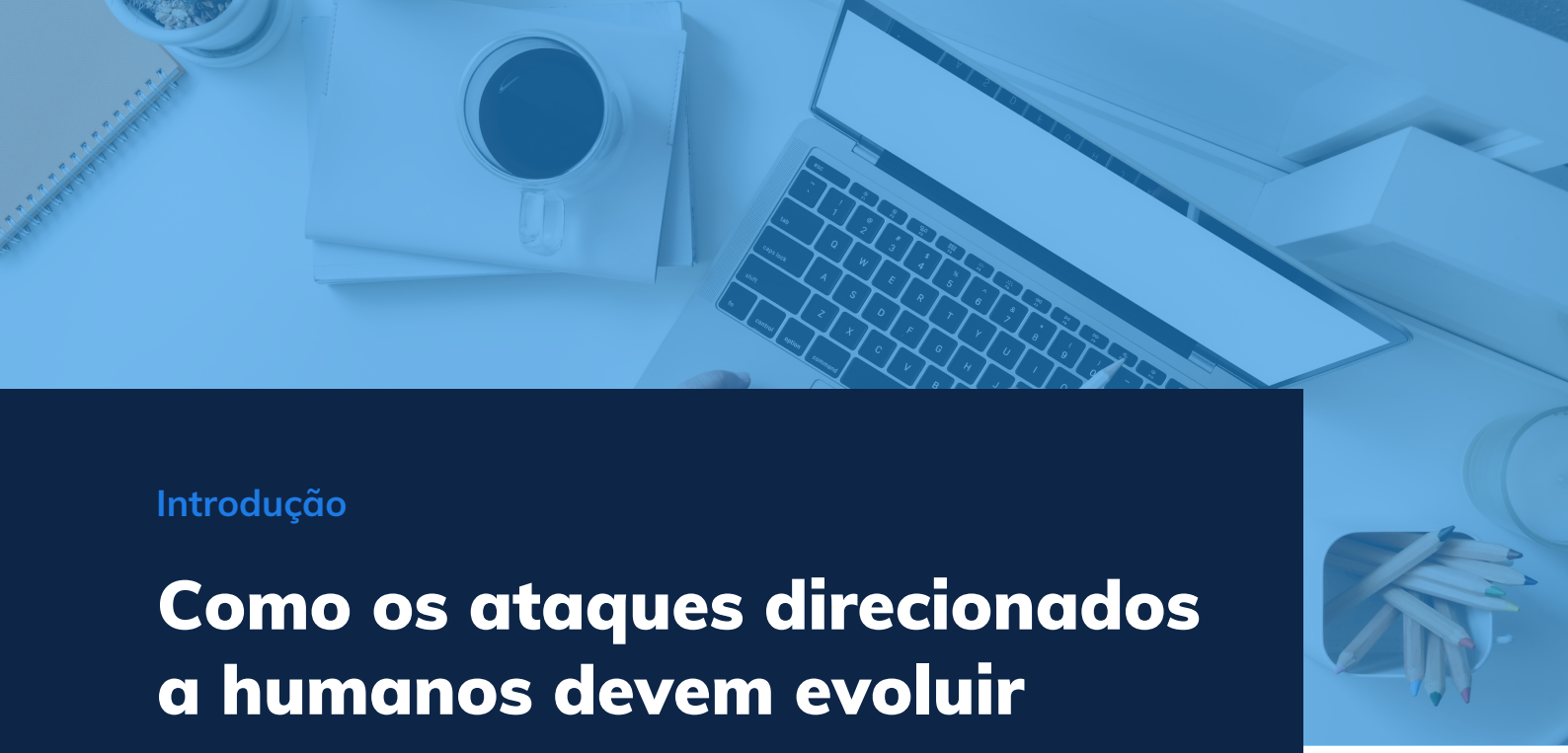
O completo guia para treinamento de conscientização de segurança

Conteúdo



Introdução

Como os ataques direcionados a humanos devem evoluir

A pandemia Covid-19 apresentou muitos desafios de segurança. As empresas em todo o mundo se adaptaram ao trabalho em casa e ao distanciamento social, ao mesmo tempo que lidam com novas ameaças representadas por cibercriminosos que exploram o medo e a curiosidade. Mesmo com as empresas lidando com esses desafios, as ameaças cibernéticas tradicionais têm prevalecido como sempre, criando um cenário de ameaças cada vez mais desafiador.

Entre as principais ameaças cibernéticas, o malware continua sendo um perigo significativo. O surto WannaCry de 2017, que custou às empresas em todo o mundo até US $ 4 bilhões, ainda está na memória recente, e outras novas cepas de malware são descobertas diariamente.

O phishing também ressurgiu nos últimos anos, com muitos novos golpes sendo inventados para tirar vantagem de empresas desavisadas. Apenas uma variação, o esquema de e-mail Fraude do CEO, custou apenas às empresas do Reino Unido £ 14,8 milhões em 2018.

A equipe que trabalha em casa está fora da supervisão direta das equipes de suporte de TI e muitas vezes se esforça para lidar com ameaças cibernéticas e proteger adequadamente as informações da empresa.

Deixar de atualizar software e sistemas operacionais, enviar dados por redes inseguras e aumentar a dependência de e-mail e mensagens online tornou os funcionários muito mais suscetíveis a ameaças que vão de malware a phishing.

Embora as soluções técnicas como filtros de spam e sistemas de gerenciamento de dispositivos móveis sejam importantes para proteger os usuários finais, com o número de ameaças e a variedade de sistemas e comunicações por meio dos quais a equipe trabalha, o único fator de risco unificador que deve ser abordado para melhorar fundamentalmente a segurança é o papel do erro humano.

Por que o erro humano é a ameaça de segurança nº 1 para sua empresa

Quase todas as violações cibernéticas bem-sucedidas compartilham uma variável em comum: erro humano. O erro humano pode se manifestar de várias maneiras: desde falha na instalação de atualizações de segurança de software a tempo até senhas fracas e fornecimento de informações confidenciais a e-mails de phishing.

Mesmo com o software moderno de anti-malware e detecção de ameaças ficando mais sofisticado, os criminosos cibernéticos sabem que a eficácia das medidas técnicas de segurança só vai até o ponto em que são utilizadas de forma adequada por humanos.

Se um cibercriminoso consegue adivinhar a senha de um portal de empresa online ou usa a engenharia social para fazer com que um funcionário faça um pagamento em uma conta bancária controlada pelo cibercriminoso, não há nada que as soluções técnicas possam fazer para impedir essa invasão.

Em 2014, a IBM conduziu um estudo sobre as violações cibernéticas que ocorreram entre milhares de seus clientes em mais de 130 países. Este estudo foi a investigação mais abrangente sobre as causas das violações cibernéticas realizadas até então, mas seus resultados foram corroborados por estudos semelhantes.

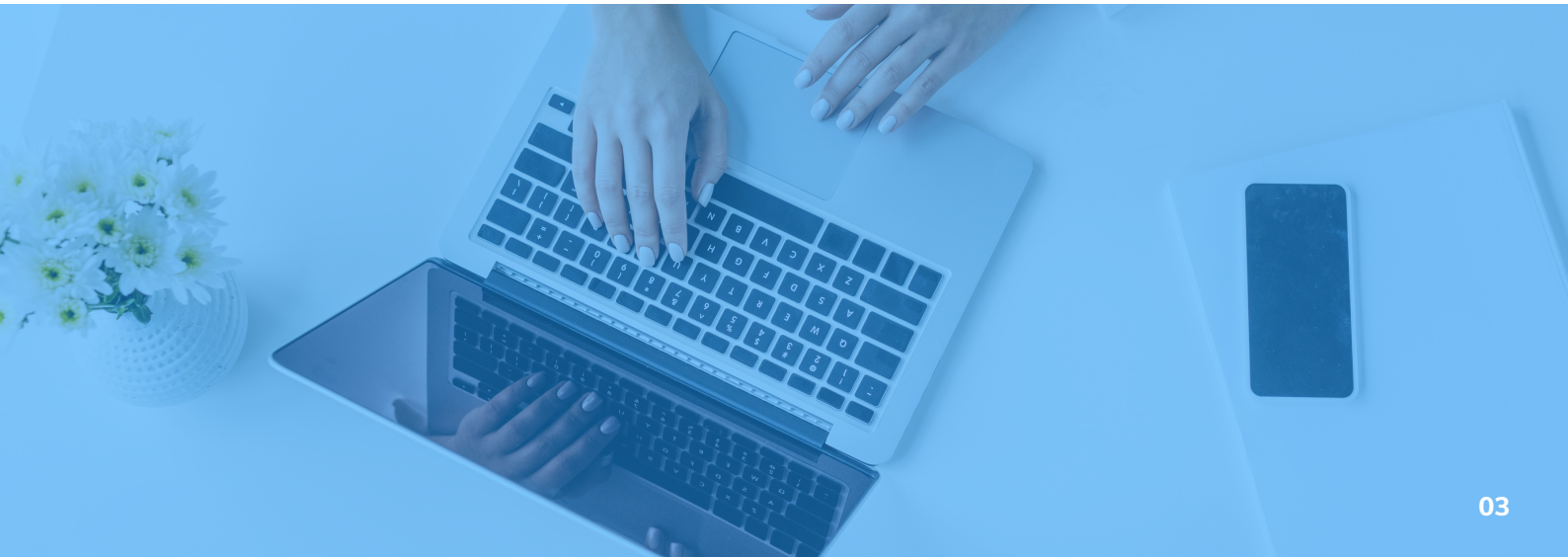
Uma das principais descobertas do estudo da IBM foi que o erro humano foi a principal causa contribuinte em 95% de todas as violações.

Em outras palavras, se o erro humano não tivesse sido um fator, as chances são de que 19 das 20 violações analisadas no estudo não teriam acontecido.

"Erro humano foi um fator que contribuiu para 95% de todas as violações"

Uma vez que o erro humano desempenha um papel tão vasto nas violações cibernéticas, abordá-lo é a chave para reduzir as chances de seu negócio ser direcionado com sucesso. Ele também permite que você proteja sua empresa de uma gama muito mais ampla de ameaças do que qualquer solução técnica poderia - e pode potencialmente capacitar sua força de trabalho para procurar ativamente e relatar novas ameaças que possam encontrar.

A mitigação do erro humano deve ser fundamental para as empresas modernas - e na próxima seção, veremos as melhores maneiras de fazer isso.



Quando ocorre o erro humano?

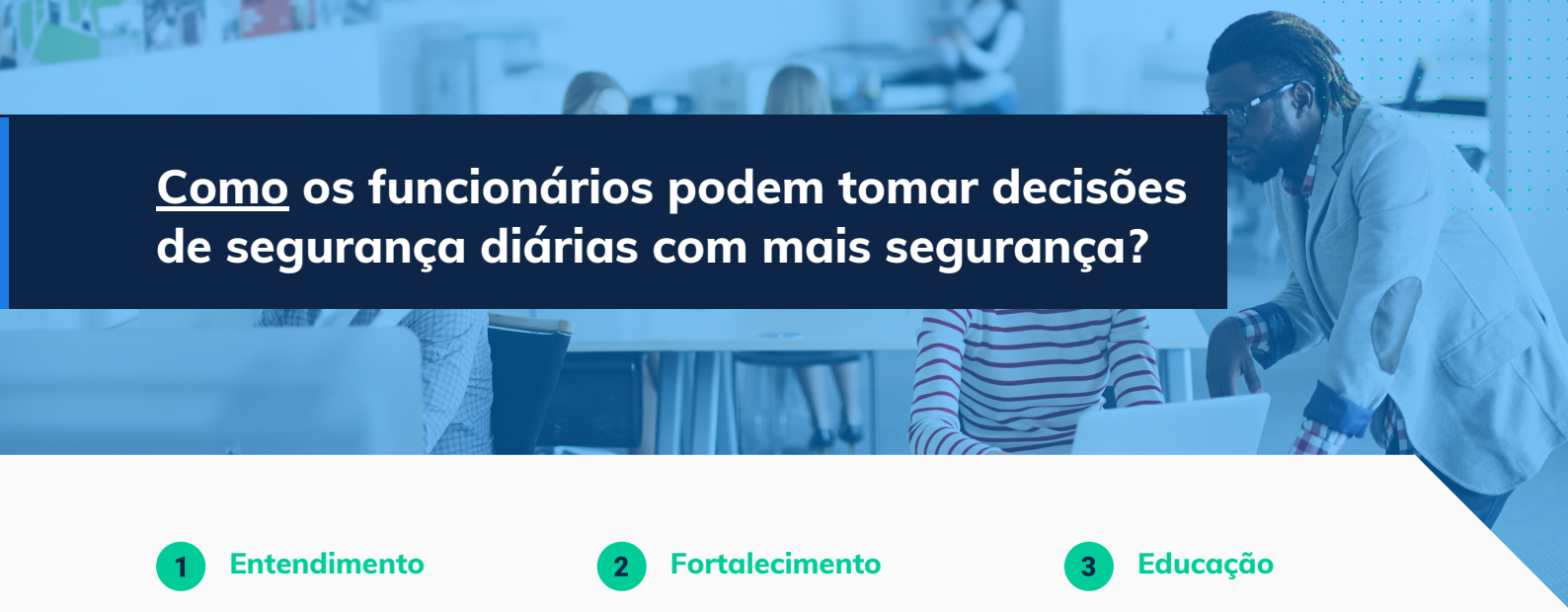
Dois fatores devem estar presentes para que o erro humano se manifeste: oportunidade e decisão. Oportunidade significa que existe uma situação em que um ser humano pode cometer um erro: por exemplo, permitir que os usuários finais lidem com as atualizações de software em vez de forçar as atualizações de segurança com o gerenciamento de patches. A decisão é a ação do indivíduo: neste caso, a falta de ação na instalação de atualizações de segurança quando disponíveis.

Um esforço de mitigação abrangente inclui a redução da oportunidade de erro e também a melhoria das decisões tomadas por parte dos usuários finais. Tomar medidas em ambas as áreas é essencial para garantir que o erro humano seja totalmente abordado.

No caso de patching, por exemplo, uma medida técnica como a introdução do gerenciamento de patch pode reduzir a oportunidade de erro humano ao mínimo na maioria dos casos - mas ainda é essencial levar em conta as situações em que as soluções técnicas têm um lapso temporário, ou se uma nova situação, como uma política BYOD, em que os usuários têm permissão para usar seus próprios dispositivos sem gerenciamento de patches, for introduzida.

Em outros casos, como e-mails de phishing, medidas técnicas como filtros de spam e software de detecção de violação têm um efeito muito limitado na redução da oportunidade de erro quando confrontado com um ataque direcionado. Nesses casos, a única maneira eficaz de mitigar o erro humano é ensinando os usuários finais a fazer julgamentos melhores.

"Dois fatores devem estar presentes para que o erro humano se manifeste: oportunidade e decisão"



Como os funcionários podem tomar decisões de segurança diárias com mais segurança?

1 Entendimento

O usuário deve reconhecer que está em uma situação em que a segurança está potencialmente em jogo. Sem reconhecer isso, o usuário pode nem mesmo perceber que está tomando uma decisão por meio de sua inação.

2 Fortalecimento

O usuário deve saber qual é o curso de ação correto. Isso não exige necessariamente que eles entendam completamente a ameaça, mas geralmente é tão simples quanto relatar a situação a uma pessoa do departamento de TI ou segurança que pode investigá-la.

3 Educação

O usuário deve saber por que a segurança é importante, para que entenda a importância de não ignorar os procedimentos de segurança e esteja ciente das implicações potenciais de uma violação.

4 Eliminando a prevenção da dor

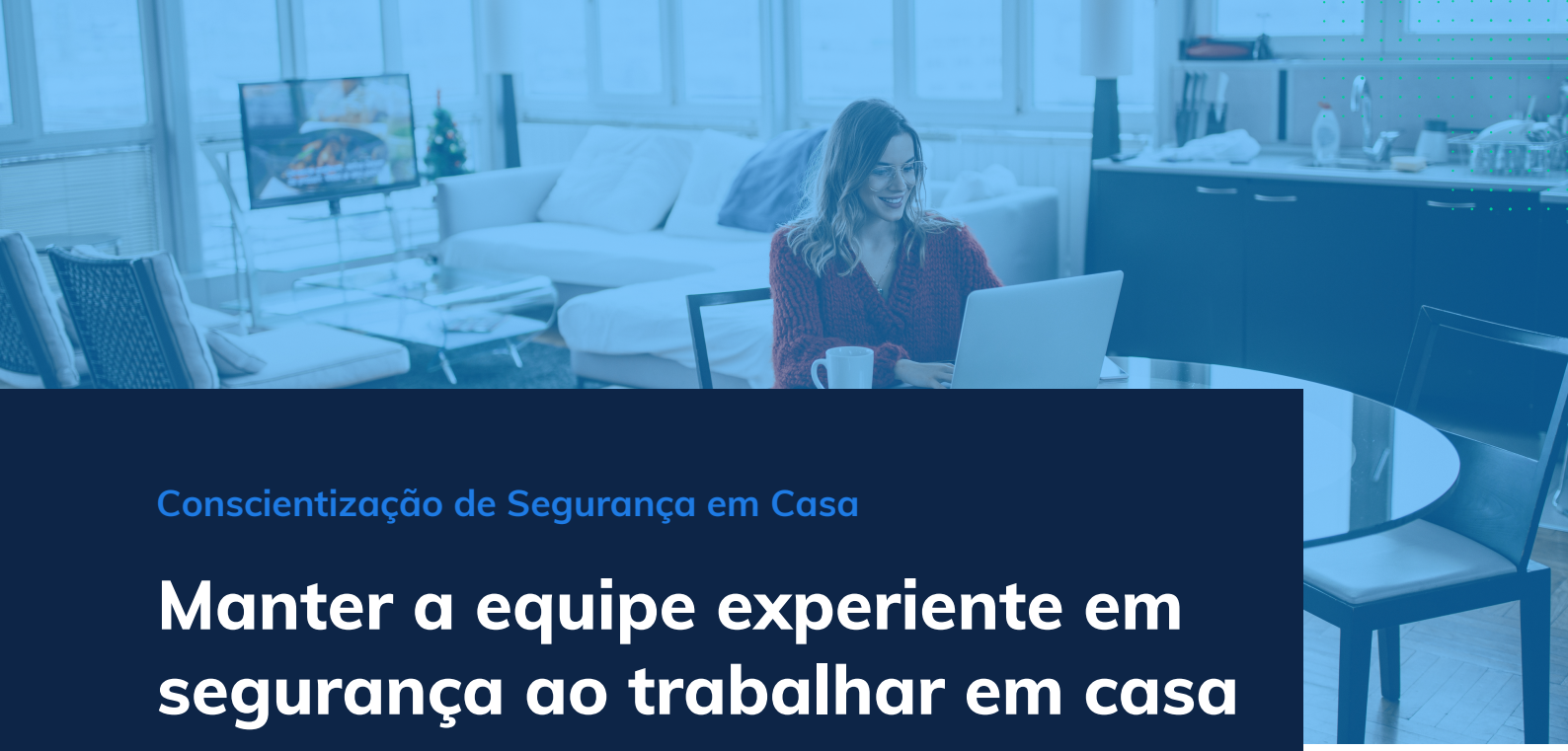
Issues such as weak password security and failure to patch software persist in organisations across the world, despite many computer users understanding why these issues are critical to security. The reason that action is not taken despite knowledge is due to what we refer to as pain avoidance. Having a unique and strong password requires more time to create, and more effort to remember, than a short, weak, or reused password.

Despite a user knowing better, this ‘pain’ caused by creating a strong password is often strong enough to make the user go against their best judgment. This is compounded by the fact that, despite many users taking the correct action under optimal circumstances, busy and urgent work situations, as well as stress, can make security measures feel even more ‘painful’ to users.

Os usuários finais precisam sentir que a dor causada por seguir as melhores práticas de segurança é menor do que a satisfação obtida por não seguir essas práticas. Medidas técnicas, como gerenciadores de senhas, são essenciais para isso, pois tornam mais fácil agir de maneira segura: se os funcionários não tiverem que criar ou lembrar suas próprias senhas, eles não terão motivo para não usar senhas seguras.

Simultaneamente, o limite para realizar a ação correta deve ser reduzido por meio da mudança cultural. Isso significa colocar a segurança na vanguarda da tomada de decisões e garantir que os usuários nunca sintam que estão "perdendo tempo" tomando as precauções de segurança adequadas.

O treinamento eficaz de conscientização sobre segurança aborda não um, mas todos os quatro desses fatores. Isso significa identificar situações em que dados ou sistemas podem ser comprometidos, compreender as melhores práticas, saber quais são as consequências potenciais das violações e, finalmente, ajudar a impulsionar uma mudança cultural para criar um ambiente onde as considerações de segurança são sempre levadas à tomada de decisões.



Conscientização de Segurança em Casa

Manter a equipe experiente em segurança ao trabalhar em casa

A resposta global à pandemia Covid-19 causou muitas mudanças nos locais de trabalho. A mudança que teve o impacto mais significativo na segurança foi a transformação de muitas empresas para que a maior parte ou toda a sua equipe mudasse para trabalhar em casa em um curto período de tempo, o que fez com que muitos usuários finais corressem um risco maior de sucumbindo às ameaças online.

Os funcionários que não estavam acostumados a trabalhar em casa antes da pandemia rapidamente descobriram alguns dos problemas que ela poderia causar: ter que cuidar de crianças e animais de estimação, lidar com a conectividade de Internet deficiente e suportar todos os outros distúrbios que podem acontecer em casa. Em meio a todas essas novas mudanças no ambiente de trabalho, a segurança muitas vezes caiu para o fim das listas de prioridades dos usuários.

Os usuários finais que trabalham em casa estão fora da supervisão do departamento de suporte de TI e podem ter dificuldades com questões simples relacionadas à tecnologia. Além disso, tarefas essenciais de segurança, como atualização de software e sistemas operacionais, atualização do firmware do roteador e proteção da rede, foram repentinamente colocadas nas mãos dos usuários finais.

Não é de se admirar que os cibercriminosos não tenham perdido um segundo explorando as circunstâncias da pandemia para inventar novas formas de golpes e crimes cibernéticos.

No meio de todas essas novas mudanças no ambiente de trabalho, a segurança muitas vezes caiu para o fim das listas de prioridades dos usuários.

Como abordar a segurança quando os usuários finais estão em casa

A equipe de suporte de TI não pode estar na casa de todos os usuários finais, por isso é essencial garantir que, além de ter o equipamento certo, os usuários finais estejam cientes de suas responsabilidades individuais em manter a segurança. Os usuários finais precisam saber que são responsáveis por garantir que acessem apenas as informações e redes da empresa em dispositivos e redes atualizados e seguros.

O treinamento de conscientização sobre segurança é fundamental para garantir que os usuários finais saibam como manter a segurança. É melhor dividir o treinamento em componentes pequenos e digeríveis, pois isso garante que os usuários não fiquem sobrecarregados. O treinamento também deve ocorrer regularmente - uma vez por mês, no mínimo - para garantir que o aprendizado fundamental seja retido e que os usuários não se esqueçam da segurança assim que o próximo projeto de trabalho surgir, que abale a lista de prioridades. Por último, é importante testar os usuários finais.

Deve ficar claro que isso não é para julgar ou penalizar usuários que lutam com seu treinamento, mas sim para identificar as principais lacunas de segurança na força de trabalho e resolvê-las antes que possam ser exploradas por criminosos cibernéticos.

"O treinamento de conscientização de segurança é fundamental para garantir que os usuários finais saibam como manter a segurança"

Moda antiga VS Treinamento Moderno

Como escolher o melhor formato para treinamento de conscientização de segurança

O treinamento de conscientização de segurança não é tudo o mesmo. A maneira como o treinamento é executado, estruturado e apresentado terá um grande efeito em sua eficácia, melhorando genuinamente os resultados de segurança em sua organização. Nesta seção, veremos qual é exatamente a melhor maneira de realizar o treinamento de conscientização de segurança para seus usuários finais.

O treinamento de conscientização sobre segurança costumava significar fazer os usuários finais assistirem a uma sessão anual que consistia em horas de palestras e apresentações de slides. A ideia era que os usuários se lembrassem de algo do que viram e ouviram - e, no pior dos casos, pelo menos a caixa para "educar os usuários" poderia ser marcada. Porém, como foi realmente melhorar os resultados de segurança? Não funcionou e todos odiaram.

Por que o treinamento anual 'tick-box' falha miseravelmente

Há uma série de razões pelas quais este tipo de treinamento anual baseado em palestras não é eficaz.

A primeira delas é que num treinamento em sessão anual simplesmente haverá informações demais de uma vez para qualquer funcionário digerir e lembrar.

Mesmo que os usuários recebam material didático para levar com eles ou sejam enviados lembretes ocasionais, é provável que a maior parte do material da sessão de treinamento entre por um ouvido e saia pelo outro - esquecido em poucos momentos.

Palestras e apresentações de slides simplesmente não são formatos envolventes para os usuários finais aprenderem. Eles não conseguem despertar o interesse dos funcionários da mesma forma que o vídeo e o conteúdo interativo, e muitas vezes são preenchidos com informações desnecessárias que não são relevantes para todos os usuários finais.

Slides cheios até a borda com pequenos textos certamente farão qualquer funcionário adormecer no meio da sessão.

A principal razão final pela qual o treinamento tradicional não é eficaz é que ele não usa o aprendizado por repetição. Se houver um ano entre as sessões de aprendizado, os usuários simplesmente não se lembrarão do que aprenderam - e a conscientização sobre os problemas de segurança em geral cairá nos dias e semanas após o treinamento. A segurança não pode ser uma coisa única, mas deve durar o ano todo para ser eficaz.

O treinamento de conscientização sobre segurança mudou cada vez mais para soluções de software como serviço online. O treinamento baseado em nuvem oferece alguns benefícios imediatos sobre os métodos tradicionais, mas não é necessariamente a resposta definitiva para a conscientização de segurança, a menos que entregue em certas áreas que são essenciais para melhorar genuinamente os resultados de segurança.

Como tornar o treinamento moderno realmente eficaz

Dividindo o material

Há uma quantidade limitada de informações que uma pessoa pode absorver por vez. Para não sobrecarregar os usuários finais, o treinamento deve ser dividido em segmentos, cada um com sua própria mensagem clara e simples, que é apresentada de forma fácil de digerir.

Aprendizado contínuo

Dividir o material de aprendizagem também permite que o aprendizado seja facilmente contínuo, em vez de uma única vez, e permite que os cursos sejam enviados regularmente ao longo do ano - ajudando a manter a consciência de segurança de forma consistente na mente dos usuários finais, bem como melhorando o aprendizado retenção.

Material relevante

Quando um usuário final recebe informações que considera irrelevantes para ele, rapidamente começa a perder o interesse e a prestar menos atenção. O material de aprendizagem precisa não apenas evitar jargões e termos técnicos, mas ser feito com situações da vida real em mente que o usuário final possa encontrar.

Incorpore a segurança à sua cultura

O treinamento deve ser parte de uma cultura empresarial onde a segurança é sempre levada em consideração de que ele precisa e os usuários são incentivados a levantar questões e fazer perguntas.

Conselho prático

É essencial que os funcionários saiam do treinamento com etapas reais em mente que podem ser colocadas em prática imediatamente em suas atividades diárias de trabalho. Dar aos funcionários a chance de colocar seu treinamento em teste imediatamente também ajuda a construir memória - e pode ser obtido usando ferramentas como simulação de phishing.

Vídeo e conteúdo interativo

Vídeo e conteúdo interativo são ótimos para envolver usuários que podem preferir um tipo diferente de experiência de aprendizado. Muitas pessoas aprendem fazendo, respondendo a perguntas ou de outra forma participando.

Medindo o impacto

É essencial que, após as sessões de treinamento, os usuários sejam testados sobre o que aprenderam. Isso ajuda você a saber que os usuários estão indo embora depois de aprender algo - mas também ajuda o processo de aprendizagem dos usuários, pois eles recolhem as informações que acabaram de aprender de sua própria memória.

Construindo uma cultura de segurança

Como incorporar a segurança à cultura cotidiana da equipe

O treinamento de conscientização sobre segurança não será eficaz para melhorar os resultados de segurança se não for acompanhado por uma mudança cultural. O treinamento abrangente ensinará os usuários finais a reconhecer as situações em que a segurança está em risco e como lidar com elas de forma adequada - mas esse conhecimento não será colocado em prática a menos que o usuário sinta que a segurança é valorizada em sua cultura.

Com o crescente número de ameaças presentes, bem como a crescente complexidade dos serviços de negócios e acesso a dados e sistemas de dispositivos móveis, é impossível saber onde a próxima ameaça ou vazamento acidental para sua empresa pode aparecer.

É por isso que a segurança não deve ser sobre garantir que seus usuários finais escolham senhas fortes ou seguir outras etapas específicas - mas sim sobre capacitá-los para serem tutores ativos de sua empresa, seus sistemas, dispositivos e dados.

"O treinamento abrangente vai ensinar os usuários finais como reconhecer situações em que a segurança está em risco e como lidar com elas de forma adequada - mas esse conhecimento não será colocado em prática a menos que o usuário sinta que a segurança é valorizada em sua cultura."

Como construir uma cultura experiente em segurança

Obter suporte de nível C

A mudança cultural e os valores da empresa têm que vir de cima. A alta administração tem um papel importante a desempenhar ao enfatizar o papel da segurança nos negócios - mas é essencial que eles desenvolvam, em vez de ditar, a nova cultura.

Isso significa encorajar os funcionários a assumir um papel ativo, pedindo-lhes que levantem questões relacionadas às suas próprias funções e levando-os a fazer perguntas e se envolver com as questões de segurança. Dessa forma, os usuários sentem que estão envolvidos no processo de segurança e começam a pensar ativamente sobre as considerações de segurança em suas próprias funções.

Acesso com menos privilégios

Embora o princípio do menor privilégio seja frequentemente visto como uma medida técnica - limitando cada usuário apenas aos privilégios que eles exigem para suas funções específicas - ele também deve ser incorporado diretamente na cultura corporativa.

Isso significa encorajar os usuários a relatar ativamente quando tiverem acesso a mais dados ou sistemas do que precisam - ajudando a limitar as possibilidades de violações.

Segurança física

Em termos de medidas físicas, itens como pôsteres podem ser úteis na construção de uma cultura de segurança e também contêm lembretes úteis sobre tópicos como a força da senha.

É importante lembrar, porém, que apenas colar um pôster na parede não vai resultar em nada por si só, mas deve ser usado como ponto de partida para a discussão ou servir como complemento ao material de treinamento com o qual os usuários já estão envolvidos.

Tópicos de treinamento essenciais

Quais são os tópicos essenciais de treinamento?

Embora cada organização e cada função de trabalho tenham requisitos diferentes, existem algumas áreas essenciais que valem a pena garantir que cada usuário final esteja ciente.

Os 12 principais tópicos de treinamento:

1. **Técnicas de Phishing**
2. **Engenharia social**
3. **Segurança em casa**
4. **Uso seguro de Internet e e-mail**
5. **Trabalhando Remotamente**
6. **Segurança de dispositivo móvel**
7. **Senha e autenticação**
8. **Segurança na nuvem**
9. **Wi-Fi público**
10. **Segurança física**
11. **Midia removivel**
12. **Uso seguro de mídia social**

1. Técnicas de Phishing

Phishing remains a huge threat. One of the reasons why phishing is so popular among cyber criminals is that it can be easily customised to make use of any event or circumstance - such as the Covid-19 pandemic - to target users with new scams. Template-based scams offering information to victims have become more popular than ever - while spear-phishing attacks that target individual users and businesses remain the most dangerous kind.

End users are most susceptible to phishing emails that create a sense of urgency or offer something valuable to the user. It's essential to train end users to double-check that they can trust who an email is from before clicking links or giving up information. While it's impossible for users to catch every phishing email, security awareness combined with spam filters ensure that the potential reach of phishing emails is limited to the minimum.

2. Engenharia social

Phishing é apenas um dos muitos tipos de ataques de engenharia social. Ataques de engenharia social físicos e por telefone também são usados por criminosos para obter acesso a instalações seguras e dados confidenciais.

É essencial que os funcionários sejam educados sobre os diferentes tipos de ataques de engenharia social - desde aqueles por telefone até ameaças pessoais - e entendam como lidar adequadamente com qualquer infrator em potencial.

3. Segurança em casa

Trabalhar em casa foi promovido para a vanguarda da segurança do usuário final em 2020, à medida que empresas em todo o mundo incentivavam seus funcionários a mudar para o trabalho remoto. A velocidade dessa transferência fez com que muitos usuários ficassem mal equipados com ferramentas e conhecimentos para garantir que pudessem realizar seu trabalho com segurança.

É essencial treinar todos os funcionários que trabalham em casa como eles podem garantir que os dados e a rede da empresa não sejam comprometidos por meio de acesso remoto. Atualizar software, proteger redes Wi-Fi e usar ferramentas de segurança como VPNs para garantir acesso seguro se tornaram uma parte essencial do treinamento do usuário final.

4. Uso seguro de Internet e e-mail

É raro o funcionário que não usa a internet ou e-mail no trabalho. Embora a pandemia tenha tornado as empresas mais dependentes da Internet do que nunca, o uso da Internet também acarreta riscos de segurança. Os usuários podem inadvertidamente instalar malware, vazar dados, fornecer credenciais para e-mails de phishing ou cair em qualquer um dos muitos outros ataques que os criminosos cibernéticos os têm como alvo.

É essencial treinar os usuários para usar a Internet e o e-mail com segurança. A maior parte disso se resume à conscientização: saber que e-mails podem causar violações de dados se enviados sem cuidado e que sites maliciosos podem conter malware.

Também deve haver conselhos práticos no treinamento, como informar os usuários sobre a diferença entre os campos cc e bcc e o que significa o símbolo de criptografia HTTPS em sites.

5. Trabalhando Remotamente

O trabalho remoto será mais popular do que nunca. Embora a pandemia tenha dado um impulso inicial ao trabalho doméstico em muitas empresas, é provável que continue além da pandemia. Os funcionários começaram a se acostumar a trabalhar em casa e as empresas estão percebendo seus benefícios.

Trabalhar remotamente também traz riscos. Laptops, telefones celulares, tablets e outros dispositivos podem representar uma séria ameaça à segurança se forem perdidos ou roubados. Se os funcionários armazenam ou acessam dados da empresa a partir de seus dispositivos móveis, todos esses dados se tornam vulneráveis se um dispositivo cair nas mãos erradas. Ao educar os usuários sobre o trabalho remoto seguro, o foco deve ser colocado em ajudar os usuários a identificar os pontos onde os sistemas ou dados podem ser comprometidos - e as etapas que eles podem realizar para mitigar esses riscos.

6. Segurança de dispositivo móvel

O uso de dispositivos móveis nas empresas tem crescido rapidamente e essa tendência deve se tornar ainda mais disseminada do que antes. Dispositivos móveis como laptops, telefones celulares e tablets permitem que os funcionários trabalhem em casa, em cafeterias, enquanto viajam ou em qualquer lugar que desejarem, proporcionando flexibilidade para eles e para a empresa. Por mais convenientes que sejam os dispositivos móveis, eles apresentam riscos sobre os quais os usuários devem ser informados.

Os usuários devem ser educados sobre como os dispositivos móveis podem potencialmente expor os dados e sistemas da empresa a acesso não autorizado. Isso envolve acesso por meio de dispositivos perdidos ou roubados, bem como software malicioso e aplicativos ilegítimos de terceiros.

7. Senhas e autenticação

As senhas continuam a ser uma grande dor de cabeça para empresas, funcionários e clientes. Os humanos simplesmente não foram projetados para lembrar frases longas e complexas - especialmente dezenas delas. Isso significa que os funcionários são constantemente tentados a escolher o caminho mais fácil e torná-los fáceis de lembrar - especialmente quando precisam compartilhar o acesso a aplicativos e serviços com seus colegas.

A maioria dos usuários finais saberá por que a segurança da senha é importante e terá a noção básica do que torna uma senha forte. O foco no treinamento de senhas e autenticação deve ser em conselhos práticos sobre como manter a segurança das senhas sem dificultar a vida dos usuários finais. Isso significa incentivar o uso de gerenciadores de senha (se isso for algo que sua empresa permitir), pedindo aos funcionários que ativem a autenticação de dois fatores para todos os serviços e sistemas com acesso a dados confidenciais, bem como ensinando os funcionários a fazer uma senha que seja ambos razoavelmente complexos, embora sejam razoavelmente fáceis de lembrar.

#8. Segurança na nuvem

Nos últimos anos, os serviços de negócios e dados têm mudado cada vez mais para a nuvem, com muitas operações sendo conduzidas inteiramente usando ferramentas e serviços baseados na web. Embora a nuvem ofereça grande flexibilidade para as empresas, é essencial que os usuários saibam como usá-la e acessá-la com segurança.

Senhas e autenticação fortes, bem como segurança de e-mail, tornam-se extremamente importantes quando sua empresa usa serviços em nuvem.

Um malfeitor que adivinha as senhas de um funcionário pode acessar seus dados confidenciais de qualquer lugar do mundo, por isso é essencial que os funcionários sejam instruídos sobre as medidas necessárias para manter as contas na nuvem seguras. A autenticação multifator é especialmente obrigatória para todos os serviços e aplicativos que contêm dados de negócios confidenciais.

#9. Wi-Fi público

À medida que os usuários trabalham cada vez mais em trânsito, é provável que se conectem a serviços, redes ou dados de negócios de pontos de acesso Wi-Fi públicos. O Wi-Fi público é altamente conveniente para o trabalho móvel, mas também apresenta riscos de segurança.

É importante ensinar aos usuários finais que seus dados podem ser potencialmente interceptados em redes Wi-Fi públicas. Se você permitir que seus usuários finais acessem os dados ou serviços da empresa por meio de redes Wi-Fi públicas, você deve equipá-los com o software de Rede Privada Virtual e instruí-los sobre como usá-lo de maneira segura.

#10. Segurança física

Mesmo com a multiplicação das ameaças à segurança cibernética, é essencial que a segurança física não seja esquecida. Não adianta proteger dados com senhas fortes e autenticação multifator se uma pessoa não autorizada pode simplesmente entrar no escritório e pegar uma cópia em papel de um documento confidencial na bandeja da impressora.

Ao treinar usuários finais em segurança física, é essencial que o foco seja colocado na identificação e mitigação de ameaças relevantes para as atividades diárias dos usuários finais individuais. Se a sua empresa estiver localizada em um escritório, todos os funcionários passarão pela porta do escritório - portanto, a utilização não autorizada é um exemplo de ameaça à segurança que é relevante para todos os funcionários. Os usuários finais devem ser treinados para pensar ativamente sobre quais áreas e documentos estão protegidos e garantir que eles estejam sempre trancados com segurança ou controlados quando não estiverem em uso.

#11. Midia removivel

Mesmo com o compartilhamento de arquivos e serviços de colaboração online na Internet se tornando mais populares, os dispositivos removíveis ainda estão sendo amplamente utilizados nas empresas. Por mais úteis que sejam os dispositivos de mídia removível, eles apresentam muitos riscos: são facilmente perdidos ou roubados, levando ao comprometimento de dados ou podem ser substituídos por dispositivos contendo malware. Um golpe comum é deixar uma unidade USB infectada por vírus no estacionamento de um escritório, esperando para ser retirada e inserida em um computador da empresa por um funcionário desavisado. Além disso, muitos usuários não sabem que não são apenas os dispositivos de armazenamento que podem representar um risco: até mesmo um simples cabo USB ou de carregamento pode ser modificado por um criminoso cibernético para conter malware.

Educar os usuários finais sobre o uso seguro de mídia removível se resume à responsabilidade. Deve ficar claro para os usuários que eles devem assumir a responsabilidade pelos dispositivos que estão sob seu controle - e que eles não devem conectar nenhum dispositivo que não tenha sido contabilizado em nenhum computador, mas, em vez disso, relatá-los à equipe de TI ou à segurança pessoal.

#12. Uso seguro de mídia social

Funcionários - e empresas - passam uma parte cada vez maior do seu dia nas redes sociais. É essencial, no entanto, garantir que a segurança da empresa não seja comprometida pelo uso descuidado das redes sociais.

O foco no treinamento de mídia social deve ser colocado em conscientizar os usuários de que o que eles compartilham pode estar disponível para qualquer pessoa na Internet - e que mesmo pequenos detalhes de dentro do escritório podem ser cruciais para os invasores. Por exemplo, uma selfie inocente de dentro do escritório pode mostrar um quadro branco no fundo com informações comerciais confidenciais ou até mesmo os detalhes de um cliente.