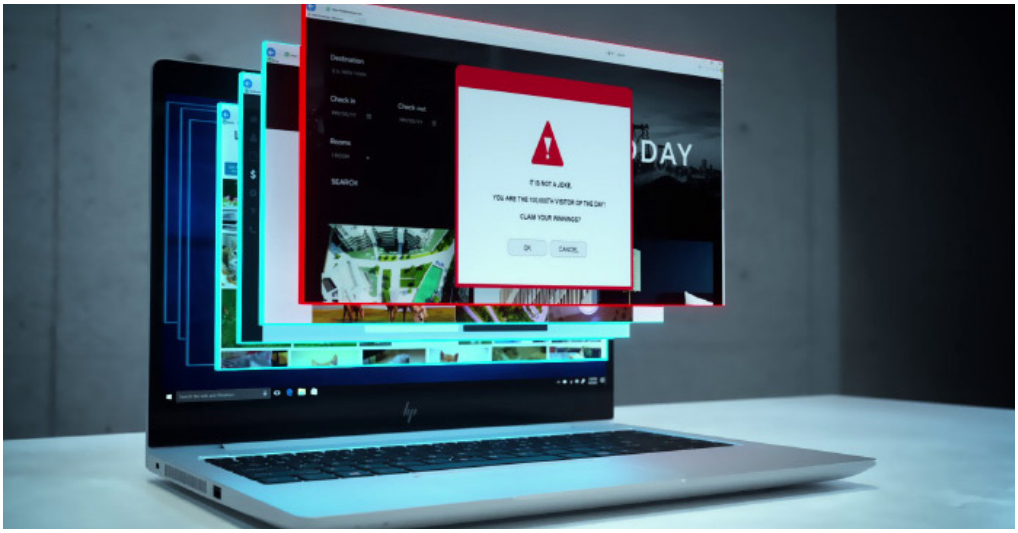
O phishing deixou de ser apenas para e-mails

Escrito por Alexandre Silveira

Saiba mais



Um web browser é um portal de informações...e ameaças. O que pode fazer para proteger a sua empresa?

Os web browsers servem para muitas coisas. Num inquérito recente a 400 CIO's 68% afirmaram que os cibercriminosos são sofisticados, e que os seus colaboradores têm dificuldade em diferenciar entre sites seguros e não seguros[1]. Tendo isso em consideração, não surpreende que 70% dos profissionais de TI sofram ataques de phishing semanais – e não apenas por e-mail[2]. Os hackers sofisticados usam agora redes sociais, publicidade e erros ortográficos frequentes para enganar os colaboradores para que revelem informações pessoais confidenciais. Como os esquemas de phishing são cada vez mais difíceis de identificar, as empresas esforçam-se para proteger os seus colaboradores destes ataques.

Apesar da maior consciência e investimento em software de segurança e formação dos colaboradores, houve um aumento de 232% de ataques cibernéticos em portáteis e desktops nos últimos seis anos[3]. Os cibercriminosos continuam a ter sucesso, porque os números estão do seu lado. São necessários muitos esforços para salvaguardar os dados, mas basta que um colaborador clique numa ligação maliciosa para destruir a sua empresa.

Os ciber ataques nas redes sociais são uma grande parte do problema. Plataformas como o Facebook e Twitter são terrenos propícios a ataques cibernéticos. Não são desenhados apenas para envolvimento e comunicação, mas também são fáceis de usar e económicos. É incrivelmente fácil criar contas fraudulentas e iniciar publicações de conteúdos maliciosos, desde ligações a recolha de dados para páginas de destino com pop-ups inseguros.

A maioria destas atividades online baseiam-se em técnicas de phishing, normalmente reservadas ao e-mail. As redes sociais permitem ligações entre pessoas, e é fácil criar uma identidade substancial e credível e seguir com utilizadores genuínos das plataformas.

Vevo, o conhecido serviço de streaming, foi a vítima recente de uma enorme violação de dados. Um dos seus colaboradores foi alvo de um esquema de phishing no LinkedIn, que levou a que 3,12 TB de ficheiros internos fossem divulgados online. Isto incluiu vídeos, documentos empresariais, material promocional, conteúdos para redes sociais, e informações sobre os artistas que assinaram contratos com empresas participantes[4].

A equipa de hacking OurMine reivindicou a responsabilidade pelo ataque, após uma discussão por e-mail com um membro da Vevo. Isto demonstra o perigo do **spear-phishing**, um ataque específico que tenta roubar dados específicos de um alvo específico. Os hackers disfarçam-se frequentemente de amigos ou de fontes seguras (i.e., o seu banco) para enganar o alvo a divulgar informações - o que representa 91% dos ataques.

O phishing deixou de ser apenas para e-mails

Para a maioria das empresas que são vítimas de ataques de phishing, como a Vevo, as consequências podem ser prejudiciais e duradouras. Podem resultar não só na perda de produtividade dos colaboradores e dados de clientes, mas também na perda dos próprios clientes. A confiança que os clientes têm na empresa pode ser fortemente afetada devido à falha de segurança - para eles, a sua empresa deixa de ser um detentor seguro das suas informações. E, apesar de isto ser passível de recuperação, na maioria das vezes as implicações são permanentes.

No 4º trimestre de 2017, os ataques de phishing nas redes sociais atingiu os 500%, com uma tendência para contas falsas como apoio ao cliente de grandes marcas[5]. Este desenvolvimento tornou-se conhecido como **angler-phishing**, porque os hackers colocam o isco e esperam que os utilizadores das redes sociais vão até eles. Usando a mesma marca e um nome de conta que parece verdadeiro, milhões de pessoas que confiam nas redes sociais são frequentemente enganadas por um ataque convincente. Assim, logo que o utilizador entra em contacto, a conta falsa envia uma ligação para um site de phishing e solicita o início de sessão, permitindo ao phisher ter acesso a dados privados.

Uma das formas mais fáceis de evitar que os seus colaboradores se envolvam em phishing nas redes sociais é promover uma mudança de comportamento na empresa. Deverá ajudar os seus colaboradores a evitar estes simples erros que levam a consequências devastadoras para a sua empresa:

1. Limite as interações a utilizadores de confiança
2. Não clique em ligações de fontes não verificadas
3. Nunca transfira anexos de ficheiros nas redes sociais
4. Ative a autenticação de dois fatores em todas as contas de redes sociais e dispositivos - isso dificultará os ataques de hacking
5. Forneça formação adicional aos colaboradores com privilégios de acesso elevado ou funções de gestão de redes sociais

Outro aspeto essencial do seu plano de segurança é a tecnologia que usa para resistir aos ataques cibernéticos. A família HP Elite, por exemplo, é uma família de computadores portáteis e PCs desenhada com a segurança em mente desde o primeiro momento.

Uma das suas funcionalidades é o HP Sure Click, disponível em plataformas HP Elite selecionadas, que aborda a segurança de navegação de forma diferente. Em vez de criar apenas alertas para sites perigosos, evita também que o malware, ransomware e vírus infetem outros separadores do browser e o sistema geral. Quando um utilizador inicia uma sessão de navegação, cada site visitado aciona o HP Sure Click. Por exemplo, sempre que um website é visitado, o HP Sure Click cria uma sessão de navegação isolada com base em hardware, eliminando a capacidade de um website infetar outros separadores ou o próprio sistema.

Em relação a empresas que mudam a sua estratégia de segurança e investem nestes dispositivos modernos, como a série HP EliteBook 800, com processadores opcionais de 8ª geração Intel® Core™, é mais fácil passar à ação. É aqui que uma solução como o HP Device as a Service (DaaS) entra em ação. É um modelo moderno de utilização de PCs que simplifica a forma como as empresas equipam os seus colaboradores com o hardware e acessórios adequados, gerem as frotas de dispositivos com diversos SO's e obtêm serviços de vida útil adicional. O HP DaaS oferece planos simples e flexíveis, com um preço por dispositivo para manter o funcionamento simples e eficiente.

Por fim, dispor de uma equipa bem formada e de dispositivos otimizados para segurança irá ajudá-lo a combater o cibercrime nas redes sociais, uma das maiores ameaças atuais. Será cada vez maior e mais assustador, pelo que está na hora de melhorar as suas defesas.

Descubra as vantagens das soluções de segurança HP para o seu negócio.

Fontes:

1. https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
2. https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/8355/HP-Nearly-70-of-IT-Professionals-Experience-Weekly-Phishing-Attacks.aspx
3. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
4. https://www.zerofox.com/blog/vevo-hacked-via-linkedin-phishing-campaign/
5. https://www.infosecurity-magazine.com/news/social-media-phishing-attacks-soar/

4AA7-3218PTE, Maio de 2018