KnowBe4
Human error. Conquered.

Sete ameaças de engenharia social que o coaching em tempo real ajuda a mitigar

INTRODUÇÃO

Fortalecer o firewall humano da sua organização representa a última linha de defesa contra ataques cibernéticos e violações de dados. Um treinamento moderno de conscientização em segurança é uma das melhores maneiras de se fazer isso.
Outra maneira é o coaching em tempo real dos usuários em resposta a comportamentos de segurança arriscados, enviando a orientação certa no momento da ação perigosa. Para isso, uma plataforma de coaching em tempo real, como o SecurityCoach da KnowBe4, consolida os dados de alerta dos recursos de segurança da sua organização (gerenciamento de pontos de extremidade, e-mail/web, acesso a identidades, SIEM/SOAR etc.), faz uma análise deles e determina quais ameaças oferecem as melhores oportunidades para treinar seus usuários. O coaching em tempo real oferece às organizações a oportunidade de fortalecer seu firewall humano contra uma série de ameaças de engenharia social.

SETE AMEAÇAS DE ENGENHARIA SOCIAL

Aqui estão sete das ameaças mais comuns de engenharia social e como o coaching em tempo real pode ajudar a mitigá-las, aproveitando os dados de alerta dos seus recursos de segurança existentes.

Download de anexos de arquivos potencialmente perigosos
Muitas das tentativas de engenharia social giram em torno de fazer com que uma vítima em potencial baixe e/ou abra um anexo de arquivo perigoso, como um arquivo EXE, DOC ou HTML. Grande parte das ferramentas de segurança mencionadas anteriormente bloqueará a maioria dos downloads de arquivos de alto risco. No entanto, quando integradas ao coaching em tempo real, essas ações podem ser usadas como uma oportunidade para treinar os usuários a não baixar arquivos potencialmente maliciosos.

Clique em links de alto risco Muitas das tentativas de engenharia social contêm URLs maliciosos disfarçados de links confiáveis de um determinado fornecedor ou de outra fonte confiável. Mais uma vez, várias das ferramentas de segurança mencionadas anteriormente bloquearão esses links nocivos. Porém, ao fazer a integração com o coaching em tempo real, esses dados de alerta podem ser usados para lembrar os usuários de passar o mouse sobre o URL dos links para verificar a legitimidade antes de clicar neles.

Filtragem de conteúdo
Diversas ferramentas de segurança bloqueiam o conteúdo que consideram questionável, conforme definido pelas políticas de conteúdo de uma organização. Por exemplo, um usuário pode tentar assistir a um vídeo violento ou ser levado a ler conteúdo questionável/inadequado. O acesso a esse conteúdo é bloqueado, e o usuário pode receber uma mensagem de aviso para evitar conteúdo semelhante que vá contra as políticas da organização.

Execução ou instalação de software não autorizado
Frequentemente, os usuários tentam instalar software não aprovado pela organização. Um programa de controle de aplicativos de segurança bloquearia a instalação ou execução, ao mesmo tempo em que o coaching em tempo real poderia ser usado para lembrar os usuários de não instalar aplicativos ou serviços não autorizados, além de outras informações relevantes.

Início de conexões de saída nocivas Determinadas ferramentas de análise e monitoramento de tráfego de rede identificam conexões de saída nocivas para locais reconhecidamente perigosos. Ao usar uma plataforma de coaching em tempo real, o usuário poderia ser lembrado de não instalar nem usar nenhum software ou serviço de comunicação não autorizado.

Tentativa de fazer login em computadores não autorizados
Na maioria das organizações, os logins de computador para computador são raros. Um dos principais sinais de atividade maliciosa são os logins inesperados provenientes de um computador para outro sem que haja um motivo legítimo. Várias das ferramentas de segurança mencionadas anteriormente bloquearão essas conexões não autorizadas, e uma plataforma de coaching em tempo real poderia lembrar os usuários de não tentar fazer login em computadores que não estão autorizados a usar.

Tentativa de driblar os requisitos de autenticação multifator
Muitas organizações exigem que os usuários utilizem a autenticação multifator (MFA) para fazer login nas redes ou nos computadores da organização. Os usuários que tentarem driblar a MFA ou usar uma forma não autorizada de MFA normalmente acionarão um mecanismo de detecção e bloqueio. Uma plataforma de coaching em tempo real poderia ser usada para lembrar aos usuários de que eles devem usar um login com MFA aprovado pela empresa.

REDUÇÃO DOS RISCOS E MELHORIA DA CULTURA DE SEGURANÇA

Por fim, é mais provável que as pessoas aceitem a correção quando seus erros são imediatamente identificados e as melhores práticas de segurança são fornecidas em tempo real.

O coaching em tempo real permite à sua organização:

- Reforçar o treinamento de conscientização em segurança existente;
- Obter insights sobre os riscos de segurança, acompanhando as tendências das atividades arriscadas dos usuários ao longo do tempo;
- Reduzir o risco humano e melhorar a cultura geral de segurança da organização;
- Aumentar o valor dos seus recursos de segurança existentes, fazendo a integração com ferramentas de segurança comuns que você ja utiliza.

Derrote os agentes de ameaças e suas táticas maliciosas adicionando coaching de segurança em tempo real ao seu conjunto de ferramentas de conscientização em segurança.

SAIBA MAIS **Como o SecurityCoach pode reforçar seu firewall humano**

de segurança comuns que você já utiliza

Recursos adicionais

Teste de phishing gratuito
Faça este teste de phishing gratuito e descubra qual é a Porcentagem de Phish-prone dos seus funcionários

Automated Security Awareness Program gratuito
Crie um programa de conscientização em segurança personalizado para sua organização

Phish Alert Button gratuito
Agora, seus funcionários podem denunciar ataques de phishing de maneira segura com apenas um clique

Email Exposure Check gratuito
Descubra quais e-mails de usuários estão expostos antes que os infratores façam isso

Domain Spoof Test gratuito
Descubra se os hackers conseguem falsificar um endereço de e-mail no seu domínio

Sobre a KnowBe4

A KnowBe4 é a maior plataforma integrada do mundo em treinamento de conscientização em segurança e simulação de phishing. Reconhecendo que o elemento de segurança humano tem sido seriamente negligenciado, a KnowBe4 foi criada para ajudar as organizações a administrar o problema constante da engenharia social por meio de uma abordagem moderna e completa de treinamento de conscientização.

Esse método integra testes de linha de base que simulam ataques do mundo real, treinamento interativo e envolvente e avaliação contínua por meio de relatórios simulados de integridade corporativa para criar uma organização mais resiliente que tenha a segurança como prioridade.

Dezenas de milhares de organizações no mundo todo usam a plataforma da KnowBe4 em todos os setores, incluindo campos altamente regulamentados, como finanças, saúde, energia, governo e seguros, para mobilizar seus usuários finais como uma última linha de defesa e capacitá-los a tomar decisões mais inteligentes sobre segurança.

Para obter mais informações, acesse: www.KnowBe4.com

microhard
mais próxima para proteger sua informação

Somos Revenda KnowBe4. Escaneie o QRcode, fale com um especialista e solicite uma demonstração gratuita!