, gravações telefônicas e outras comunicações não criptografadas foram interceptadas pelo governo e usadas em tribunal contra proeminentes políticos e ativistas da oposição, muitos dos quais passaram anos na prisão. Em 2020, em outra onda de protestos pós-eleitorais na Bielorrússia, milhares de manifestantes passaram a acessar aplicativos de mensagens seguros e de fácil uso que não estavam tão prontamente disponíveis para proteger suas comunicações confidenciais dez anos antes.



O QUE É CRIPTOGRAFIA E POR QUE ELA É IMPORTANTE?

A criptografia é um processo matemático usado para embaralhar uma mensagem ou um arquivo, para que apenas uma pessoa ou entidade que possua a chave possa "descriptografar" e ler o conteúdo. O Guia de autodefesa contra vigilância da Electronic Frontier Foundation fornece uma explicação prática (com gráficos) do que significa criptografia:

Mensagens não criptografadas

Sem qualquer criptografia, todos os envolvidos na retransmissão da mensagem, e qualquer um que possa dar uma espiada enquanto ela é transmitida, pode acessar o conteúdo. Esse aspecto não é tão preocupante se tudo o que você está dizendo é "olá, mas pode ser um grande problema se estiver comunicando algo mais privado ou sensível que não deseja que seja visto por sua companhia telefônica, ISP, um governo hostil ou qualquer outro adversário. Por causa disso, é essencial evitar o uso de ferramentas não criptografadas para enviar mensagens confidenciais (e idealmente qualquer mensagem). Tenha em mente que alguns dos métodos de comunicação mais populares – como SMS e chamadas telefônicas – operam praticamente sem criptografia (como nesta imagem).



Como você pode ver na imagem acima, um smartphone envia uma mensagem de texto verde e não criptografada ("olá") para outro smartphone na extrema direita. Ao longo do caminho, uma torre de celular (ou, no caso de algo enviado pela Internet, seu provedor de serviços de Internet, conhecido como ISP) transmite a mensagem para os servidores da companhia. De lá, o conteúdo salta pela rede para outra torre de celular, que pode ver a mensagem "olá" não criptografada e que, por fim, é roteada para o destino. É importante observar que, sem qualquer criptografia, todos os envolvidos na retransmissão da mensagem, e qualquer um que possa dar uma espiada enquanto ela é transmitida, pode acessar o conteúdo. Esse aspecto não é tão preocupante se tudo o que você está dizendo é "olá", mas pode ser um grande problema se estiver comunicando algo mais privado ou sensível que não deseja que seja visto por sua companhia telefônica, ISP, um governo hostil ou qualquer outro adversário. Por causa disso, é essencial evitar o uso de ferramentas não criptografadas para enviar mensagens confidenciais (e idealmente qualquer mensagem). Tenha em mente que alguns dos métodos de comunicação mais populares – como SMS e chamadas telefônicas – operam praticamente sem criptografia (como na imagem acima).

Há duas maneiras de criptografar dados à medida que se movimentam: ***criptografia da camada de transporte*** e ***criptografia de ponta a ponta***. É importante saber o tipo de criptografia que um provedor de serviços suporta, pois sua organização faz escolhas para adotar práticas e sistemas de comunicação mais seguros. Tais diferenças são bem descritas pelo Guia de autodefesa contra vigilância sendo novamente adaptadas aqui:

Criptografia da camada de transporte

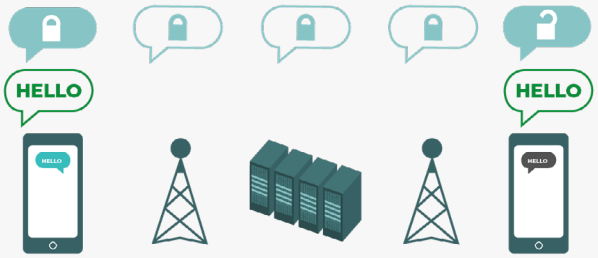
A **criptografia da camada de transporte**, também conhecida como segurança da camada de transporte (TLS), protege as mensagens enquanto elas migram do seu dispositivo para os servidores do aplicativo/serviço de mensagens e de lá para o dispositivo do destinatário. O recurso protege o conteúdo dos olhares indiscretos de hackers que estão acessando sua rede ou dos provedores de serviços de Internet ou telecomunicações. No entanto, no meio do processo, seu provedor de serviços de mensagens/e-mail, o site em que você está navegando ou o aplicativo que você está usando podem visualizar cópias não criptografadas de suas mensagens. Como suas mensagens podem ser vistas (e geralmente são armazenadas) por servidores da companhia, podem ficar vulneráveis a pedidos de execução judicial ou roubo se os servidores da companhia forem afetados.



A imagem acima mostra um exemplo de criptografia da camada de transporte. À esquerda, um smartphone envia uma mensagem verde não criptografada: "Olá". Essa mensagem é criptografada e, depois, transmitida para uma torre de celular. No meio do processo, os servidores da companhia conseguem descriptografar a mensagem, ler o conteúdo, decidir para onde enviá-la, criptografá-la novamente e enviá-la para a próxima torre de celular em direção ao seu destino. No final do processo, o outro smartphone recebe a mensagem criptografada e a descriptografa para ler "Olá".

Criptografia de ponta a ponta

A **criptografia de ponta a ponta** protege as mensagens em trânsito desde o remetente ao destinatário. O recurso garante que a informação seja transformada em mensagem secreta por seu remetente original (o primeiro "fim") e decodificada apenas por seu destinatário final (o segundo "fim"). Ninguém, incluindo o aplicativo ou serviço que você está usando, pode "ouvir" e espionar sua atividade.



A imagem acima mostra um exemplo de criptografia de ponta a ponta. À esquerda, um smartphone envia uma mensagem verde não criptografada: "Olá". Essa mensagem é criptografada e transmitida a uma torre de celular e, em seguida, para os servidores do aplicativo/serviço, que não podem ler o conteúdo, mas repassam a mensagem secreta ao seu destinatário. No final do processo, o outro smartphone recebe a mensagem criptografada e a descriptografa para ler "Olá". Ao contrário da criptografia da camada de transporte, seu ISP ou host de mensagens não pode descriptografar a mensagem. Apenas os pontos da extremidade (os dispositivos originais que enviam e recebem mensagens criptografadas) possuem as chaves para descriptografar e ler a mensagem.

QUE TIPO DE CRIPTOGRAFIA PRECISAMOS?

Ao decidir se sua organização precisa de criptografia da camada de transporte ou criptografia de ponta a ponta para suas comunicações (ou uma combinação das duas para diferentes sistemas e atividades), as grandes questões a serem feitas envolvem confiança. Por exemplo, você confia no aplicativo ou serviço que está usando? Você confia em sua infraestrutura técnica? Você se preocupa com a possibilidade de que um governo hostil possa forçar a companhia a entregar suas mensagens – e, em caso afirmativo, você confia nas políticas da companhia para proteção contra pedidos de execução judicial? Se responder "não" a qualquer uma dessas perguntas, você precisará de criptografia de ponta a ponta. Se responder "sim", um serviço que suporte apenas a criptografia da camada de transporte pode ser suficiente – mas geralmente é melhor optar por serviços compatíveis com criptografia de ponta a ponta quando possível.

Ao enviar mensagens em grupos, lembre-se de que o grau de segurança das suas mensagens se iguala à segurança de todos que as recebem. Além de escolher cuidadosamente aplicativos e sistemas seguros, é importante que todos no grupo sigam outras práticas recomendadas em relação à segurança da conta e do dispositivo. Basta um único agente mal-intencionado ou dispositivo infectado para causar o vazamento do conteúdo de um bate-papo ou chamada do grupo inteiro.

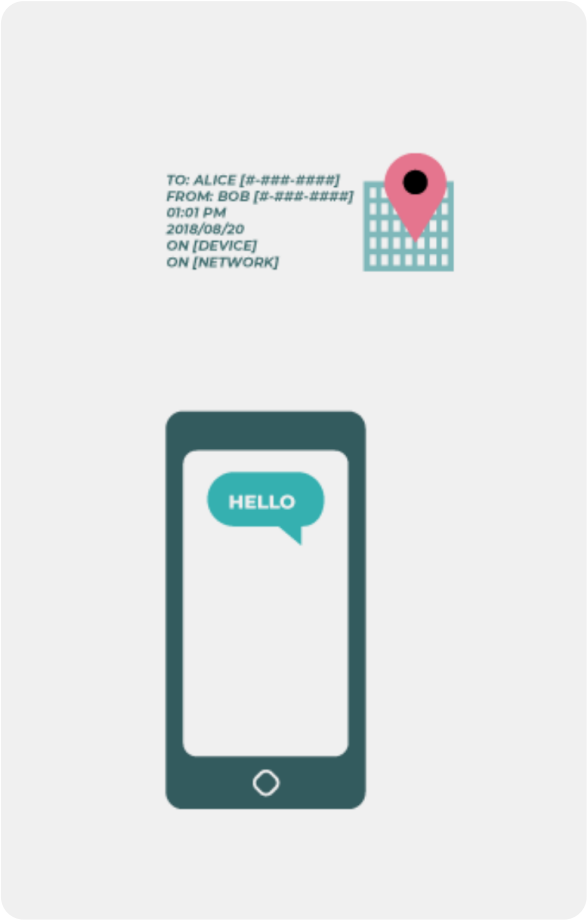
QUAIS FERRAMENTAS DE MENSAGENS CRIPTOGRAFADAS DE PONTA A PONTA DEVEMOS USAR (A PARTIR DE 2022)?

Se você precisar usar criptografia de ponta a ponta ou quiser apenas adotar as práticas recomendadas, independentemente do contexto de ameaças da sua organização, veja alguns exemplos confiáveis de serviços que, **a partir de 2022,** oferecem mensagens e chamadas criptografadas de ponta a ponta. Esta seção do manual será atualizada regularmente no ambiente online. No entanto, observe que tudo muda rapidamente no mundo das mensagens seguras, e essas recomendações podem não estar atualizadas quando você estiver lendo esta seção. Lembre-se de que o grau de segurança das suas comunicações se iguala ao do seu próprio dispositivo. Portanto, além de adotar práticas de mensagens seguras, é essencial implementar as práticas recomendadas descritas na seção **Dispositivos seguros** deste manual.

Ferramentas de comunicação recomendadas com criptografia de ponta a ponta

MENSAGENS DE TEXTO (INDIVIDUAIS OU EM GRUPO)	• **Sinal** • **WhatsApp (somente com configurações específicas detalhadas abaixo)**
CHAMADAS DE ÁUDIO E VÍDEO	• **Sinal (até 40 pessoas)** • **WhatsApp (até 32 pessoas em áudio, oito em vídeo)**
COMPARTILHAMENTO DE ARQUIVOS	• **Sinal** • **Keybase / Keybase Teams** • **OnionShare + um aplicativo de mensagens criptografadas de ponta a ponta como o Signal**

O QUE SÃO METADADOS? DEVEMOS NOS PREOCUPAR COM ELES?



Com quem você e sua equipe conversam e quando e onde você conversa com esses integrantes pode ser tão sensível quanto o que você fala. É importante lembrar que a criptografia de ponta a ponta protege apenas o conteúdo (o "o quê") das suas comunicações. É aqui que os metadados entram em jogo. O Guia de autodefesa contra vigilância da EFF fornece uma visão geral dos metadados e por que eles são importantes para as organizações (incluindo uma ilustração de como são os metadados):

Os metadados costumam ser descritos como todos os aspectos, com exceção do conteúdo de suas comunicações. Você pode pensar em metadados como o equivalente digital de um envelope. Assim como um envelope contém informações sobre o remetente, o destinatário e o destino de uma mensagem, os metadados também contêm esses dados. Os metadados consistem em informações sobre as comunicações digitais que você envia e recebe.

Alguns exemplos de metadados incluem:
- com quem você está se comunicando
- a linha de assunto de seus e-mails
- a duração de suas conversas
- o momento em que uma conversa aconteceu
- sua localização ao se comunicar

Mesmo uma pequena amostra de metadados pode fornecer uma visão íntima das atividades de sua organização. Vamos dar uma olhada em como os metadados podem realmente ser reveladores para os hackers, agências governamentais e companhias que os coletam:

Eles sabem que você ligou para um jornalista e que conversaram por uma hora antes desse mesmo jornalista publicar uma história com uma citação anônima. No entanto, eles não sabem sobre o que vocês conversaram.

Eles sabem que vários funcionários da sua organização enviaram mensagens a um importante instrutor de segurança digital local. No entanto, o tema das mensagens permanece em sigilo.

Eles sabem que você recebeu um e-mail de um serviço de teste de COVID, ligou para seu médico e visitou o site da Organização Mundial da Saúde na mesma hora. No entanto, eles desconhecem o conteúdo do e-mail ou o que você falou no telefone.

Eles sabem que você recebeu um e-mail de um grupo local de defesa dos direitos humanos com o assunto "Diga ao governo: pare de abusar do seu poder". Mas o conteúdo do e-mail é invisível para eles.

Os metadados não são protegidos pela criptografia fornecida pela maioria dos serviços de mensagens. Se estiver enviando uma mensagem no WhatsApp, por exemplo, lembre-se de que, embora o conteúdo seja criptografado de ponta a ponta, ainda é possível que outras pessoas saibam para quem você está enviando mensagens, com que frequência e, para ligações telefônicas, por quanto tempo permaneceu na chamada. Como resultado, você deve ter em mente quais riscos existem (se houver) se determinados adversários puderem descobrir com quem sua organização fala, quando você falou com essas pessoas e (no caso de e-mail) as linhas de assunto gerais das comunicações da sua organização.

Um dos motivos pelos quais o **Signal** é altamente recomendado é que, além de fornecer criptografia de ponta a ponta, **introduziu recursos e assumiu compromissos para reduzir a quantidade de metadados que registra e armazena**. Por exemplo, o recurso Remitente selado do Signal criptografa os metadados sobre quem está falando com quem, para que o Signal conheça apenas o destinatário de uma mensagem, mas não o remetente. Por padrão, esse recurso só funciona ao se comunicar com contatos ou perfis (pessoas) existentes com quem você já se comunicou ou que armazenou em sua lista de contatos. No entanto, você pode habilitar essa configuração "Remitente selado" para "Permitir de qualquer pessoa" se considerar importante eliminar esses metadados em todas as conversas do Signal, mesmo com pessoas desconhecidas para você.

E O E-MAIL?

A maioria dos provedores de e-mail, como Gmail, Microsoft Outlook e Yahoo Mail, emprega criptografia da camada de transporte. Portanto, se for necessário comunicar conteúdo confidencial usando o e-mail e estiver preocupado com o fato de seu provedor de e-mail ser legalmente obrigado a fornecer informações sobre suas comunicações ao governo ou outro adversário, considere usar uma opção de e-mail criptografado de ponta a ponta. Tenha em mente, no entanto, que mesmo as opções de e-mail criptografado de ponta a ponta deixam algo a desejar do ponto de vista da segurança, por exemplo, ao não criptografar linhas de assunto de e-mails e não proteger metadados. Se precisar comunicar informações particularmente confidenciais, o e-mail não é a melhor opção. Em vez disso, opte por opções de mensagens seguras, como o Signal.

Se sua organização continuar usando o e-mail, é fundamental adotar um sistema para toda a organização. Essa opção ajuda a limitar os riscos comuns que surgem quando a equipe usa endereços de e-mail pessoais para seu trabalho, como práticas inadequadas de segurança da conta. Por exemplo, ao fornecer contas de e-mail para a equipe que foram emitidas pela organização, você pode aplicar as práticas recomendadas, como senhas fortes e autenticação de dois fatores (2FA) em qualquer conta gerenciada por sua organização. Se, de acordo com sua análise acima, a criptografia de ponta a ponta for necessária para seu e-mail, tanto o Protonmail quanto o Tutanota oferecem planos para organizações. Se a criptografia da camada de transporte for adequada para o e-mail da sua organização, opções como Google Workspace (Gmail) ou Microsoft 365 (Outlook) podem ser úteis.

PODEMOS REALMENTE CONFIAR NO WHATSAPP?

O WhatsApp é uma escolha popular para o envio de mensagens seguras e pode ser uma boa opção devido à sua onipresença. Algumas pessoas se preocupam com a propriedade e controle do recurso, que são detidos pelo Facebook, plataforma que vem trabalhando para integrá-lo a seus outros sistemas. As pessoas também estão preocupadas com a quantidade de metadados (ou seja, informações sobre com quem você se comunica e quando) que o WhatsApp coleta. Se optar por usar o WhatsApp como uma opção de mensagens seguras, leia a seção acima sobre metadados. Há também algumas configurações necessárias para garantir que estejam configuradas corretamente. O mais importante é desativar os backups na nuvem ou, no mínimo, ativar o novo recurso de backups criptografados de ponta a ponta do WhatsApp usando uma chave criptográfica de 64 dígitos ou uma senha longa, aleatória e exclusiva salva em um local seguro (como seu gerenciador de senhas). Além disso, certifique-se de mostrar as notificações de segurança e verificar os códigos de segurança. Você pode encontrar guias de instruções simples sobre como definir essas configurações para telefones Android aqui e iPhones aqui. **Se sua equipe *e aqueles com quem você se comunica* não configurarem adequadamente essas opções, deixe de considerar o WhatsApp uma boa opção para comunicações confidenciais que exigem criptografia de ponta a ponta.** O Signal continua sendo a melhor opção para essas necessidades de mensagens criptografadas de ponta a ponta, dadas suas configurações padrão seguras e proteção de metadados.

E QUANTO A MENSAGENS DE TEXTO?

Mensagens de texto básicas são altamente precárias em termos de segurança (o SMS padrão é efetivamente não criptografado) e devem ser evitadas para qualquer assunto que não seja de conhecimento público. Embora as mensagens de iPhone para iPhone da Apple (conhecidas como iMessages) sejam criptografadas de ponta a ponta, se um smartphone que não seja iPhone estiver na conversa, as mensagens não serão protegidas. É melhor estar seguro e **evitar mensagens de texto para qualquer assunto remotamente sensível, privado ou confidencial**.

POR QUE O TELEGRAM, O FACEBOOK MESSENGER OU O VIBER NÃO SÃO RECOMENDADOS PARA BATE-PAPOS SEGUROS?

Alguns serviços, como o Facebook Messenger e o Telegram, só oferecem criptografia de ponta a ponta se você a ativar deliberadamente (e apenas para bate-papos individuais), ou seja, não são boas opções para mensagens confidenciais ou privadas, principalmente para uma organização. Não confie nessas ferramentas se precisar usar criptografia de ponta a ponta, afinal, é muito fácil esquecer de mudar as configurações padrão e menos seguras. O Viber afirma oferecer criptografia de ponta a ponta, mas não disponibilizou seu código para revisão a pesquisadores de segurança externos. O código do Telegram também não foi disponibilizado para uma auditoria pública. Como resultado, muitos especialistas temem que a criptografia do Viber (ou "chats secretos" do Telegram) possa ser inferior ao padrão e, portanto, não adequada para comunicações que exigem a verdadeira criptografia de ponta a ponta.

NOSSOS CONTATOS E COLEGAS ESTÃO USANDO OUTROS APLICATIVOS DE MENSAGENS; COMO PODEMOS CONVENCÊ-LOS A BAIXAR UM NOVO APLICATIVO PARA SE COMUNICAR CONOSCO?

Às vezes, há uma troca entre segurança e conveniência, mas certo grau de esforço extra vale a pena para comunicações confidenciais. Apresente um bom exemplo para seus contatos. Se tiver que usar outros sistemas menos seguros, esteja muito consciente do que está dizendo. Evite discutir assuntos delicados. Em algumas organizações, pode ser usado um sistema para bate-papo geral e outro para comunicação com a liderança sobre questões mais confidenciais. Certamente seria mais simples se todos os recursos fossem criptografados automaticamente o tempo todo, sem a necessidade de lembretes ou preocupações. Felizmente, aplicativos criptografados de ponta a ponta, como o Signal, estão se tornando cada vez mais populares e fáceis de usar, sem mencionar que foram traduzidos para dezenas de idiomas para uso global. Se seus parceiros ou outros contatos precisarem de ajuda para alternar as comunicações para uma opção criptografada de ponta a ponta, como o Signal, reserve um tempo para explicar a eles por que é tão importante proteger devidamente suas comunicações. Quando todos entenderem a importância, os poucos minutos exigidos para baixar um novo aplicativo e os dias necessários para se acostumar a usá-lo não parecerão grande coisa.

EXISTEM OUTRAS CONFIGURAÇÕES PARA APLICATIVOS CRIPTOGRAFADOS DE PONTA A PONTA QUE DEVEMOS CONHECER?

No aplicativo Signal, a verificação dos códigos de segurança (que eles chamam de números de segurança) também é importante. Para ver um número de segurança e verificá-lo no Signal, abra seu bate-papo com um contato, toque no nome dele na parte superior da tela e role para baixo para tocar em "Ver número de segurança". Se o seu número de segurança corresponder ao seu contato, marque-o como "verificado" nessa mesma tela. Se receber uma notificação em um bate-papo de que seu número de segurança com determinado contato foi alterado, é especialmente importante prestar atenção a esses números de segurança e verificar seus contatos. Se você ou outra equipe precisar de ajuda para definir essas configurações, o próprio Signal **fornece instruções úteis**. Se estiver usando o Signal, que é amplamente considerado a melhor opção intuitiva para mensagens seguras e chamadas individuais, certifique-se de **definir um PIN forte**. Use pelo menos seis dígitos, e não algo fácil de adivinhar como sua data de nascimento. Para obter mais dicas sobre como configurar corretamente o **Signal** e o **WhatsApp**, confira os **guias de ferramentas** para ambos desenvolvidos pela EFF no Guia de autodefesa contra vigilância.

Uso de aplicativos de bate-papo no mundo real

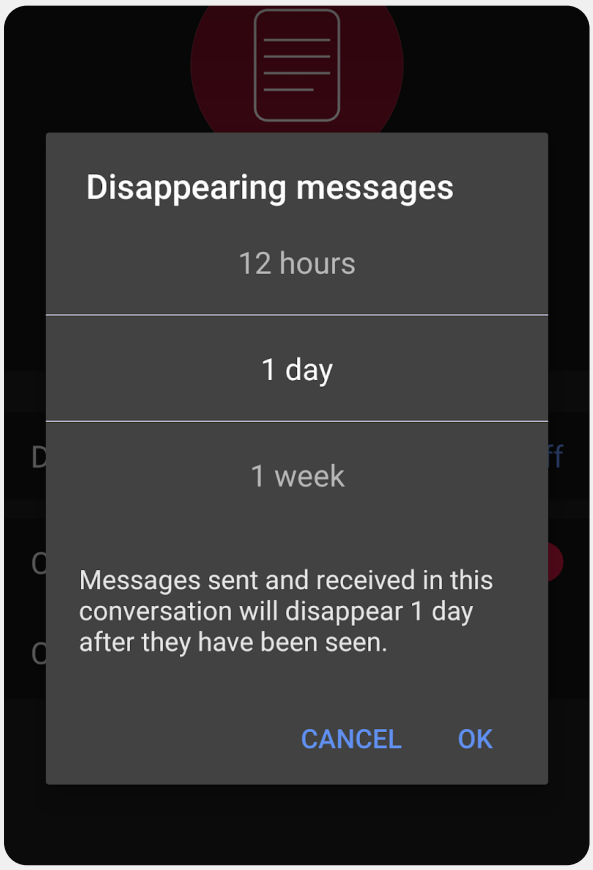
Para limitar os danos em caso de perda, roubo ou confisco de um telefone, a prática recomendada é minimizar o histórico de mensagens salvas no telefone. Uma maneira fácil de fazer isso é ativar as **"mensagens que desaparecem"** para os bate-papos em grupo da sua organização e incentivar a equipe a fazer o mesmo nos bate-papos pessoais.

No Signal e em outros aplicativos de mensagens populares, você pode definir um cronômetro para que as mensagens desapareçam depois a leitura, após um número de minutos ou horas definido. Essa configuração pode ser personalizada com base no bate-papo ou grupo individual. Para a maioria de nós, definir uma janela de desaparecimento para o período de uma semana proporciona tempo suficiente para conferir o conteúdo sem preservar mensagens desnecessárias, mas que podem ser usadas contra você no futuro. Lembre-se, ninguém pode roubar o que você não possui.

Para ativar as mensagens que desaparecem no Signal, abra um bate-papo, toque no nome da pessoa/grupo com quem você está conversando, toque em mensagens que desaparecem, escolha um cronômetro e toque em OK. Uma configuração semelhante existe no WhatsApp.

Em situações mais graves em que há a necessidade de excluir imediatamente uma mensagem, talvez porque o telefone de alguém foi roubado ou você enviou uma mensagem para a pessoa errada, observe que o Signal permite excluir uma mensagem para um grupo ou indivíduo do telefone dentro de três horas após o envio, apenas eliminando-a do bate-papo. O Telegram continua sendo popular em muitos países, apesar de suas limitações de criptografia para um recurso semelhante que permite que os usuários excluam mensagens entre dispositivos sem restrições.

Com isso dito, se sua organização está preocupada com a segurança da equipe como resultado de comunicações que podem ser vistas em seus telefones, usar mensagens que desaparecem com temporizadores curtos é provavelmente a opção mais simples e sustentável.



E AS VIDEOCHAMADAS EM GRUPO MAIORES? EXISTEM OPÇÕES CRIPTOGRAFADAS DE PONTA A PONTA?

Com o aumento do trabalho remoto, é importante ter uma opção segura para as videochamadas em grandes grupos da sua organização. Infelizmente, atualmente não existem grandes opções que atendam a todos os requisitos: fácil de usar, suporta um grande número de participantes e recursos de colaboração e habilita a criptografia de ponta a ponta por padrão.

Para grupos de até 40 pessoas, o Signal é uma opção criptografada de ponta a ponta altamente recomendada. As chamadas de vídeo em grupo no Signal podem ser acessadas a partir de um smartphone ou do aplicativo Signal para desktop em um computador, o que permite o compartilhamento de tela. No entanto, lembre-se de que apenas seus contatos que já usam o Signal podem ser adicionados a um grupo do Signal.

Se estiver procurando por outras opções, **Jitsi Meet** é uma plataforma que adicionou recentemente uma configuração criptografada de ponta a ponta. O Jitsi Meet é uma solução de conferência de áudio e vídeo baseada na web que pode funcionar para grandes públicos (até 100 pessoas) e não requer download de aplicativo ou software especial. Observe que, se usar esse recurso com grupos grandes (mais de 15 a 20 pessoas), a qualidade da chamada pode diminuir. Para configurar uma reunião no Jitsi Meet, você pode acessar **meet.jit.si**, digitar o código da reunião e compartilhar esse link (por meio de um canal seguro como o Signal) com os participantes desejados. Para usar criptografia de ponta a ponta, dê uma olhada nessas **instruções** descritas por Jitsi. Observe que todos os usuários individuais precisarão habilitar a criptografia de ponta a ponta para que funcione. Ao usar o Jitsi, certifique-se de criar nomes aleatórios de salas de reunião e usar senhas fortes para proteger suas chamadas.

Se essa opção não funcionar para sua organização, considere usar uma opção comercial popular como Webex ou Zoom com criptografia de ponta a ponta habilitada. Faz um tempo desde que o Webex passou a permitir a criptografia de ponta a ponta; no entanto, essa opção não está ativada por padrão e exige que os participantes baixem o Webex para entrar na sua reunião.

Para obter a opção criptografada de ponta a ponta para sua conta Webex, abra um caso de suporte Webex e siga **essas instruções** para garantir que a criptografia de ponta a ponta esteja configurada. Apenas o organizador da reunião precisa habilitar a criptografia de ponta a ponta. Se as instruções forem seguidas, a reunião completa será criptografada de ponta a ponta. Se estiver usando Webex para reuniões e workshops de grupo seguros, também certifique-se de habilitar senhas fortes em suas chamadas.

Após meses de imprensa negativa, o Zoom desenvolveu uma **opção de criptografia de ponta a ponta** para suas chamadas. No entanto, essa opção não está ativada por padrão, exige que o host da chamada associe sua conta a um número de telefone e só funciona se todos os participantes ingressarem por meio do aplicativo Zoom para desktop ou móvel em vez de discar. Como é fácil configurar incorretamente essas configurações por acidente, não é ideal confiar no Zoom como uma opção criptografada de ponta a ponta. No entanto, se a criptografia de ponta a ponta for necessária e o Zoom for sua única opção, siga as **instruções** do Zoom para configurá-la. Apenas certifique-se de verificar qualquer chamada antes de começar para garantir que ela seja realmente criptografada de ponta a ponta. Para isso, clique no cadeado verde no canto superior esquerdo da tela do Zoom e confira se a indicação "ponta a ponta" está listada ao lado da configuração de criptografia. Você também deve definir uma senha forte para qualquer reunião do Zoom.

Além das ferramentas mencionadas acima, **este fluxograma**, desenvolvido pela Frontline Defenders destaca algumas opções de videochamada e conferência que, dependendo do seu contexto de risco, podem fazer sentido para sua organização.

Vale a pena notar, no entanto, que certos recursos populares das ferramentas acima só funcionam com criptografia da camada de transporte. Por exemplo, ativar a criptografia de ponta a ponta no Zoom desativa as salas de sessão de grupo, recursos de pesquisa e gravação na nuvem. No Jitsi Meet, as salas temáticas podem desabilitar o recurso de criptografia de ponta a ponta, levando a uma diminuição involuntária da segurança.

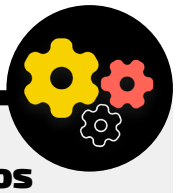
E SE REALMENTE NÃO PRECISARMOS DE CRIPTOGRAFIA DE PONTA A PONTA PARA TODAS AS NOSSAS COMUNICAÇÕES?

Se a criptografia de ponta a ponta não for necessária para todas as comunicações da sua organização com base em sua avaliação de risco, considere o uso de aplicativos protegidos por criptografia da camada de transporte. Lembre-se de que esse tipo de criptografia exige que você confie no provedor de serviços, como Google para Gmail, Microsoft para Outlook/Exchange ou Facebook para Messenger, porque eles (e qualquer pessoa com quem possam ser obrigados a compartilhar informações) podem ver/ouvir suas informações. comunicações. Mais uma vez, as melhores opções dependerão do seu modelo de ameaça (por exemplo, se você não confia no Google ou se o governo dos EUA é seu adversário, o Gmail não é uma boa opção), mas algumas opções populares e normalmente confiáveis incluem:

E-MAIL	• **Gmail (via Google Workspace)** • **Outlook (via Office 365)** • Não hospede seu próprio servidor Microsoft Exchange para o e-mail de sua organização. **Se estiver fazendo isso, é necessário migrar para o Office 365.**
MENSAGENS DE TEXTO (INDIVIDUAIS OU EM GRUPO)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
CONFERÊNCIAS EM GRUPO, CHAMADAS DE ÁUDIO E VÍDEO	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **Webex** • **GotoMeeting** • **Zoom**
COMPARTILHAMENTO DE ARQUIVOS	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**

UMA OBSERVAÇÃO SOBRE O COMPARTILHAMENTO DE ARQUIVOS

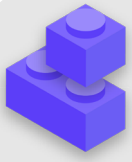
Além de compartilhar mensagens com segurança, compartilhar arquivos com essa mesma proteção provavelmente consiste em uma parte importante do plano de segurança da sua organização. A maioria das opções de compartilhamento de arquivos é integrada aos aplicativos ou serviços de mensagens que você já pode estar usando. Por exemplo, compartilhar arquivos via Signal é uma ótima opção se a criptografia de ponta a ponta for necessária. Se a criptografia da camada de transporte for suficiente, usar o Google Drive ou o Microsoft SharePoint pode ser uma boa opção para sua organização. Apenas certifique-se de definir as configurações de compartilhamento corretamente para que somente as pessoas adequadas tenham acesso a determinado documento ou pasta, e verifique se esses serviços estão conectados às contas de e-mail organizacionais (não pessoais) da equipe. Se puder, proíba o compartilhamento de arquivos confidenciais através de anexos por e-mail ou fisicamente com USBs. O uso de dispositivos como USBs em sua organização aumenta consideravelmente a probabilidade de malware ou roubo. Ou seja, confiar em e-mails ou outras formas de anexos enfraquece as defesas de sua organização contra ataques de phishing.



Alternativas organizacionais para compartilhamento de arquivos

Se estiver procurando por uma opção segura de compartilhamento de arquivos para sua organização que não esteja diretamente incorporada a uma plataforma de mensagens (ou talvez esteja atingindo limites de tamanho de arquivo ao compartilhar documentos grandes), considere o OnionShare. **OnionShare** é uma ferramenta de código aberto que permite compartilhar arquivos de qualquer tamanho de forma segura e anônima. Para que funcione, o remetente deve baixar o aplicativo OnionShare (disponível em computadores Mac, Windows e Linux), fazer upload do(s) arquivo(s) que deseja compartilhar e gerar um link exclusivo. Este link, que só pode ser processado no navegador Tor, pode ser compartilhado através de qualquer canal de mensagens seguro (Signal, por exemplo) para o destinatário pretendido. O destinatário pode, então, abrir o link no navegador Tor e baixar o(s) arquivo(s) em seu computador. Lembre-se de que o grau de segurança dos seus arquivos se iguala ao do método pelo qual você compartilha o link. O Tor será explicado mais detalhadamente em uma seção "avançada" posterior do manual. No entanto, se você não tem uma opção de provedor de nuvem confiável para fins de compartilhamento de arquivos em sua organização, lembre-se do OnionShare como uma alternativa mais segura ao compartilhamento de arquivos grandes em USBs no escritório.

Se sua organização já está investindo em um gerenciador de senhas, conforme descrito na seção sobre senhas deste manual, e opta pela conta premium ou de times do Bitwarden, o recurso **Bitwarden Send** é outra opção para compartilhamento seguro de arquivos. Esse recurso permite que os usuários criem links seguros para compartilhar arquivos criptografados por meio de qualquer canal de mensagens seguro (como o Signal). O tamanho do arquivo é limitado a 100 MB, mas o Bitwarden Send permite definir uma data de expiração nos links, proteger com senha o acesso a arquivos compartilhados e limitar o número de vezes que seu link pode ser aberto.



Comunicação e compartilhamento de dados com segurança

- **Exija o uso de serviços confiáveis de mensagens criptografadas de ponta a ponta para as comunicações confidenciais de sua organização (e idealmente para todas as comunicações).**
  - Reserve um tempo para explicar à equipe e aos parceiros externos por que as comunicações seguras são tão importantes. Fazer isso aumentará o sucesso do seu plano.
- **Defina uma política sobre por quanto tempo você reterá mensagens e quando e se a organização usará comunicações de "desaparecimento".**
- **Certifique-se de que as configurações adequadas estejam em vigor para aplicativos de comunicações seguras, incluindo:**
  - Certifique-se de que toda a equipe esteja atenta às notificações de segurança e, se estiver usando o WhatsApp, não faça backup dos bate-papos.
  - Se estiver usando um aplicativo em que a criptografia de ponta a ponta não esteja habilitada por padrão (por exemplo, Zoom ou Webex), verifique se os usuários necessários ativaram as configurações adequadas no início de qualquer chamada ou reunião.
- **Use serviços de e-mail baseados em nuvem, como Office 365 ou Gmail para sua organização.**
  - Não tente hospedar seu próprio servidor de e-mail.
  - Não permita que os funcionários usem contas de e-mail pessoais para trabalhar.
- **Relembre a organização com frequência das práticas recomendadas de segurança relacionadas a mensagens e metadados de grupo.**
  - Esteja ciente de quem está incluído em mensagens de grupo, bate-papos e conversas de e-mail.

Como armazenar dados com segurança

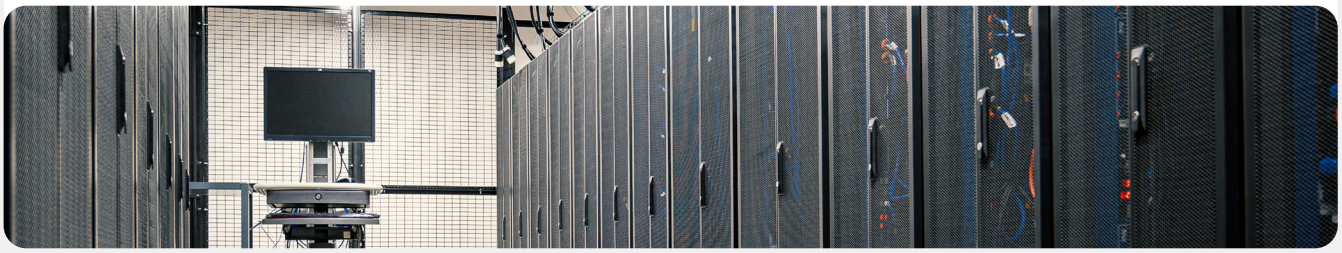
Para a maioria das organizações da sociedade civil, uma das decisões mais importantes a serem tomadas é onde armazenar seus dados.

É "mais seguro" armazenar dados nos computadores da equipe, em um servidor local, em dispositivos de armazenamento externo ou na nuvem? Em 99% das situações, a opção mais fácil e segura é manter os dados armazenados em serviços confiáveis de armazenamento em nuvem. Talvez os exemplos mais comuns sejam o Microsoft 365 e o Google Drive. Sem um plano abrangente de armazenamento em nuvem, é provável que os dados da sua organização sejam mantidos em vários locais, incluindo computadores da equipe, discos rígidos externos e até mesmo servidores locais. Embora seja possível proteger os dados em todos esses dispositivos, é muito difícil que isso seja feito de forma bem-sucedida sem gastar muito dinheiro e sem contratar uma equipe de TI significativa.

Ao selecionar uma ferramenta ou serviço para armazenar seus dados, certifique-se de confiar na companhia ou grupo relacionado. Uma rápida pesquisa no Google e uma verificação com especialistas em segurança digital podem ajudar significativamente na confiabilidade de um fornecedor de tecnologia em potencial. Algumas perguntas a serem lembradas incluem: Ele vende ou compartilha seus dados privados? Ele tem recursos de segurança adequados na equipe? Ele oferece recursos de segurança (como 2FA) para ajudá-lo a proteger sua conta?

O armazenamento de dados e a sociedade civil

O advento do armazenamento acessível de dados baseado em nuvem (às vezes gratuito) tornou a vida mais fácil (e mais segura) para muitas organizações da sociedade civil com recursos limitados. Infelizmente, muitos ainda tentam hospedar seus próprios servidores com orçamento, equipe e suporte de TI relativamente limitados. Em março de 2021, a ameaça de tal infraestrutura organizacional tornou-se real para milhares de organizações do mundo, quando Hafnium, um agente de ameaças afiliado ao governo chinês, desencadeou uma catástrofe de segurança cibernética global através de um ataque sofisticado feito em servidores Microsoft Exchange auto-hospedados. O ataque comprometeu os servidores locais e permitiu que os hackers tivessem acesso a contas de e-mail organizacionais, instalassem malware adicional nos servidores das vítimas e sistemas conectados e, por fim, extraíssem dados confidenciais. Embora a Microsoft tenha publicado rapidamente uma atualização e instruções para identificar e remover possíveis invasores assim que os ataques se tornaram públicos, muitas organizações não tinham a devida capacidade de TI para aplicar essas atualizações com urgência, deixando-as expostas por longos períodos. O escopo e impacto desse ataque global revelam o perigo que pode surgir quando organizações cívicas optam por auto-hospedar servidores de e-mail e outros tipos de dados confidenciais. principalmente sem um investimento significativo em uma equipe dedicada de segurança cibernética.



BENEFÍCIOS DO ARMAZENAMENTO EM NUVEM

Mesmo que você tome todas as medidas certas para proteger seus computadores contra malware e roubo físico, ainda é possível que um adversário invada seu computador ou servidor local. É muito mais difícil para eles derrotar as defesas de segurança, por exemplo, do Google ou Microsoft. Boas companhias de armazenamento em nuvem possuem recursos de segurança incomparáveis e têm um forte incentivo comercial para fornecer segurança máxima aos seus usuários. Resumindo: uma estratégia confiável de armazenamento em nuvem será muito mais fácil de implementar e manter segura ao longo do tempo. Portanto, em vez de se preocupar em tentar proteger seu próprio servidor, você pode concentrar sua energia em tarefas mais simples. Manter a maior parte de suas informações na nuvem ajuda com uma série de riscos comuns. O computador de alguém foi deixado em um restaurante ou o celular no ônibus? Seu filho derrubou um copo de suco no teclado, o que prejudicou a operação do dispositivo? Um funcionário foi infectado por malware, precisa apagar seu computador e começar do zero? Se a maioria dos documentos e dados estiver na nuvem, é fácil sincronizar novamente e começar do zero em um computador limpo ou totalmente novo. Além disso, se o malware entrar em um computador ou se um ladrão escanear um disco rígido, não há nada a ser roubado se a maioria dos documentos for acessada pelo navegador de internet.

QUAL PROVEDOR DE ARMAZENAMENTO EM NUVEM DEVEMOS ESCOLHER?

As duas opções de armazenamento em nuvem mais populares são o Google Workspace (anteriormente conhecido como GSuite) e o Microsoft 365. Se você e sua equipe já usam o Gmail, faz muito sentido inscrever sua organização no Google Workspace e armazenar dados no Google Drive com os aplicativos Google Docs, Sheets e Slides integrados para processamento de texto, planilhas e apresentações. Da mesma forma, se você for uma organização que depende do Excel e do Word, a opção mais fácil é assinar o Microsoft 365, que concede à sua organização acesso ao Outlook para e-mail e versões licenciadas do Microsoft Word, Excel, Powerpoint e Teams. Independentemente de qual provedor você escolher, armazenar dados com segurança na nuvem requer a implementação de boas configurações de compartilhamento e treinamento da equipe para entender como e quando compartilhar (e não compartilhar) pastas e documentos. Em geral, você deve configurar pastas em sua unidade de armazenamento em nuvem que restrinjam o acesso apenas à equipe que precisa delas para determinados arquivos. Faça auditorias rotineiras em seu sistema para garantir que você não esteja "compartilhando demais" nenhum arquivo (como ativar o compartilhamento de link universal para arquivos que deveriam ser limitados a apenas algumas pessoas).

E SE NÃO CONFIARMOS NO GOOGLE OU NA MICROSOFT OU EM OUTROS PROVEDORES DE ARMAZENAMENTO EM NUVEM?

Se um de seus adversários (por exemplo, um governo estrangeiro ou local) puder forçar legalmente o Google ou a Microsoft (ou outro provedor de armazenamento em nuvem) a entregar dados, talvez não faça sentido escolhê-los como opções de armazenamento de dados. Esse risco pode ser maior se seu adversário for o governo dos Estados Unidos, por exemplo, mas muito menor se seu adversário for um regime autoritário. Lembre-se de que o Google e a Microsoft têm políticas sobre apenas entregar dados quando legalmente obrigados a fazê-lo e reconhecem que sua própria organização pode estar vulnerável ao mesmo tipo de demandas legais de seu próprio governo se hospedar dados localmente. Em situações em que o armazenamento em nuvem do Google ou da Microsoft não faz sentido para sua organização, uma opção alternativa a ser considerada é o **Keybase**. O recurso "times" no Keybase permite que sua organização compartilhe arquivos e mensagens usando criptografia de ponta a ponta em um ambiente de nuvem seguro sem precisar depender de um provedor terceirizado. Por isso, pode ser uma boa opção para armazenar documentos e arquivos com segurança em toda a sua organização. No entanto, o Keybase é menos familiar para a maioria dos usuários, portanto, esteja ciente de que a adoção dessa ferramenta provavelmente exigirá mais treinamento e esforço do que outras soluções mencionadas. Com isso dito, se você optar por seguir sozinho e não usar o armazenamento em nuvem, é crucial que você invista tempo e recursos para fortalecer as defesas digitais dos dispositivos de sua organização e garantir que todos os servidores locais sejam configurados, criptografados e mantidos fisicamente seguros. Você pode economizar nas taxas de assinatura mensais, mas isso custará à sua organização tempo e recursos da equipe, além de ser muito mais vulnerável a ataques.

COMO FAZER O BACKUP DE DADOS

Quer sua organização armazene dados em dispositivos físicos ou na nuvem, é importante ter um backup. Lembre-se de que, se você confiar no armazenamento físico do dispositivo, é muito fácil perder o acesso aos seus dados. Você pode derramar café

no seu computador e destruir o disco rígido. Os computadores da equipe podem ser invadidos e todos os arquivos locais bloqueados com ransomware. Alguém pode perder um dispositivo no trem ou ter sua pasta com o aparelho roubada. Como mencionado acima, esse é outro motivo pelo qual o uso do armazenamento em nuvem pode ser um benefício, pois não está vinculado a um dispositivo específico que pode ser infectado, perdido ou roubado. Os computadores Mac vêm com um software de backup integrado chamado Time Machine, que é usado em conjunto com um dispositivo de armazenamento externo; para dispositivos Windows, o Histórico de arquivos oferece funcionalidade semelhante. iPhones e Androids podem fazer backup automático de seus conteúdos mais importantes na nuvem, se ativado nas configurações do seu telefone. Se sua organização estiver usando armazenamento em nuvem (como o Google Drive), o risco de o Google ser desativado ou seus dados destruídos em um desastre é bastante baixo, mas o erro humano (como excluir arquivos importantes acidentalmente) ainda é uma possibilidade. Explorar uma solução de backup em nuvem como Backupify ou SpinOne Backup pode valer a pena. Se os dados forem armazenados em um servidor local ou dispositivos locais, um backup seguro se torna ainda mais crucial. Você pode fazer backup dos dados da sua organização em um disco rígido externo, mas certifique-se de criptografar esse disco rígido com uma senha forte. O Time Machine pode criptografar discos rígidos para você ou você pode usar ferramentas de criptografia confiáveis para todo o disco rígido, como VeraCrypt ou BitLocker. Certifique-se de manter todos os dispositivos de backup em um local separado de seus outros dispositivos e arquivos. Lembre-se, um incêndio que destrói seus computadores e seus backups significa que você não tem nenhum backup. Considere manter uma cópia em um local muito seguro, como um cofre.

Observação: se estiver usando um provedor de nuvem em um país com leis específicas de localização de dados, consulte especialistas jurídicos para entender melhor como uma solução de armazenamento em nuvem pode cumprir os requisitos locais. Muitos provedores de armazenamento em nuvem, incluindo o Google e a Microsoft, agora oferecem opções que permitem que alguns clientes escolham a localização geográfica de seus dados na nuvem, por exemplo.



Como aprimorar a segurança das contas das organizações na nuvem

Se a sua organização optar por configurar um domínio no Google Workspace ou no Microsoft 365, saiba que ambas as companhias oferecem níveis mais elevados de segurança (gratuitamente, em muitos casos) para organizações da sociedade civil. O Programa de Proteção Avançada do Google e o AccountGuard da Microsoft proporcionam segurança ainda mais robusta para todas as contas na nuvem da sua organização. Além disso, esses recursos ajudam a reduzir consideravelmente a probabilidade de phishing eficaz e comprometimento da conta. Se você acredita que sua organização se qualifica e estiver interessado em inscrever sua organização em qualquer um dos planos, visite os sites vinculados acima ou entre em contato com cyberhandbook@ndi.org para obter mais assistência.



Como armazenar dados com segurança

- **Armazene dados confidenciais exclusivamente em um serviço de armazenamento em nuvem confiável.**
  - Certifique-se de que todas as contas conectadas usadas para acessar esse serviço tenham senhas fortes e autenticação de dois fatores.
- **Defina e aplique uma política para limitar as configurações de compartilhamento na nuvem.**
  - Treine todos os funcionários sobre como compartilhar corretamente (e não compartilhar demais) os documentos.
- **Se sua organização optar por armazenar dados localmente, invista em uma equipe de TI qualificada.**
- **Mantenha seus backups de dados seguros – criptografe os discos rígidos de backup ou outros dispositivos de backup.**



Como estar seguro na Internet

Desenvolvimento de uma cultura de segurança

Uma base forte: Como proteger contas e dispositivos

Comunicação e armazenamento de dados com segurança

Como estar seguro na Internet

Proteção da segurança física

O que fazer diante de imprevistos

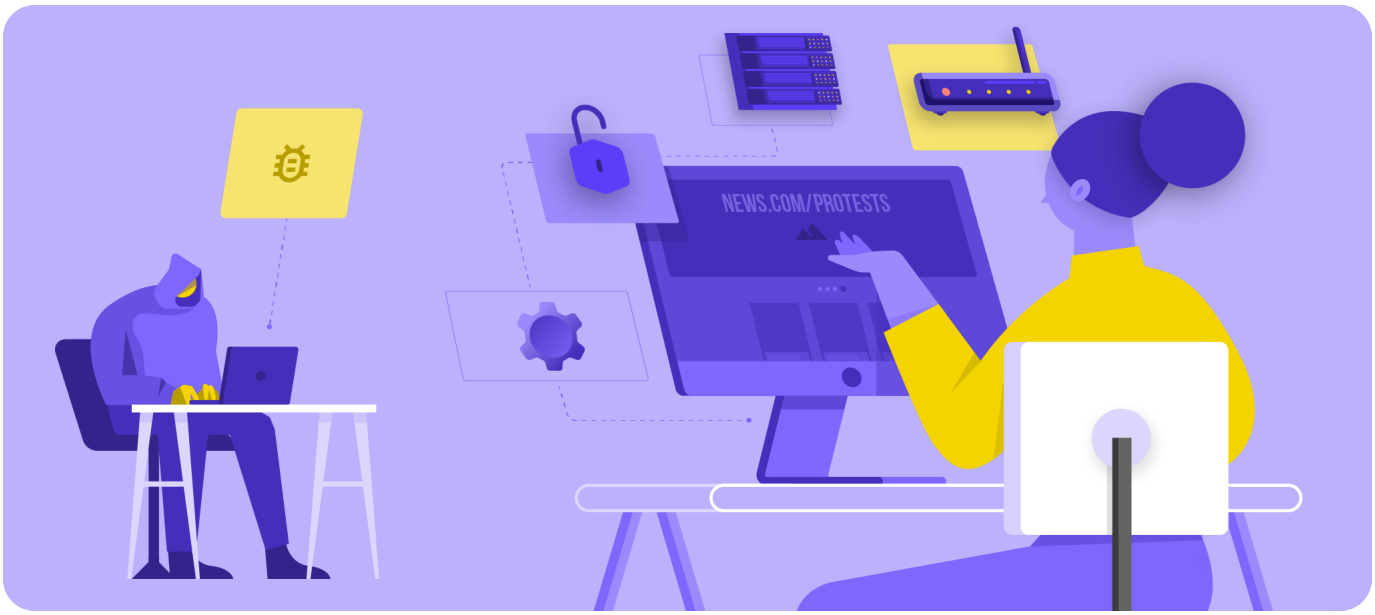
Ao usar a Internet em seu telefone ou computador, sua atividade pode dizer muito sobre você e sua organização.

É importante manter dados confidenciais – como nomes de usuário e senhas que você digita em um site, suas postagens de mídia social ou, em certos contextos, até os nomes dos sites que você visita – fora da vista de olhares indiscretos. Ter seu acesso a determinados sites ou aplicativos bloqueados ou restritos também é uma preocupação comum. Esses dois problemas – vigilância na Internet e censura na Internet – andam de mãos dadas, e as estratégias para reduzir seus impactos são semelhantes.

Navegação com segurança

USAR HTTPS

O passo mais importante para limitar a capacidade de um adversário de vigiar sua organização online é minimizar a quantidade de informações disponíveis sobre você e a atividade de seus colegas na Internet. Sempre verifique se você está se conectando a sites com segurança: certifique-se de que o URL (local) comece com "https" e mostre um pequeno ícone de cadeado na barra de endereços do seu navegador. Quando você navega na Internet **sem criptografia**, as informações que você digita em um site (como senhas, números de conta ou mensagens) e os detalhes do site e das páginas que você está visitando são expostos. Isso significa que (1) quaisquer hackers em sua rede, (2) seu administrador de rede, (3) seu ISP e qualquer entidade com quem eles possam compartilhar dados (como autoridades governamentais), (4) o ISP do site que você está visitando e qualquer entidade com a qual eles possam compartilhar dados e, claro, (5) o site que você está visitando têm acesso a muitas informações potencialmente confidenciais.



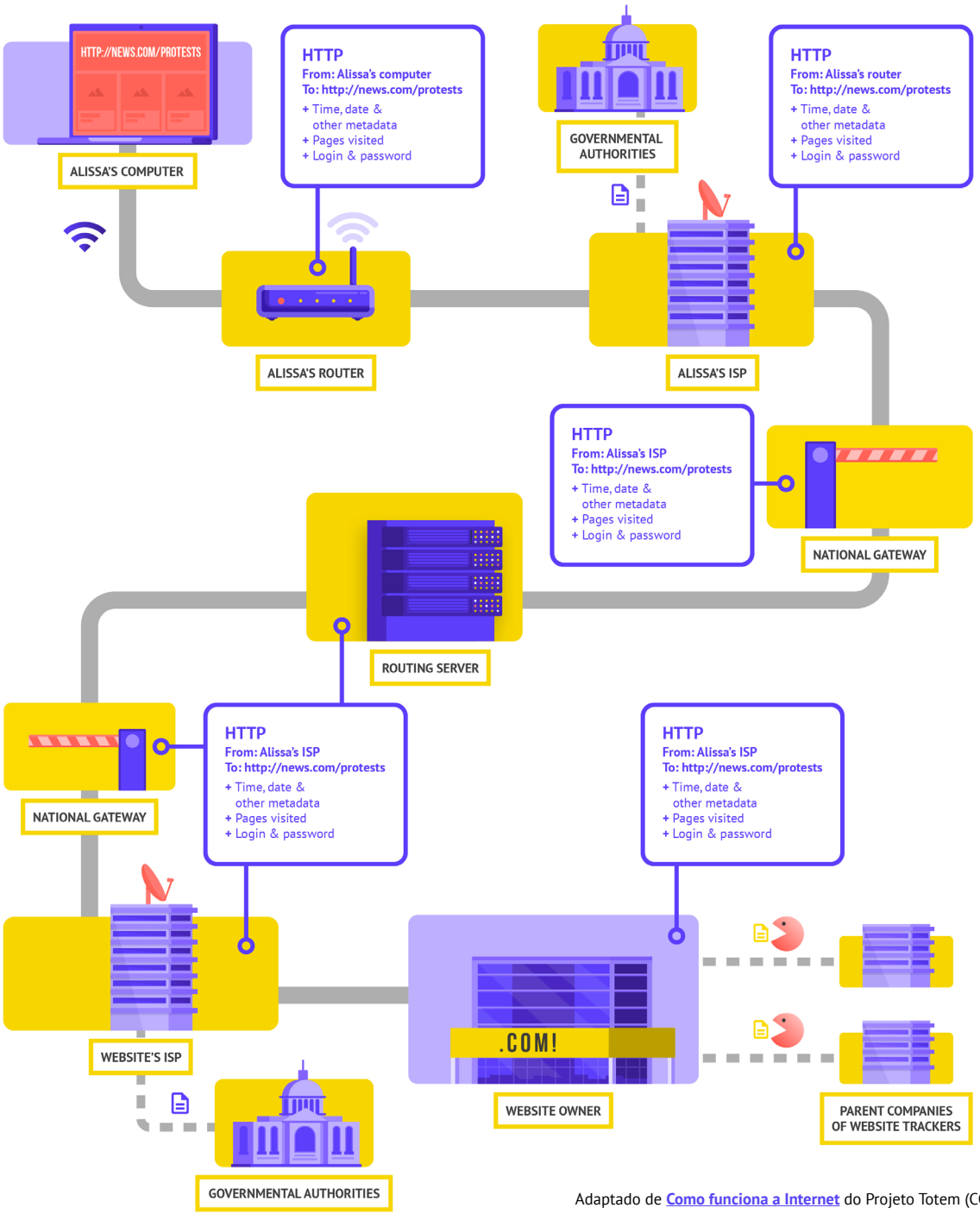
A vigilância, a censura e a sociedade civil

Os governos estão cada vez mais usando sua influência e autoridade sobre provedores de serviços de Internet e outras infraestruturas locais de Internet para impedir que indivíduos e grupos da sociedade civil acessem informações na Internet. Em alguns casos, essas interrupções na Internet visam derrubar as principais plataformas de comunicação e compartilhamento de informações, incluindo mídias sociais e sites de notícias. Por exemplo, em resposta aos protestos resultantes de um golpe militar, os militares de Mianmar instruíram as operadoras móveis a desligar temporariamente toda a rede de dados móveis do país. Isso ocorreu logo após o bloqueio mais direcionado ao Facebook, Twitter e Instagram. Além de bloquear o acesso à Internet e sites, governos e outros agentes de ameaças em todo o mundo estão usando tecnologia de vigilância cada vez mais acessível para monitorar a atividade dos cidadãos online. Por exemplo, de acordo com o relatório Libertade na Rede 2020 da Freedom House, o governo de Uganda fez uma parceria com a companhia de tecnologia chinesa Huawei para **vigilar figuras da oposição e ativistas civis** antes e depois de uma eleição presidencial contenciosa no país.

A crescente frequência desses ataques ao acesso e à liberdade de informação online destaca o quão essencial é para os grupos da sociedade civil entender os riscos de operar na Internet e desenvolver planos de como se conectar quando a conectividade for afetada.



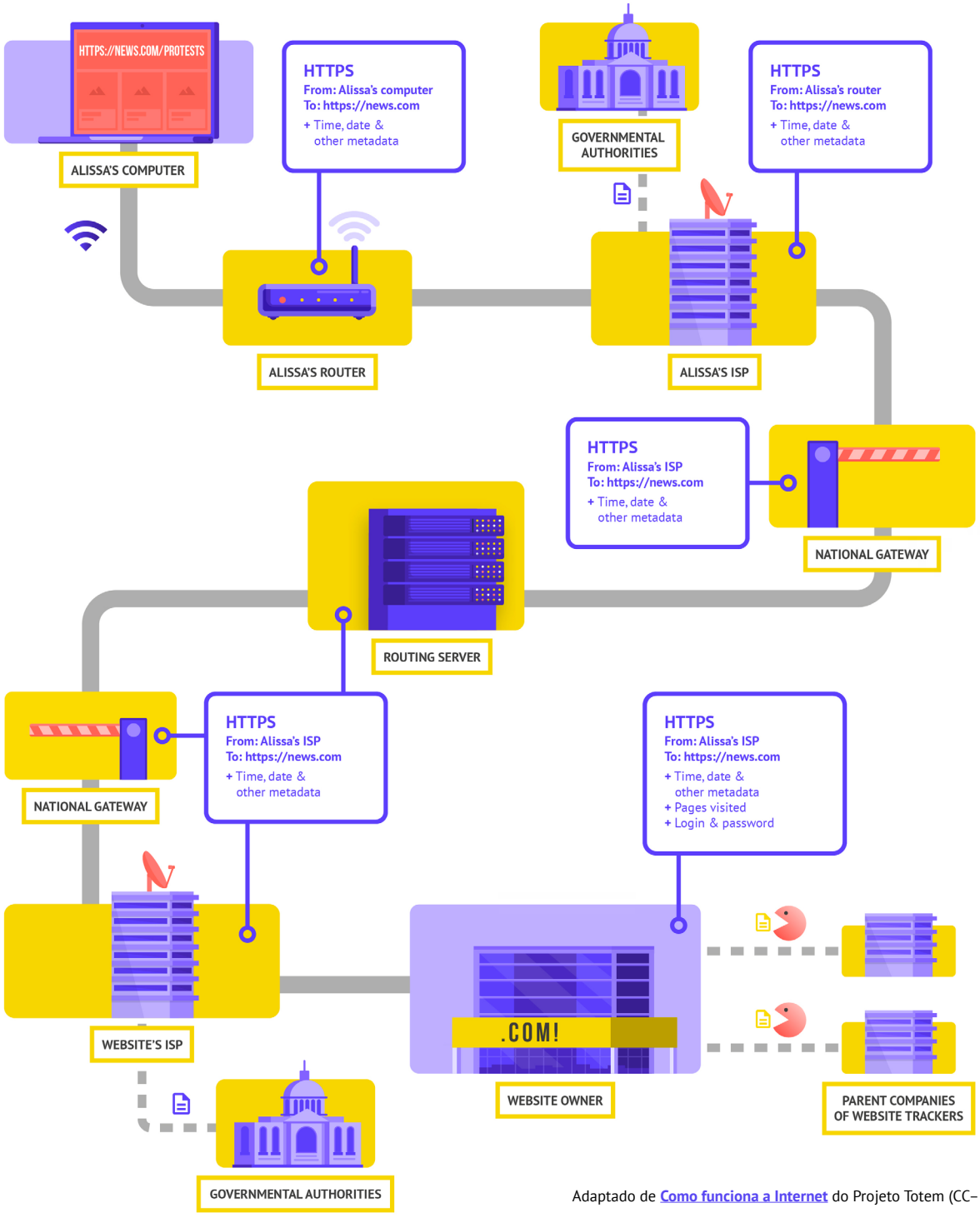
Vamos dar um exemplo do mundo real de como é a navegação sem criptografia:



Adaptado de [Como funciona a Internet]() do Projeto Totem (CC–BY–NC–SA)

Ao navegar sem criptografia, todos os seus dados ficam expostos. Como mostrado acima, um adversário pode ver onde você está, que você está acessando o news.com, olhando especificamente para a página de protestos em seu país e ver sua senha que você compartilha para fazer login no próprio site. Essas informações em mãos erradas não apenas expõem sua conta, mas também dão a possíveis adversários uma boa ideia do que você pode estar fazendo ou pensando.

O uso de HTTPS (“s” significa seguro) indica que a criptografia está em vigor. Isso oferece muito mais proteção. Vamos dar uma olhada em como é navegar com HTTPS (também conhecido como criptografia):



Adaptado de [Como funciona a Internet](#) do Projeto Totem (CC–BY–NC–SA)

Com o HTTPS em vigor, um adversário em potencial não pode mais ver sua senha ou outras informações confidenciais que você possa compartilhar com um site. No entanto, eles ainda podem ver quais domínios (por exemplo, news.com) você está visitando. E enquanto o HTTPS também criptografa informações sobre as páginas individuais de um site (por exemplo, website.com/protests) que você visita, adversários sofisticados ainda podem ver essas informações inspecionando seu tráfego na Internet. Com o HTTPS em vigor, um adversário pode saber que você está acessando news.com, mas não poderá ver sua senha e será mais difícil (mas não impossível) para ele ver que você está procurando informações sobre protestos (para usar este exemplo). Essa é uma diferença importante. Sempre verifique se o HTTPS está em vigor antes de navegar por um site ou inserir informações confidenciais. Você também pode usar a **extensão de navegador HTTPS Everywhere** para garantir que está usando HTTPS o tempo todo ou, se usar o Firefox, ative o **modo somente HTTPS** no navegador.
Se você receber um aviso do seu navegador de que um site pode ser inseguro, não o ignore. Algo está errado. Pode ser benigno – como o site tem um certificado de segurança expirado – ou o site pode ser falsificado ou falsificado maliciosamente. De qualquer forma, é importante prestar atenção ao aviso e não prosseguir para o site. O HTTPS é essencial e o DNS criptografado fornece alguma proteção extra contra espionagem e bloqueio de sites, mas se sua organização estiver preocupada com a vigilância altamente direcionada em relação às suas atividades online e enfrentar censura online sofisticada (como sites e aplicativos bloqueados), convém usar uma rede privada virtual (VPN) confiável.



Usar DNS criptografado

Se você quiser tornar mais difícil (mas não impossível) para um ISP saber os detalhes dos sites que você visita, você pode usar o DNS criptografado.

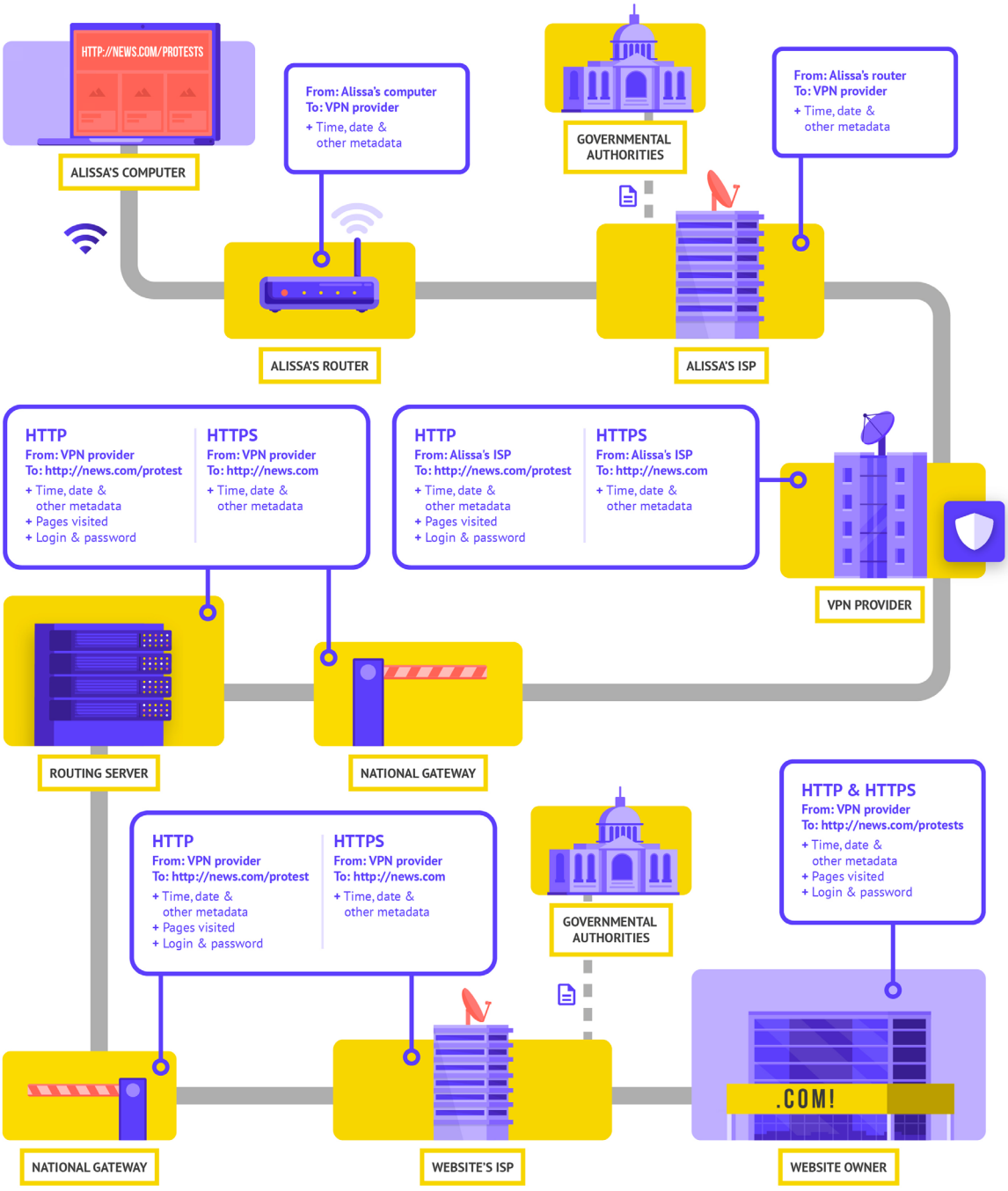
Se você está **se perguntando**, DNS e a sigla em inglês que significa Sistema de Nomes de Domínio. É essencialmente a lista telefônica da Internet, traduzindo nomes de domínio amigáveis para humanos (como ndi.org) para endereços de protocolo de Internet (IP) amigáveis para a web. Isso permite que as pessoas usem navegadores de Internet para pesquisar e carregar recursos da Internet e visitar sites com facilidade. Por padrão, porém, o DNS não é criptografado.

Para usar o DNS criptografado e adicionar um pouco de proteção ao seu tráfego de Internet ao mesmo tempo, uma opção fácil é baixar e ativar o **aplicativo 1.1.1.1 da Cloudflare** em seu computador e dispositivo móvel. Outras opções de DNS criptografado, incluindo o 8.8.8.8 do Google, estão disponíveis, mas exigem **mais etapas técnicas** para serem configuradas. Se você usa o navegador Firefox, o DNS criptografado agora está ativado por padrão. Os usuários dos navegadores Chrome ou Edge **podem ativar o DNS criptografado** por meio das configurações avançadas de segurança do navegador, ativando "usar DNS seguro" e selecionando "Com: Cloudflare (1.1.1.1)" ou o provedor de sua escolha.

O 1.1.1.1 da Cloudflare com WARP criptografa seu DNS e criptografa seus dados de navegação, com um serviço semelhante a uma VPN tradicional. Embora o WARP não proteja totalmente sua localização de todos os sites que você visita, é um recurso fácil de usar que pode ajudar a equipe da sua organização a aproveitar o DNS criptografado e a proteção adicional do seu ISP em situações em que uma VPN completa não é funcional ou necessária dado o contexto da ameaça. No 1.1.1.1 com configurações avançadas de DNS WARP, a equipe também pode ativar o 1.1.1.1 para Famílias para fornecer proteção adicional contra malware ao acessar a Internet.

O QUE É UMA VPN?

Uma VPN é essencialmente um túnel que protege contra a vigilância e o bloqueio de seu tráfego de Internet por hackers em sua rede, seu administrador de rede, seu ISP e qualquer pessoa com quem eles possam compartilhar dados. Ainda é essencial usar HTTPS e garantir que você confie na VPN que sua organização usa. Veja um exemplo de navegação com uma VPN:



Adaptado de [Como funciona a Internet](#) do Projeto Totem (CC–BY–NC–SA)

Para descrever VPNs com mais detalhes, esta seção faz referência ao Guia de autodefesa contra vigilância da EFF:

As VPNs tradicionais são projetadas para disfarçar seu endereço de IP de rede real e criar um túnel criptografado para o tráfego da Internet entre seu computador (ou telefone ou qualquer dispositivo "inteligente" em rede) e o servidor da VPN. Como o tráfego no túnel é criptografado e enviado para sua VPN, é muito mais difícil para terceiros, como ISPs ou hackers em Wi-Fi público, monitorar, modificar ou bloquear seu tráfego. Depois de passar pelo túnel de você para a VPN, seu tráfego deixa a VPN para seu destino final, mascarando seu endereço de IP original. Isso ajuda a disfarçar sua localização física para qualquer pessoa que veja o tráfego depois que ele sair da VPN. Isso oferece mais privacidade e segurança, mas usar uma VPN não o torna completamente anônimo online: seu tráfego ainda é visível para o operador da VPN. Seu ISP também saberá que você está usando uma VPN, o que pode aumentar seu perfil de risco.

Isso significa que **escolher um provedor de VPN confiável é essencial**. Em alguns lugares como o Irã, governos hostis criaram suas próprias VPNs para rastrear o que os cidadãos estão fazendo. Para encontrar a VPN certa para sua organização e sua equipe, você pode avaliar as VPNs com base em seu modelo de negócios e reputação, quais dados eles coletam ou não e, claro, a segurança da própria ferramenta.

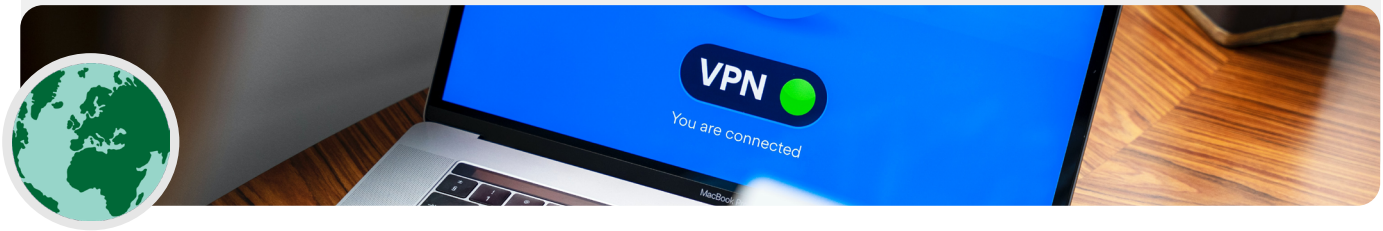
Por que você não deve usar apenas uma VPN gratuita? A resposta curta é que a maioria das VPNs gratuitas, incluindo aquelas que vêm pré-instaladas em alguns smartphones, vêm com um grande problema. Como todas as companhias e provedores de serviços, as VPNs precisam se sustentar de alguma forma. Se a VPN não vende seu serviço, como ela mantém seus negócios à tona? Solicita doações? Cobra por serviços premium? É apoiada por organizações de caridade ou financiadores? Infelizmente, muitas VPNs gratuitas ganham dinheiro coletando e vendendo seus dados.

Um provedor de VPN que não coleta dados em primeiro lugar é a melhor escolha. Se os dados não forem coletados, não poderão ser vendidos ou entregues a um governo, se solicitado. Ao analisar a política de privacidade de um provedor de VPN, veja se a VPN realmente coleta dados do usuário. Se não declarar explicitamente que os dados de conexão do usuário não estão sendo registrados, é provável que estejam. Mesmo que uma companhia afirme não registrar dados de conexão, isso nem sempre é garantia de bom comportamento.

Vale a pena fazer uma pesquisa sobre a companhia por trás da VPN. É endossada por profissionais de segurança independentes? A VPN tem artigos de notícias escritos sobre ela? Já foi pega enganando ou mentindo para seus clientes? Se a VPN foi estabelecida por pessoas conhecidas na comunidade de segurança da informação, é mais provável que seja confiável. Desconfie de uma VPN que oferece um serviço no qual ninguém quer apostar sua reputação ou que é administrado por uma companhia que ninguém conhece.

VPNs falsas no mundo real

No final de 2017, após uma onda de protestos no país, os iranianos começaram a descobrir uma versão "gratuita" (mas falsa) de uma VPN popular que era compartilhada por meio de mensagens de texto. A VPN gratuita, que na verdade não funcionava, prometia conceder acesso ao Telegram, que na época estava bloqueado localmente. Infelizmente, o aplicativo falso nada mais era do que um malware que permitia às autoridades rastrear o movimento e monitorar as comunicações de quem o baixou.

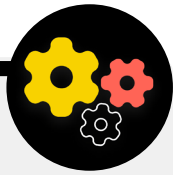


Então, qual VPN devemos usar?

Se usar uma VPN faz sentido para sua organização, algumas opções confiáveis incluem TunnelBear e ProtonVPN. Outra opção é configurar seu próprio servidor usando o Outline do Jigsaw, onde não há uma companhia gerenciando sua conta, mas em troca você precisa configurar seu próprio servidor. Se sua organização for um pouco maior, você pode considerar uma VPN empresarial que forneça recursos de gerenciamento de contas, como o plano de times do TunnelBear. Para certas organizações qualificadas na sociedade civil e no espaço de direitos humanos, o TunnelBear fornece créditos para uso gratuito de sua VPN (que geralmente custa cerca de US$ 3 por mês). Se você acredita que sua organização se qualifica e estiver interessada, entre em contato com cyberhandbook@ndi.org para obter mais informações.

Embora a maioria das VPNs modernas tenha melhorado em termos de desempenho e velocidade, vale a pena ter em mente que usar uma VPN pode diminuir a velocidade de navegação se você estiver em uma rede de largura de banda muito baixa, sofrer de alta latência ou atrasos de rede, ou sofrer interrupções intermitentes na Internet. Se você estiver em uma rede mais rápida, deve usar uma VPN por padrão o tempo todo.

Se você recomendar que a equipe use uma VPN, também é importante garantir que as pessoas mantenham a VPN ligada. Pode parecer óbvio, mas uma VPN instalada, mas não em execução, não oferece nenhuma proteção.



Anonimato através do Tor

Além das VPNs, você já deve ter ouvido falar do Tor como outra ferramenta para usar a Internet com mais segurança. É importante entender o que são ambos, por que você pode usar um ou outro e como ambos podem afetar sua organização.

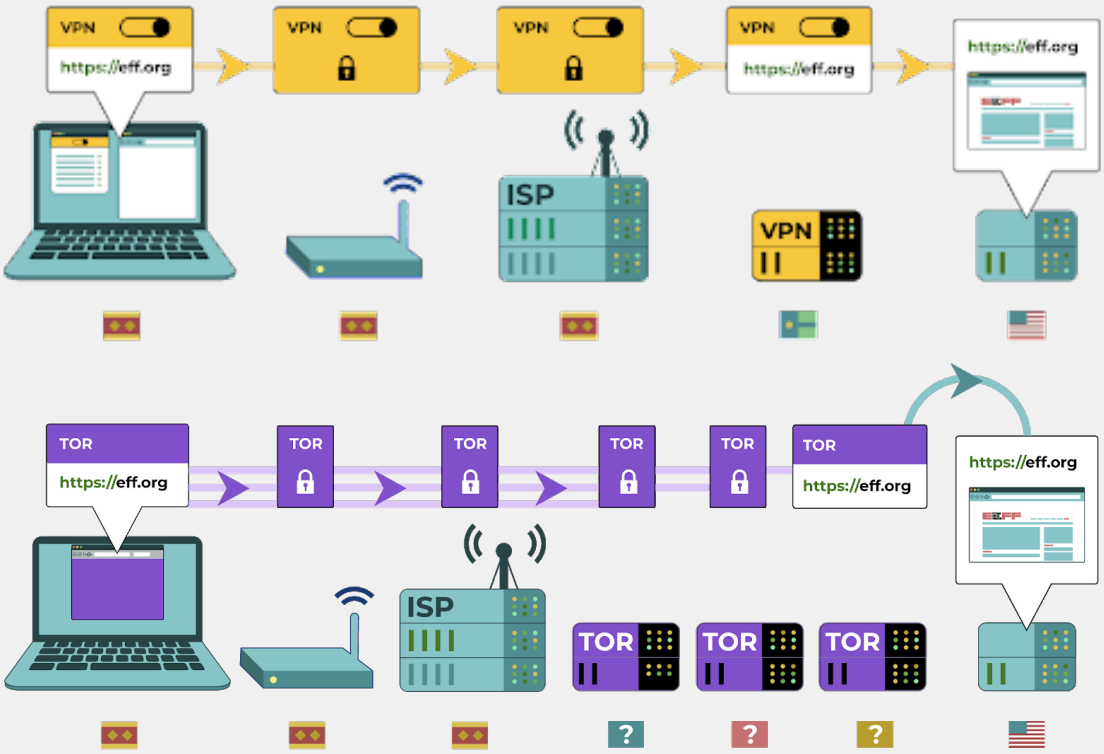
Tor é um protocolo para transmitir dados anonimamente pela Internet, encaminhando mensagens ou dados através de uma rede descentralizada. Você pode aprender mais sobre como o Tor funciona aqui, mas resumindo, ele encaminha seu tráfego por vários pontos ao longo do caminho até o destino, de modo que nenhum ponto tenha informações suficientes para expor quem você é e o que você está fazendo online de uma só vez.

O Tor é diferente de uma VPN em alguns aspectos. Mais fundamentalmente, difere porque não depende da confiança de nenhum ponto específico (como um provedor de VPN).

Este gráfico, desenvolvido pela EFF, mostra a diferença entre uma VPN tradicional e o Tor.

A maneira mais fácil de usar o Tor é através do navegador de Internet Tor. Ele funciona como qualquer navegador normal, exceto que encaminha seu tráfego pela rede Tor. Você pode baixar o navegador Tor em dispositivos Windows, Mac, Linux ou Android. Tenha em mente que ao usar o navegador Tor, você está apenas protegendo as informações que você acessa **enquanto está no navegador**. Ele não oferece proteção a outros aplicativos ou arquivos baixados que você pode abrir separadamente no seu dispositivo. Lembre-se também de que o Tor não criptografa seu tráfego, portanto – assim como ao usar uma VPN – ainda é essencial usar práticas recomendadas como HTTPS ao navegar.

Se você quiser estender as proteções de anonimato do Tor para todo o seu computador, usuários mais experientes em tecnologia podem instalar o Tor como uma conexão de Internet em todo o sistema ou considerar o uso do sistema operacional Tails, que encaminha todo o tráfego através do Tor por padrão. Os usuários do Android também podem usar o aplicativo Orbot para executar o Tor para todo o tráfego da Internet e aplicativos em seus dispositivos. Independentemente de como você usar o Tor, é importante saber que, ao usá-lo, seu provedor de serviços de Internet não pode ver quais sites você está visitando, mas eles *podem* ver que você está usando o próprio Tor. Assim como ao usar uma VPN, isso pode aumentar consideravelmente o perfil



de risco de sua organização, porque o Tor não é uma ferramenta muito comum e, portanto, se destaca para adversários que podem estar monitorando seu tráfego de Internet.

Então, sua organização deve usar o Tor? A resposta é: depende. Para a maioria das organizações em risco, uma VPN confiável que seja usada adequadamente por todos os funcionários em todos os momentos é mais fácil, mais conveniente e, na era de maior uso de VPN globalmente, é menos provável que levante bandeiras vermelhas. No entanto, se você não puder pagar uma VPN confiável ou operar em um ambiente onde as VPNs são rotineiramente bloqueadas, o Tor pode ser uma boa opção, se legal, para limitar o impacto da vigilância e evitar a censura online.

Há algum motivo para não usarmos uma VPN ou Tor?

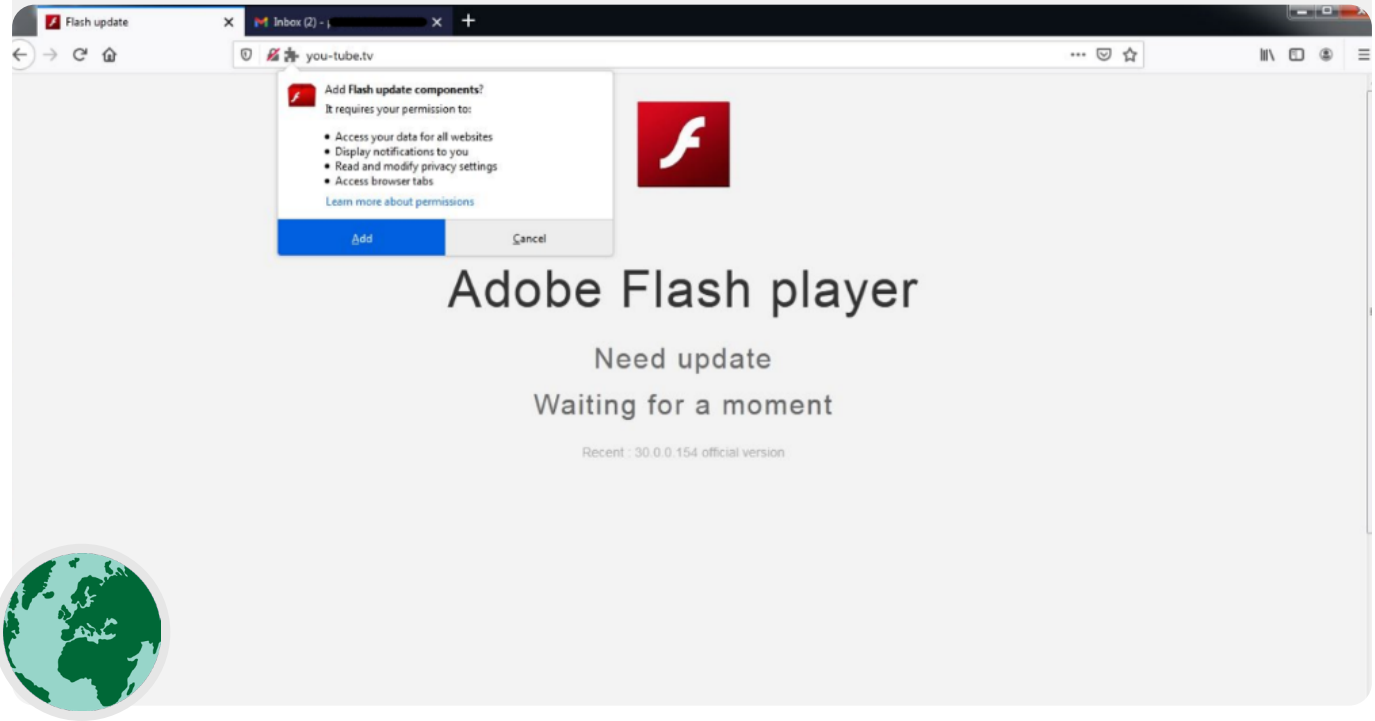
Além das preocupações com serviços de VPN não confiáveis, a maior coisa a considerar é se o uso de uma VPN ou Tor pode atrair atenção indesejada ou, em algumas jurisdições, ser contra a lei. Embora seu ISP não saiba quais sites você está visitando enquanto usa esses serviços, consegue identificar que você está conectado ao Tor ou a uma VPN. Se isso for ilegal onde sua organização opera ou pode causar mais atenção ou risco do que simplesmente navegar na web com HTTPS padrão e DNS criptografado, talvez uma VPN ou especialmente o Tor (que é muito menos usado e, portanto, uma "bandeira vermelha" maior) não seja a escolha certa para sua organização. No entanto, à medida que o uso de VPN se torna mais comum, esse é um fator menos distintivo. O padrão de ter uma VPN o tempo todo é a melhor escolha, se legal e possível.

QUAL NAVEGADOR DEVEMOS USAR?

Use um navegador respeitável, como Chrome, Firefox, Brave, Safari, Edge ou Tor. Tanto o Chrome quanto o Firefox são muito usados e fazem um ótimo trabalho com segurança. Algumas pessoas preferem o Firefox devido ao seu foco na privacidade. De qualquer forma, é importante reiniciá-los e reiniciar seu computador com relativa frequência para manter seu navegador atualizado. Se você estiver interessado em comparar os recursos do navegador, confira este recurso da Freedom of the Press Foundation. Independentemente do navegador, também é uma boa ideia usar uma extensão ou complemento como Privacy Badger, uBlock Origin ou Privacy Essentials da DuckDuckGo que interrompa os anunciantes e outros rastreadores de terceiros ao rastrearem onde você vai e quais sites você visita. E ao navegar na Internet, considere mudar suas pesquisas padrão do Google para DuckDuckGo, Startpage ou outro mecanismo de pesquisa que proteja a privacidade. Essa mudança também ajudará a limitar anunciantes e rastreadores de terceiros.

A segurança do navegador no mundo real

Ativistas da sociedade civil tibetana foram alvo no início de 2021 de uma extensão maliciosa de navegador projetada de forma inteligente para roubar seus e-mails e dados de navegação. A extensão intitulada "Componentes de atualização do Flash" foi apresentada aos usuários que visitaram sites vinculados a e-mails de phishing. Extensões de navegadores ou ataques complementares podem ser tão prejudiciais quanto o malware compartilhado diretamente por meio de downloads de phishing ou outro software.



Segurança de mídia social

Sua organização pode revelar muito – e às vezes mais do que pretende – postando e comentando nas mídias sociais.

Seja Facebook, Twitter, Instagram, YouTube ou sites de mídia social específicos da região, como VKontakte e Odnoklassniki, você deve sempre pensar com cuidado sobre o que publica e configurar adequadamente quaisquer configurações de privacidade que possam estar disponíveis. Isso vale não apenas para as páginas oficiais da sua organização, mas também, em alguns casos, para as contas pessoais dos funcionários e de seus familiares e amigos também.

A segurança de mídia social e a sociedade civil

Mesmo organizações de baixo risco podem ser atacadas e assediadas nas mídias sociais sem políticas de segurança adequadas. Neste exemplo de 2018, um abrigo de animais sem fins lucrativos perdeu milhares de dólares e alienou apoiadores depois que um administrador de conta não autorizado criou uma campanha de arrecadação de fundos falsa e contas falsas se passando por funcionários apareceram na plataforma. Se os hackers chegarem a esse ponto para ganhar alguns milhares de dólares em um abrigo de animais, você pode imaginar o dano que adversários sofisticados podem causar se obtiverem acesso às contas de sua organização ou se passarem por você online com sucesso. Além de hackear contas, grupos da sociedade civil e usuários individuais em muitos países também estão enfrentando repercussões por conteúdo postado nas mídias sociais. Em um exemplo na Zâmbia de 2020, a polícia prendeu um estudante de 15 anos por supostamente difamar o presidente em uma postagem no Facebook. A criança, que postou sob pseudônimo, foi identificada pelo número de telefone usado para registrar a conta e seu endereço de protocolo de Internet (IP).



DESENVOLVA UMA POLÍTICA ORGANIZACIONAL DE MÍDIA SOCIAL

Suponha que qualquer coisa postada nas mídias sociais possa se tornar de conhecimento público e elabore uma política organizacional de mídia social apropriada. Esta política deve responder a perguntas como: Quem tem acesso às suas contas de mídia social? Quem tem permissão para postar e quem precisa aprovar postagens? Quais informações devem ou não devem ser compartilhadas nas mídias sociais? Se você postar fotos, informações de localização ou outras informações de identificação sobre sua equipe, parceiros ou participantes de evento, você pediu a permissão deles e eles consideraram os riscos? Além de desenvolver sua política e deixá-la clara para a equipe, certifique-se de configurar adequadamente suas configurações de privacidade e segurança (geralmente chamadas de "segurança"). Algumas perguntas importantes a serem feitas ao decidir quais configurações de privacidade e segurança fazem mais sentido para suas contas pessoais e organizacionais incluem:

- Você deseja compartilhar suas postagens com o público ou apenas com um grupo específico de pessoas interna ou externamente?
- Alguém deveria poder comentar, responder ou interagir com suas mensagens ou publicações?
- As pessoas podem encontrar você ou sua organização usando seu endereço de e-mail ou número de telefone (pessoal ou profissional)?
- Você quer que sua localização seja compartilhada automaticamente quando você postar?
- Deseja bloquear ou silenciar contas hostis?
- Deseja bloquear palavras ou hashtags específicas?

Cada site de mídia social terá diferentes configurações de privacidade e segurança, mas esses conceitos gerais se aplicam universalmente. Ao considerar essas perguntas, aproveite os guias de privacidade úteis das principais plataformas: **Facebook**, **Twitter**, **Instagram**, e **YouTube**. Para o Facebook, em particular, tenha cuidado com suas escolhas de privacidade em relação aos grupos. Os grupos do Facebook são um local popular para engajamento, defesa e compartilhamento de informações, mas grupos irrestritos podem ser acessados por qualquer pessoa. Não é incomum que contas "falsas" se passem por pessoas reais em um esforço para se infiltrar em grupos ou páginas privadas de mídia social. Portanto, aceite os pedidos de "amizade" e "seguir" com cuidado. Lembre-se de que as contas de mídia social da sua organização são tão seguras quanto as contas que estão "vinculadas" a elas. Isso é especialmente importante para o Facebook, onde a página da sua organização pode ser gerenciada pela conta pessoal vinculada de alguém.

ASSÉDIO ONLINE

Infelizmente, muitas organizações enfrentam assédio online significativo, especialmente nas mídias sociais. Tal assédio é **muitas vezes direcionado com ainda mais intensidade a mulheres e populações marginalizadas**. A violência online contra as mulheres, em particular, pode criar um ambiente hostil que leva à autocensura ou à retirada do discurso político ou cívico. Conforme identificado no relatório **Tweets that Chill**, do time do NDI sobre Gênero, Mulheres e Democracia, quando os ataques contra mulheres politicamente ativas são canalizados online, o amplo alcance das mídias sociais pode ampliar o efeito do assédio e do abuso psicológico, minando a sensação de segurança pessoal das mulheres de maneiras não experimentadas pelos homens.

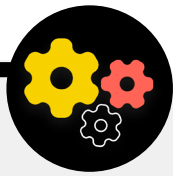
À medida que sua organização desenvolve sua política de mídia social, é importante estar ciente dessas dinâmicas. Inclua em seu plano de segurança suporte estruturado para funcionários que enfrentam mensagens negativas, insultos e ameaças nas mídias sociais, tanto como parte de seus trabalhos quanto em suas vidas pessoais. Desenvolva uma infraestrutura antiassédio em sua organização, incluindo pesquisas com seu time para entender como o assédio online os afeta e crie uma equipe de resposta rápida para ajudar o time a enfrentar situações desafiadoras. O **Manual de campo sobre assédio online** da PEN America, também fornece recomendações detalhadas sobre como você pode apoiar a equipe que enfrenta esse tipo de assédio. Você pode considerar, se sua equipe se sentir à vontade para fazer isso, **denunciar incidentes** de assédio ou contas problemáticas diretamente nas plataformas também.

Ao se envolver com funcionários que foram vítimas de assédio online (e também no mundo físico), é importante ser sensível. Conforme descrito pelo **Take Back the Tech** do Programa de direitos das mulheres, da Association for Progressive Communications, entenda que uma sobrevivente pode estar lidando com um trauma e reconheça que a violência (online ou offline) nunca é culpa da sobrevivente. Certifique-se de que tais questões possam ser levantadas e discutidas (se a equipe se sentir à vontade para fazê-lo) em um ambiente confidencial e seguro, com a opção de anonimato. E inclua no plano de segurança da sua organização uma lista de profissionais, organizações e agências locais de aplicação da lei aos quais você pode conectar a equipe para obter assistência jurídica, médica, de saúde mental e técnica, se necessário. Para ideias adicionais, confira o **Guia de segurança online**, da Feminist Frequency.

Mantenha seus sites online

Além de proteger sua capacidade de acessar a Internet com segurança, também é importante fazer o possível para garantir que outras pessoas possam acessar os sites ou propriedades da Web da sua organização.

Para páginas de mídia social, isso significa proteger essas contas com senhas fortes e exclusivas e autenticação de dois fatores. Para o seu site, isso significa protegê-lo contra hackers e ataques de negação de serviço. Ataques de negação de serviço distribuída (DDoS) são onde um grande grupo de computadores simultaneamente afoga seu servidor em tráfego malicioso. Se você é uma organização da sociedade civil ou outra organização sem fins lucrativos, provavelmente pode se qualificar para proteção gratuita contra DDoS – o que torna muito mais difícil para um adversário derrubar seu site. Algumas opções incluem o Projeto Galileo da Cloudfare, o Projeto Shield do Google e o serviço Deflect da eQualitie.



Como hospedar o site da sua organização com segurança

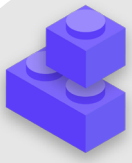
Os sites são hospedados em computadores – e esses são vulneráveis a hackers, assim como seus próprios dispositivos. Se possível, sua organização deve aproveitar os serviços de hospedagem existentes como Wordpress.com, Wix ou outros que gerenciam toda a segurança do site para você. Se você estiver lendo este manual, sua organização provavelmente também se qualifica para hospedagem segura gratuita de um site Wordpress pela eQualitie por meio do serviço de hospedagem eQPress. Essa é uma ótima opção para organizações cívicas com sites existentes do Wordpress ou se sua organização deseja criar um novo site. Se as necessidades do seu site forem mais complexas, ou se você precisar hospedar seu site por conta própria, certifique-se de se concentrar em manter seu sistema operacional e software de hospedagem na web atualizados, assim como faria com seu computador pessoal. Considere o uso de provedores de hospedagem em nuvem bem estabelecidos, como Amazon Web Services (AWS), Microsoft Azure ou eclips.is, da Greenhost, que oferecem opções de segurança aprimoradas para sites hospedados. Independentemente de quais ferramentas você usa para hospedar seu site, certifique-se de que todas as contas usadas para acessar a edição de conteúdo e as definições de configuração estejam protegidas com senhas fortes e autenticação de dois fatores.

Se sua organização tiver conhecimento técnico para hospedar seu próprio site, você deve considerar a escolha de um site chamado "site estático" ou site plano. Ao contrário de sites dinâmicos, esses tipos de sites reduzem a superfície de ataque de hackers e tornarão seu site mais resistente a ataques.

Proteja sua rede Wi-Fi

Todas essas etapas para proteger o tráfego da Web contra vigilância e censura são importantes, mas não substituem a segurança básica de rede no escritório e em casa.

Não se esqueça do básico, como usar uma senha forte (não a senha padrão) no(s) seu(s) roteador(es) Wi-Fi, garantindo que apenas usuários autorizados tenham acesso à sua rede alterando frequentemente a senha e habilitando o firewall integrado de seus roteadores sem fio. Considere criar uma rede de convidados em seu escritório também se você tiver visitantes que usam a Internet entrando e saindo do prédio.



Como estar seguro na Internet

- **Realize treinamentos regulares para a equipe sobre a importância de seguir as medidas básicas de segurança na web.**
- **Lembre a equipe de sempre navegar com HTTPS e DNS criptografado.**
- **Exija que a equipe reinicie regularmente seus navegadores para instalar atualizações.**
- **Incentive o uso de navegadores e extensões que protejam a privacidade.**
- **Se uma VPN for apropriada para o contexto da sua organização, escolha uma respeitável, treine a equipe sobre seu uso e garanta que ela seja usada de forma consistente.**
- **Desenvolva e distribua uma política organizacional clara sobre o uso de mídia social.**
- **Ative as configurações de privacidade e segurança em todas as contas de mídia social.**
- **Entenda os impactos do assédio online e esteja preparado para apoiar a equipe afetada.**
- **Desenvolva uma lista de profissionais, organizações e agências de aplicação da lei locais aos quais você pode conectar a equipe para obter assistência jurídica, de saúde mental e técnica em resposta a assédio online.**
- **Inscreva-se para proteção DDOS para seus sites.**
- **Use um provedor de hospedagem na web confiável.**
- **Use uma senha forte e uma rede de convidado para o Wi-Fi do seu escritório.**



Proteção da segurança física

É essencial manter seus dispositivos fisicamente seguros. Lembre-se de que a segurança física vai além de apenas dispositivos e deve incluir estratégias para proteger tudo o mais em seu mundo. Isso inclui documentos impressos; o escritório ou espaços de trabalho da sua organização; e, claro, você, sua equipe e voluntários.

A vigilância, a censura e a sociedade civil

Infelizmente, os ataques físicos a organizações da sociedade civil não são incomuns e muitas vezes têm implicações significativas para a segurança física e da informação. Uma tática comum adotada pelos adversários para suprimir a atividade das organizações da sociedade civil inclui invadir e fechar escritórios – tanto para intimidar funcionários quanto, em alguns casos, para roubar ou confiscar informações e equipamentos tecnológicos. Tais ameaças geralmente visam grupos minoritários e de direitos humanos e as organizações da sociedade civil que operam no espaço da democracia e governança. Por exemplo, os escritórios da LGBT+ Rights Ghana, uma organização civil que no início de 2021 abriu o primeiro centro comunitário do país para a comunidade LGBTQI+ local, foram ameaçados de serem incendiados e foram eventualmente invadidos e fechados pela polícia. Incidentes como este não afetam apenas as operações físicas de uma organização, mas também podem prejudicar a sensação de segurança da equipe.

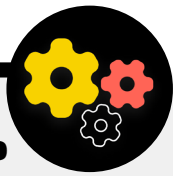


Proteção de ativos físicos

Um componente essencial da segurança da informação é a segurança física de seus dispositivos.

Além de mitigar o impacto de um dispositivo roubado usando telas de bloqueio e senhas, implementando criptografia completa de disco e ativando recursos de apagamento remoto, você também deve considerar como evitar que esses dispositivos sejam roubados em primeiro lugar. Para dificultar o roubo, certifique-se de instalar fechaduras fortes (e mudá-las sempre que a equipe mudar) no escritório ou em casa. Além disso, considere comprar um cofre para laptop ou um gabinete com chave para manter os dispositivos protegidos durante a noite. As câmeras de segurança tornaram-se muito mais baratas, com versões simples projetadas para uso doméstico disponíveis mais amplamente. Esses sistemas de câmeras ou sensores de movimento ao redor das instalações podem detectar e, com sorte, impedir arrombamentos físicos e roubos. Procure uma opção de **respeito à privacidade** disponível em seu país e certifique-se de selecionar câmeras fornecidas por companhias confiáveis que não tenham incentivo para entregar dados e informações a um possível adversário.

Se o risco de invasão ou assalto ao escritório for alto, mantenha os dados mais confidenciais da organização longe do escritório – sejam armazenados com segurança na nuvem (conforme discutido anteriormente) ou fisicamente movidos para um local menos direcionado. Se os dispositivos antigos ainda tiverem informações armazenadas neles, mas não estiverem mais em uso, considere limpá-los – **este guia** do Wirecutter é um ótimo recurso sobre como fazer isso para a maioria dos dispositivos modernos. Se não for possível limpar seus dispositivos, você também pode destruí-los fisicamente. A maneira mais fácil, se não mais ambientalmente sensível, de fazer isso é quebrar os dispositivos e seus discos rígidos com um martelo. Às vezes, as soluções mais antigas ainda funcionam melhor! Antes mesmo dessas etapas técnicas, reserve um momento para criar um inventário de todos os equipamentos da organização. Se você não tiver uma lista de todos os seus dispositivos, é mais difícil acompanhar o que pode estar faltando se um for roubado.



Como configurar seu próprio sistema de segurança de escritório

Se um sistema de segurança de escritório completo estiver fora do orçamento da sua organização e você estiver particularmente preocupado com a privacidade, experimente uma opção criativa como o **aplicativo Haven do Projeto Guardian**, para notificá-lo sobre uma possível invasão no escritório. O Haven é um aplicativo de smartphone que pode transformar qualquer telefone Android em um detector de movimento, som, vibração e luz. Você pode configurar o aplicativo em alguns dispositivos Android baratos em diferentes pontos do escritório para notificá-lo e registrar quaisquer convidados inesperados e intrusos indesejados. O aplicativo Haven também pode ser útil para instalar em um quarto de hotel ou apartamento se você estiver sob maior risco. Um sistema de segurança completo é melhor, mas se isso estiver fora de alcance e você quiser saber mais sobre como usar o aplicativo Haven, acesse **o site do projeto**.

O QUE FAZEMOS COM TODO ESSE PAPEL?

É provável que sua organização tenha muitas informações impressas em papel, escritas em cadernos ou rabiscadas em notas adesivas tipo Post-it. Parte disso pode ser muito sensível: impressões de orçamentos, listas de participantes, cartas confidenciais de doadores e notas de reuniões privadas. É fundamental pensar também na segurança dessas informações. Se você realmente precisar manter cópias impressas de informações confidenciais, certifique-se de que elas sejam armazenadas com segurança em um armário trancado ou em outro local seguro. Não mantenha nenhuma informação privada ou confidencial (incluindo senhas) em uma mesa ou escrita em um quadro branco. Se você acredita que sua organização corre alto risco de invasão ou assalto, mantenha informações altamente confidenciais em um local menos direcionado.
Na medida do possível, esforce-se para descartar informações impressas desnecessárias. Lembre-se: ninguém pode roubar o que você não possui. Defina uma política organizacional em relação à propriedade de notas impressas e certifique-se de coletar todas as notas impressas da equipe se eles decidirem sair ou forem dispensados da organização (como você coletaria um computador ou telefone fornecido pela) organização. Para se livrar de documentos confidenciais, compre uma trituradora de qualidade. Uma atividade divertida de fim de semana pode ser fazer uma pausa de 15 minutos com sua equipe para destruir quaisquer impressões ou anotações confidenciais da semana anterior.

A POLÍTICA DO ESCRITÓRIO

Embora para muitos as realidades do "escritório" tenham mudado significativamente desde o início da pandemia de COVID-19, ainda é importante que sua organização defina uma política clara em relação ao acesso ao escritório. Essa política deve abordar questões-chave, incluindo quem tem permissão para entrar no escritório (e quando), quem pode acessar quais recursos do escritório (como a rede Wi-Fi) e o que fazer com os convidados.

Uma pergunta simples, mas importante, a ser respondida é quem recebe uma chave do escritório. Somente funcionários de confiança devem ter as chaves e as fechaduras devem ser trocadas quando os funcionários saem ou de forma semi-regular. Durante o dia, todas as portas que forem deixadas destrancadas devem estar sempre à vista de alguém de confiança na organização. Considere também se a organização tem um relacionamento de confiança com o proprietário ou com a equipe de limpeza. Pense em quais informações ou dispositivos essas pessoas podem ter acesso e certifique-se de que estejam protegidos, principalmente se não houver uma relação de confiança. Seja lá quem tenha acesso, alguém de confiança deve sempre ser designado para trancar o escritório e garantir que os dispositivos estejam devidamente protegidos antes de sair no final do dia.

Os convidados são permitidos dentro do escritório? Em caso afirmativo, certifique-se de que eles não tenham acesso (ou pelo menos acesso autônomo) a dispositivos ou dados confidenciais em papel. Se for um requisito ou expectativa que os hóspedes tenham acesso à Internet quando visitam, você deve configurar uma rede de "convidados" para que esses convidados não tenham a capacidade de monitorar seu tráfego regular. Em geral, apenas pessoal confiável deve poder acessar a rede e os dispositivos de rede, como impressoras. Geralmente, também é uma boa ideia exigir o registro de convidados para que você tenha um registro de quem o visitou.

À medida que você desenvolve uma política de escritório, o objetivo deve ser permitir que apenas pessoas confiáveis acessem dispositivos, documentos, espaços e sistemas confidenciais.

EQUIPE DE APOIO E VOLUNTÁRIOS

As ameaças de segurança física à sua organização também podem afetar sua equipe. Semelhante ao assédio nas mídias sociais, essas ameaças à segurança física geralmente afetam desproporcionalmente as mulheres e as comunidades marginalizadas. Não se trata apenas de janelas quebradas e laptops roubados. Intimidação, ameaças ou casos de violência física ou sexual, abuso doméstico e medo de ataque podem ter um sério impacto negativo na vida dos funcionários. Para organizações que trabalham com ou apoiam mulheres politicamente ativas em particular, a ferramenta de planejamento de segurança **#Think10** do NDI é um recurso útil para fornecer àqueles que podem estar em maior risco pessoal como resultado de sua atividade.

O bem-estar dos funcionários é obviamente um recurso importante para eles como indivíduos, mas também é um elemento crucial para uma organização saudável e que funcione bem. Para isso, considere quais recursos adicionais você pode fornecer aos funcionários para mantê-los protegidos e, em caso de ataque físico ou digital, ajudá-los a se recuperar. Conforme mencionado anteriormente no manual, isso significa, no mínimo, desenvolver uma lista de recursos aos quais você pode conectar a equipe para assistência jurídica, médica, de saúde mental e técnica, se necessário. Mais uma vez, o **Manual de campo sobre assédio online** da PEN America inclui ideias sobre como as organizações podem apoiar a equipe durante e após as crises, e o **Manual de segurança holística** da Tactical Tech inclui conteúdo relevante sobre como as organizações costumam responder durante períodos de ameaça intensa.

SEGURANÇA DURANTE VIAGENS

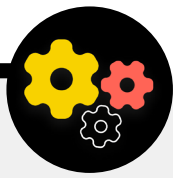
Viajar – seja para outro país ou uma cidade próxima – muitas vezes intensifica os riscos de segurança da informação física. Geralmente, é seguro presumir que você e seus dispositivos não têm direitos de privacidade ao cruzar fronteiras. Como tal, é uma boa ideia incluir uma política de viagem organizacional em seu plano de segurança que inclua lembretes sobre as principais práticas recomendadas de segurança. A política de viagens da sua organização deve incluir muitas das informações abordadas em outras seções do manual, incluindo o uso seguro da Internet e a manutenção de dispositivos e outras fontes de informações fisicamente seguras e sempre com você durante a viagem. Se possível, deixe suas informações confidenciais para trás e use um computador novo e limpo, acesse os arquivos de que você realmente precisa na nuvem e apague-os quando voltar para casa.

Além de se preparar para a viagem e minimizar os dados compartilhados quando você viaja, há algumas dicas operacionais essenciais que você deve considerar e incluir em sua política de viagens organizacional.

Considere usar laptops ou telefones específicos para viagens que tenham pouco ou nenhum dado confidencial armazenado neles. Se a maior parte do trabalho da sua organização for feita na nuvem, um Chromebook relativamente barato pode ser uma boa opção para esse aparelho. Faça uma redefinição de fábrica ou "limpe" esses dispositivos ao retornar, antes de se conectar a redes Wi-Fi comuns em casa ou no escritório.

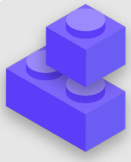
Prepare os funcionários sobre o que fazer se forem questionados pelas autoridades ou parados em uma passagem de fronteira. Considere como você pode limitar a quantidade de informações com as quais alguém viaja se isso for uma preocupação e crie protocolos de check-in para funcionários que viajam para regiões sensíveis. Forneça aos funcionários informações de contato e um plano de ação para o que eles devem fazer se algo der errado em sua viagem. Isso inclui informações sobre hospitais, clínicas ou farmácias locais, caso precisem de assistência médica durante a viagem.

Os funcionários também devem manter todos os dispositivos consigo durante a viagem. Por exemplo, mantenha seu laptop aos seus pés (não no compartimento superior ou na bagagem despachada) quando estiver em um ônibus, trem ou avião. Não presuma que um quarto de hotel – ou mesmo o cofre do hotel – é um "lugar seguro" para guardar dispositivos e itens confidenciais. Não confie nas portas de carregamento USB públicas. Portas de carregamento USB em aeroportos, estações e veículos estão se tornando uma visão cada vez mais comum e uma maneira muito conveniente de ligar dispositivos. No entanto, eles podem ser um vetor fácil para pegar vírus. Portanto, certifique-se de carregar os dispositivos da maneira tradicional por meio de um plugue na parede ou adquirir **bloqueadores de dados USB** para permitir que a equipe em viagem carregue seus dispositivos com segurança via USB.



Como reservar viagens com segurança para sua organização

Ao montar uma política de viagens, lembre-se de quais informações podem ser expostas ao organizar ou reservar uma viagem. Isso pode ser particularmente importante se você estiver organizando grandes eventos, treinamentos ou conferências para os quais está lidando com informações confidenciais de uma variedade de funcionários, parceiros ou participantes. Pense com cuidado sobre como você compartilhará e armazenará com segurança (se necessário) informações pessoais, como detalhes do passaporte, itinerários de viagem e registros médicos. O Livro de atividades do organizador, da Tactical Tech, tem uma ótima planilha para ajudar sua organização a refletir sobre as principais questões relacionadas à segurança de viagens, link aqui.



Como proteger sua segurança física

- **Lembre a equipe de manter os dispositivos fisicamente protegidos o tempo todo.**
- **Verifique e proteja todas as maneiras pelas quais as pessoas podem entrar em seu espaço – portas e janelas.**
- **Desenvolva uma política de acesso e convidado do escritório.**
- **Use travas fortes e alterne ou troque-as quando necessário.**
- **Considere instalar uma câmera ou outro sistema de segurança do escritório.**
- **Tenha e use um triturador de papel.**
  - Reserve um tempo da equipe dedicado a descartar documentos impressos que contenham informações confidenciais.
- **Desenvolva uma lista de profissionais, organizações e agências de aplicação da lei locais aos quais você pode conectar a equipe para obter assistência jurídica, médica e de saúde mental em resposta a ataques físicos ou ameaças.**
- **Desenvolva uma política de viagens organizacional.**
- **Garanta que a equipe saiba o que fazer em caso de emergência durante a viagem, incluindo preparar a equipe para o que fazer se parar em uma fronteira ou posto de controle.**
- **Antes de qualquer viagem local, nacional ou internacional, lembre a equipe de limitar as informações armazenadas nos dispositivos.**
- **Esteja atento aos dados adicionais que são criados e compartilhados ao organizar viagens ou eventos.**



O que fazer diante de imprevistos

Você sabe as coisas certas a se fazer. Você implementou as políticas e treinou todos na organização em todas as melhores práticas. Mesmo com todo esse trabalho duro, é muito provável que haja algum imprevisto.

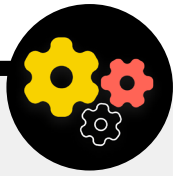
Simplesmente acontece. Quando acontecer, é essencial ter um plano de resposta a incidentes implementado. A resposta a incidentes é uma parte crucial e muitas vezes subestimada do plano de segurança de sua organização, porque pode ser a diferença entre um ataque que destrói a reputação de sua instituição ou um obstáculo desagradável no caminho. Lembre-se de que você só pode responder a um incidente se souber sobre ele. Ter uma forte cultura de segurança organizacional e incentivar a equipe a relatar problemas é muito importante. É por isso que é melhor recompensar o bom comportamento de segurança do que punir lapsos ou erros de segurança. Também é importante expressar empatia e verificar o bem-estar dos funcionários quando eles relatam um incidente. Você quer que a equipe denuncie imediatamente um link clicado em uma mensagem de phishing, um telefone roubado ou uma conta de mídia social invadida – não que ela hesite por medo de represália ou falta de apoio. Afinal, a resposta a incidentes, assim como as estratégias de mitigação mencionadas em outras seções do manual, é um esforço de toda a organização.

- Para que você deve se planejar? Em suma, tudo o que é um pouco provável de acontecer. Isso será diferente para cada organização, mas as perguntas comuns que um plano de resposta a incidentes ajuda a responder incluem:
- O que fazemos se nossas contas ou sites forem invadidos?
- O que fazemos se alguém clicar em um e-mail de phishing ou se um dispositivo estiver agindo de forma suspeita?
- O que fazemos se nossos e-mails ou documentos mais confidenciais forem roubados e vazados?
- O que fazemos se um de nossos funcionários for colocado em perigo físico ou for preso? Ou se eles estão lutando contra o estresse e a ansiedade devido a essas ameaças?
- O que fazemos se nosso escritório for danificado por um incêndio, inundação ou desastre natural?
- O que fazemos se o computador ou telefone de um funcionário for perdido ou roubado?

As respostas a essas e outras perguntas diferem de acordo com a organização, mas é importante pensar nelas em conjunto e articular claramente e compartilhar um plano para que todos em sua organização estejam preparados para agir imediatamente para limitar os danos.

Tomando emprestado do Manual de segurança holística da Tactical Tech, um bom ponto de partida para um plano de resposta a incidentes é definir um incidente ou uma emergência no contexto de sua organização. Decida o que é uma "emergência" – ou seja, o ponto em que devemos começar a implementar as ações e medidas de contingência planejadas. Isso é importante, porque às vezes não fica claro – se você imaginar um cenário como perder contato com um colega em uma missão de campo; quanto tempo você esperaria antes de declarar uma emergência? Não se quer pular muito cedo, mas esperar muito tempo pode, em algumas circunstâncias, ser desastroso. Também é importante pensar em todas as etapas de **operações**. Atribua a cada pessoa uma função clara da qual ela esteja ciente e com a qual tenha concordado com antecedência – isso reduzirá a desorganização e o pânico no caso de um incidente. No caso de cada ameaça, considere os diferentes papéis que você pode ter que assumir e os aspectos práticos envolvidos na resposta a uma emergência. Dentro dessa importante estratégia para emergências está a ativação de uma rede de apoio – uma ampla rede de aliados, que pode incluir amigos e familiares, comunidade, aliados locais, recursos governamentais e aliados nacionais ou internacionais, como ONGs e jornalistas. Como seus aliados podem apoiá-lo? Você deve contatá-los com antecedência para verificar se estarão dispostos a ajudá-lo em uma emergência e informá-los sobre o que você espera deles?

Ao responder a um incidente, **comunicações** eficazes tornam-se cada vez mais importantes. Decida qual é o meio mais seguro e eficaz de comunicação com cada ator em diferentes cenários e identifique um meio de backup. Esteja ciente de que, para emergências, pode ser útil ter diretrizes claras sobre o que (e o que não) comunicar, quando comunicar, quais canais usar e com quem você deve se comunicar. Considere também o impacto reputacional de um incidente em sua organização e esteja preparado para responder adequadamente. Certifique-se de que o líder da comunicação da organização (em algumas organizações pode ser apenas quem gerencia a página do Facebook ou a conta do Twitter) está ciente do incidente e pode observar as mídias sociais ou outras mídias quanto ao impacto potencial. Eles também devem estar preparados para responder a possíveis perguntas do público ou da mídia sobre um incidente, se relevante. Isso é especialmente importante para se antecipar a possíveis histórias negativas ou danos à reputação. Embora cada incidente e contexto sejam diferentes, comunicações honestas e transparentes geralmente ajudam a criar confiança após um incidente.



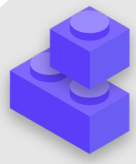
Criar um sistema de alerta e resposta antecipado

Considere estabelecer um sistema de alerta e resposta antecipado. Tal sistema parece refinado, mas é essencialmente apenas um documento centralizado (eletrônico ou não) a ser aberto em caso de emergência. No documento, você deve registrar todos os detalhes sobre os indicadores de segurança e incidentes ocorridos em uma linha do tempo, fornecer uma descrição clara das ações e sequência para a resposta planejada e indicar o que precisa ser alcançado para significar que o risco mais uma vez diminuiu. Também deve incluir ações a serem tomadas após um incidente, a fim de proteger os envolvidos de mais danos e ajudá-los a se recuperar física e emocionalmente. Um sistema de alerta e resposta antecipado pode fornecer documentação útil para compartilhamento com a aplicação da lei (se aplicável), análise subsequente do que aconteceu e orientação sobre como melhorar suas táticas de prevenção e respostas a ameaças no futuro.

Além desses conceitos importantes de resposta a incidentes, sua organização também deve se preparar para qualquer resposta **técnica** específica. Em alguns casos, uma resposta técnica pode ser gerenciada pela equipe interna de TI ou pelos administradores do sistema. Por exemplo, se uma conta de e-mail parece ter sido invadida, o administrador da sua conta deve estar preparado e capaz de encerrar ou desabilitar a conta afetada. Alguns incidentes técnicos, no entanto, podem exigir conhecimentos que você não possui em sua organização. Para situações como essas, é importante identificar uma lista confiável de especialistas técnicos externos que possam ajudá-lo na resposta a incidentes. Em alguns casos, você pode querer pré-negociar os termos com os provedores de serviços (como o host do seu site ou um consultor de TI) para garantir que eles estejam disponíveis (e não cobrariam mais) para tal resposta a incidentes técnicos.

Por último, mas certamente não menos importante, você deve considerar as etapas **legais**. É importante entender as proteções legais que você pode ter, bem como as obrigações ou consequências legais que sua organização pode enfrentar como resultado de uma violação de dados ou outro incidente de segurança. Um primeiro passo pode ser identificar um aconselhamento jurídico de confiança que entenda as leis e regulamentos específicos do seu país ou localidade. Reserve um tempo para analisar possíveis incidentes com um aconselhamento jurídico relevante, se necessário, e faça um plano para o que você faria em resposta. É uma boa ideia fazer um acordo com este advogado de confiança para representar você e seus interesses, se necessário, após um incidente. Como parte desta preparação legal, certifique-se de que compreende as obrigações legais de quaisquer fornecedores ou parceiros. Eles são obrigados a notificá-lo no caso de sua própria violação de dados? Que apoio (se houver) eles devem fornecer a você no caso de um incidente? Ao desenvolver contratos e acordos com fornecedores externos, tenha em mente a possibilidade de violação de dados ou outro incidente.

Embora não exista uma abordagem única para a resposta a incidentes, é essencial ter planos operacionais, de comunicação, técnicos e jurídicos claros. À medida que você prepara seu plano de resposta a incidentes, recomendamos fortemente que faça uso dos excelentes recursos existentes, projetados para ajudar organizações da sociedade civil a agirem diante de uma resposta a incidentes. Esses recursos incluem o Kit de primeiros socorros digitais desenvolvido pela RaReNet e CiviCER, o Manual de campo sobre assédio online da PEN America, o Manual da campanha de segurança cibernética do Belfer Center, além do Modelo do plano de comunicação de incidentes cibernéticos e da Linha direta de segurança digital da Access Now.



Resposta a incidentes

- **Desenvolva um plano organizacional de resposta a incidentes e coloque-o em prática.**
  - Faça um brainstorming de possíveis incidentes e prepare-se para sua resposta antes que aconteça.
- **Certifique-se de que todos na organização estejam cientes de como você se comunicará e quais medidas técnicas serão tomadas no caso de um incidente.**
- **Reserve um tempo para entender suas proteções e obrigações legais.**
- **Esteja preparado para fornecer à equipe organizacional o apoio emocional e social de que precisam após um incidente.**

Apêndice A: Recursos recomendados

- Manual de segurança holística da Tactical Tech; Creative Commons Attribution-ShareAlike 4.0, Licença Internacional
  - Capítulo 2.4 - Entender e catalogar nossas informações
  - Capítulo 1.5 - Comunicar sobre ameaças em equipes e organizações
  - Capítulo 3.4 - Segurança em grupos e organizações
- Security Education Companion da Electronic Frontier Foundation; Creative Commons Attribution 3.0, Licença nos EUA
  - Folheto de atividades de modelagem de ameaças
- Guia de prevenção de phishing e higiene de e-mails da Freedom of the Press Foundation; Creative Commons Attribution 4.0, Licença internacional
- Guia de sinais de bloqueio da Freedom of the Press Foundation; Creative Commons Attribution 4.0, Licença Internacional
- Guia de autodefesa contra vigilância (SSD) da Electronic Frontier Foundation; Creative Commons Attribution 3.0, Licença nos EUA
  - O que devo saber sobre criptografia
  - Comunicação com os outros
  - Escolhendo a VPN certa para você
- Guia de ferramentas de bate-papo e conferências seguras da Frontline Defenders
- Kit de detoxicação de dados da Tactical Tech
  - Deixe a pessoa certa entrar: Torne a suas senhas mais fortes
  - Reforce seus bloqueios de tela
- Guia de segurança sobre senhas durante as eleições do Center for Democracy and Technology; Creative Commons Attribution 4.0, Licença Internacional
- Guia de segurança sobre a autenticação de dois fatores durante as eleições do Center for Democracy and Technology; Creative Commons Attribution 4.0, Licença Internacional
- Autenticação de dois fatores para iniciantes de Martin Shelton; Creative Commons Attribution 4.0, Licença Internacional
- Security-in-a-Box da Tactical Tech e Frontline Defender; Creative Commons Attribution-ShareAlike 3.0, Licença não adaptada
  - Proteja seu dispositivo contra ataques de malware e phishing
  - Proteja suas informações contra ameaças físicas
- Newsletter Ouch! da SANS: Pare esse malware
- Acesso a dispositivos e dados quando a segurança pessoal está em risco da Apple
- Higiene cibernética para organizações com uma missão social da Global Cyber Alliance

Apêndice B:
Kit básico do plano de segurança

Use o kit básico a seguir para fazer anotações enquanto você e sua organização leem o manual e digerem o material, e reflita sobre as perguntas que o acompanham com seus colegas para ajudar a gerar uma discussão produtiva.

Certifique-se de também fazer referência aos principais "componentes básicos" em cada seção do manual para garantir que você esteja abordando os tópicos importantes à medida que cria seu plano de segurança. No final do manual, os componentes básicos, as respostas a essas perguntas para discussão e suas anotações devem formar a base de um plano de segurança bem-sucedido!



Desenvolvimento de uma cultura de segurança



Uma base forte: Como proteger contas e dispositivos



Comunicação e armazenamento de dados com segurança



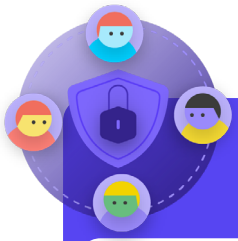
Como estar seguro na Internet



Proteção da segurança física



O que fazer diante de imprevistos



Desenvolvimento de uma cultura de segurança

QUESTÕES A CONSIDERAR:

- Quando você pode agendar uma conversa para revisar seu plano de segurança com toda a organização?
- Quais dias ou horários funcionam bem para a organização agendar conversas e treinamentos regulares sobre segurança?
- Que medidas a liderança pode tomar para modelar um bom comportamento de segurança e um compromisso com um plano de segurança? Como os outros na organização podem desempenhar um papel na segurança?

SUAS ANOTAÇÕES E IDEIAS:



Uma base forte: Como proteger contas e dispositivos

QUESTÕES A CONSIDERAR:

- Como você implementará medidas de segurança de conta – como um gerenciador de senhas e 2FA – em toda a organização? Que obstáculos você pode encontrar durante a implementação?
- Como sua organização garantirá que os dispositivos sejam mantidos seguros e atualizados? Como parte disso, a organização precisará de um plano para lidar com softwares ou computadores não licenciados?
- Quando é um bom momento para organizar treinamento para todos os funcionários sobre os perigos de phishing, malware e práticas recomendadas de segurança de dispositivos?

SUAS ANOTAÇÕES E IDEIAS:

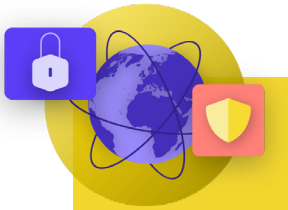


Comunicação e armazenamento de dados com segurança

QUESTÕES A CONSIDERAR:

- Como sua organização implementará mensagens criptografadas de ponta a ponta para comunicação segura? Que obstáculos você pode encontrar durante a implementação?
- Como sua organização aplicará uma solução segura de compartilhamento de arquivos interna e externamente? Que obstáculos você pode encontrar durante a implementação?
- Como sua organização implementará uma solução segura de armazenamento e backup de dados? Que obstáculos você pode encontrar durante a implementação?

SUAS ANOTAÇÕES E IDEIAS:



Como estar seguro na Internet

QUESTÕES A CONSIDERAR:

- Como sua organização implementará requisitos de navegação segura, como HTTPS, um navegador confiável e, se apropriado, uma VPN para a equipe?
- Quais serão os principais elementos da política de mídia social da sua organização? Como isso será aplicado?
- Como sua organização protegerá seus sites e propriedades da web?

SUAS ANOTAÇÕES E IDEIAS:

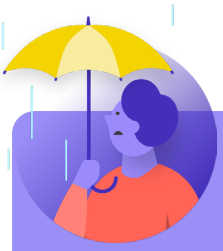


Proteção da segurança física

QUESTÕES A CONSIDERAR:

- Como a organização distribuirá e aplicará sua política de acesso e convidado do escritório?
- Quem é responsável por preparar os funcionários para os desafios de segurança física e digital que eles podem enfrentar durante as viagens a trabalho?
- Que medidas a equipe pode tomar para manter seus dispositivos seguros e protegidos tanto no escritório quanto em viagens?

SUAS ANOTAÇÕES E IDEIAS:



O que fazer diante de imprevistos

QUESTÕES A CONSIDERAR:

- Como a organização distribuirá e praticará sua política de resposta a incidentes?
- Existem recursos disponíveis para os funcionários que possam precisar de apoio emocional e social após um incidente? Se não, como a organização pode fornecer esses recursos no caso de um incidente?

SUAS ANOTAÇÕES E IDEIAS:

Apêndice C: Citações de imagens

Página 17: CNP Collection, “Security Protection Anti-Virus Software cms”, 2014, digital image, Alamy Stock Photo, https://www.alamy.com/security-protection-anti-virus-software-cms-image67114038.html?irclickid=2oWTxrXnOxyIRKXzgq3HowdNUkDzCPSFpyViRI0&utm_source=77643&utm_campaign=Shop%20Royalty%20Free%20at%20Alamy&utm_medium=impact&irgwc=1.

Página 24: Cottonbro, "Person Holding Black and Silver Key", 2020, digital image, Pexels, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.

Página 26: Blogtrepreneur, "Malware Infection", 2016, digital image, Flickr, https://www.flickr.com/photos/143601516@N03/.

Página 29: "Microsoft Loading Screen," digital image, Kompass, 23 de setembro de 2019, https://asset.kompas.com/crops/kYVdzylbrYB5llpuKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png.

Página 30: Mateuz Dach, "Turned-on iPhone and Displaying Icons," 2017, digital image, Pexels, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.

Página 33: Crete-Nishihata, "Process For a Phishing Email Sent in 2016," digital image, University of Toronto, January 30, 2017, https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/.

Página 38: Andrew Keymaster, "People Gathering on Street During Daytime Photo," 2020, digital image, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.

Página 39: Surveillance Self-Defense, "No Encryption in Transit," digital image, Electronic Frontier Foundation, 17 de janeiro de 2019. https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

Página 40: Surveillance Self-Defense, "4.Transport-layer-alternate," digital image, Electronic Frontier Foundation, 17 de janeiro de 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense, "6. End-to-end Alternate", digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.

Página 42: Surveillance Self-Defense, "9._endtoendencryptionmetadata," 2019, digital image, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

Página 50: Brett Sayles, "Server Racks on Data Center," 2020, digital image, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.

Página 55: PhotoMIX Company, 2016, "White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky," digital image, Pexels, https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/.

Página 60: Stefan Coders, "laptop-screen-vpn-cyber-security," 2020, digital image, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.

Página 62: Surveillance Self-Defense, "Using the Tor Browser," digital image, Electronic Frontier Foundation, 25 de abril de 2020. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png

Página 64: Nathan Dumlao, "White Samsung Android Smartphone on Brown Wooden Table," 2020, digital image, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.

Página 69: Matt Artz, "Two Broken 6-Pane On White Painted Wall Photo," digital image, Unsplash, 1 de outubro de 2017, https://unsplash.com/photos/vT684iB7Ejg.

NDI
NATIONAL
DEMOCRATIC
INSTITUTE

