Canais digitais são o cenário ideal para fraudes: conheça às 5 fraudes mais utilizadas

Na era da transformação digital, cada instituição pode se converter facilmente em um alvo da engenharia social, conduzindo a uma perigosa propagação viral da desinformação.

15/09/2016 17:33:31

A Easy Solutions, empresa de Proteção Total Contra Fraude®, detalha como o aumento de novos canais de comunicação também se converte em novos canais de ataque. “Aplicações, redes sociais e anúncios em motores de busca são os canais favoritos dos estelionatários,” afirma Fernando Cuervo, líder de Detect Monitoring Service e Especialista em Segurança de Easy Solutions, que explica como se proteger e ficar alerta.

“Para os cibercriminosos, é mais fácil induzir as vítimas a divulgar informação sensível do que hackear os nomes dos usuários e senhas. Essa é a razão principal porque as fraudes por meio das redes sociais, aplicações móveis e anúncios em sites de busca estão aumentando”, observa o especialista. Essas fraudes estão baseadas na engenharia social, que consiste em várias técnicas empregadas por cibercriminosos para levar os usuários desprevenidos a revelar dados confidenciais, iniciar ataques de malware inconscientemente ou abrir links de sites infectados.

Nesta era de transformação digital, cada instituição pode se converter facilmente em um alvo da engenharia social, conduzindo a uma perigosa propagação viral da desinformação. Veja abaixo as cinco fraudes que têm surgido em diversos canais online e as recomendações para evitá-las da melhor maneira possível.

1. Contas substituídas do Facebook

Esta fraude consiste em disponibilizar tickets aéreos a um custo muito baixo. No exemplo abaixo, um estelionatário oferece tickets na primeira classe e bolsas de dinheiro, usando um perfil do Facebook. Os cibercriminosos também imitam perfis nas redes sociais de conhecidas linhas aéreas como American Airlines e Emirates Air.

2. Falsas promoções nas Redes Sociais

Falsas promoções convidam os usuários das redes sociais a aproveitar ofertas e descontos como

aqueles apresentados neste perfil falso do Facebook de uma conhecida instituição financeira. As imagens e informação são muito similares ao perfil original, induzindo os usuários a entregar dados sensíveis. Inclusive há atualizações motivando as pessoas a comprar a um preço especial, mas depois de fazer clique no link são dirigidos imediatamente a um site de phishing.

3. Sequestro de contas do Twitter

O Facebook não é a única rede social em que as empresas devem se proteger. O Twitter é uma importante fonte de informação para muitos consumidores. Já que a plataforma é especializada em oferecer informação rápida, as organizações devem agir rápido também para combater abuso e evitar que a desinformação sobre uma empresa não se propague.

Quando alguém hackeou a conta do Twitter pertencente à Associated Press. Os hackers enviaram aos cerca de 2 milhões de seguidores da agência um tweet falso sobre explosões na Casa Branca que feriram o Presidente Barack Obama. A Associated Press logo anunciou que o tweet foi fabricado (Figura 5), mesmo assim Dow Jones caiu mais de 100 pontos em dois minutos como resultado do tweet.

Este caso ilustra quão negativo é o impacto que os hackers podem causar a uma organização e ao resto do mundo tão somente por obter o acesso a sua plataforma de redes sociais.

4. Ataques por meio de Anúncios de Motores de Busca

Os cibercriminosos também estão usando Google AdWords para enganar as pessoas. Os usuários clicam no link de phishing que aparece no início dos resultados de busca do Google (Figura 6). Em vez de levá-lo ao site legítimo, os usuários são direcionados a um site falso que solicita informação sensível. Como o Google não pede que os compradores de anúncios demonstrem que pertencem à empresa, qualquer pessoa pode criar um anúncio usando qualquer marca. Essa prática também se aplica ao Bing, AOL e Yahoo. As organizações que são vítimas desses ataques podem perder lucro, tráfego no site e a lealdade de seus clientes.

5. Aumento de Aplicações Falsas

Mais de 1,8 milhão de aplicações falsas do Android são descarregadas a cada ano. As lojas App Store e Google Play implementam restritos protocolos de segurança a fim de garantir que só as aplicações legítimas estejam disponíveis para os usuários. As lojas de terceiros ou não autorizadas, porém, não seguem as mesmas políticas de segurança, isto quer dizer que as aplicações disponíveis nestes lugares apresentam um risco muito maior. Por exemplo, a aplicação pode estar modificada para infectar os dispositivos com malware, além do mais, a aplicação pode não ser perigosa no momento de descarregar, mas os cibercriminosos são capazes de mudar as propriedades da

aplicação depois do download para expor os usuários a fraudes.