CEST Centro de Estudos Sociedade e Tecnologia
USP Universidade de São Paulo
Boletim - Volume 1, Número 5, Março/2016

A engenharia social e os crimes cibernéticos

Marvin Ferreira

Com a popularização do acesso à internet, por meio da utilização cada vez mais frequente da banda larga e de dispositivos móveis, e o consequente crescimento das redes sociais, ficou mais fácil e rotineiro o compartilhamento público de informações pessoais, como fotos, vídeos e textos. E junto com esta facilidade de exposição individual também aumentaram os riscos de que ocorra o uso indevido destes dados, inclusive por criminosos digitais, também conhecidos como criminosos cibernéticos. O compartilhamento desenfreado de dados pessoais em redes sociais expõe a privacidade individual, tornando as pessoas mais vulneráveis às técnicas da chamada Engenharia Social (do inglês, *Social Engineering*).

Uma tendência observada dos aplicativos e redes sociais atuais indica que, quanto mais divertidos forem, mais exigirão dados pessoais dos usuários em troca dos serviços prestados.

A Engenharia Social pode ser compreendida, no contexto da segurança da informação, como a manipulação de indivíduos para induzi-los a compartilhar suas informações confidenciais e sigilosas com criminosos e golpistas ocultos.

Estes dados confidenciais quando obtidos por pessoas mal-intencionadas podem ser usados para realizar fraudes, acessos a sistemas ou crimes cibernéticos, baseados em informações digitais.

As técnicas de Engenharia Social buscam desviar as pessoas da racionalidade. Deste modo, os criminosos cibernéticos ganham a confiança dos indivíduos para obter, por exemplo, suas senhas bancárias ou outras informações confidenciais e sigilosas.

Ações adicionais dos criminosos virtuais envolvem a investigação de hábitos, hobbies e preferências das vítimas, elementos que são obtidos sem muita dificuldade nas redes sociais.

Algumas técnicas de Engenharia Social são as seguintes:

Pretexting – Por meio da criação de um cenário, ambiente ou situação para envolver a vítima, os criminosos buscam informações confidenciais ou estimulam alguma ação que permita, por exemplo, o acesso a um computador ou sistema. Nestes casos, a vítima é induzida a acreditar em uma identidade falsa, um técnico de suporte corporativo, por exemplo, e então acaba fornecendo dados de funcionários ou clientes acreditando em uma falsa manutenção de sistemas.

Diversion Theft – Também conhecido como "roubo por desvio" consiste em fazer com que empresas de entregas ou correios desviem seus carros de remessa de suas rotas originais e entreguem conteúdos em endereços diferentes dos corretos – ou seja, para os ladrões.

Phishing – Uma das técnicas mais antigas e um golpe eletrônico ainda muito praticado. Ocorre pelo envio de um *e-mail* aparentemente legítimo de um amigo ou empresa conhecida pela vítima. Há um link que, quando clicado, direcionada o receptor do *e-mail* para um site falso onde suas informações podem ser furtadas ou seu computador infectado por algum vírus capaz de coletar informações – como dados bancários, senhas e documentos – e enviá-las ao criminoso.

Phone Phishing – Técnica semelhante ao *phishing* e que muitas vezes começa por *e-mail*. A vítima recebe um *e-mail* ou carta

falsos pedindo para ligar ao seu serviço bancário, por exemplo. Depois de digitar dados e senhas por telefone, suas informações passam automaticamente para os ladrões.

Baiting – Funciona como um Cavalo de Troia, utilizando-se da curiosidade das vítimas. Neste caso, o criminoso cria um CD ou *pendrive* ou qualquer mídia que pode realizar a operação de boot (desligar e ligar) no computador – com um título do tipo "fotos da festa surpresa" ou "salários da equipe" – e o abandona em lugares públicos, onde possíveis vítimas terão a curiosidade de pegar estas mídias e inseri-las em seus computadores.

A partir daí, a simples inserção da mídia no computador irá infectá-lo com a instalação de um malware que dará acesso à máquina da vítima, gerando uma brecha de invasão no sistema ou até mesmo capturando os dados contidos na máquina e enviando ao criador do ataque.

Existem inúmeras outras técnicas baseadas na descoberta e exploração de vulnerabilidades das pessoas, que acabam sendo envolvidas em situações que parecem legítimas, mas que, na verdade, são meras criações planejadas pelos manipuladores.

Uma delas envolve ligar para diversos números de uma empresa se passando por seu funcionário de suporte técnico e perguntando sobre possíveis problemas nos computadores e, após a aprovação do usuário, abrir uma brecha no sistema.

A exposição de dados nas redes sociais coloca indivíduos em risco, pois facilita o trabalho de criminosos digitais. Um simples aplicativo de paquera como o Tinder, por exemplo, que usa informações do Facebook ou Instagram, pode abrir brechas para se levantarem dados de outras pessoas pela internet.

Alguns dos usuários também expõe abertamente seus números de celular, Snapchat, redes sociais e diversos detalhes de suas vidas nas pequenas biografias do Tinder. Por exemplo, ao obter o Snapchat de uma pessoa, pode-se acompanhar em tempo real suas atividades diárias, ao acessar seu Facebook, e extrair locais onde estuda, trabalha, mora, passeia, nomes de parentes etc.

O acesso a essas informações depende diretamente do nível de exposição que as pessoas aceitam e dos dados que publicam em suas redes sociais. Esta superexposição nas redes sociais desenvolveu uma sociedade exposta em vitrines, onde todos podem ver, acompanhar e comentar uns sobre os outros.

Uma tendência observada dos aplicativos e redes sociais atuais indica que, quanto mais divertidos forem, mais exigirão dados pessoais dos usuários em troca. O objetivo é combinar, manipular e até mesmo vender os dados, como forma de financiar o serviço prestado. Empresas como Facebook e Google já fariam isto com as informações dos seus usuários.

Portanto, temos de estar alertas para o uso constante de redes sociais, dos aplicativos para aparelhos celulares e até de sites de paquera e relacionamentos, por exemplo. Afinal, tudo o que utilizamos na internet cada vez mais nos expõem e nos torna mais vulneráveis a crimes virtuais.

Ou até mesmo nos transforma em possíveis vítimas de crimes no mundo real, devido à utilização de dados do mundo virtual por criminosos de todos os tipos.

Marvin Ferreira *é Graduado em Ciência da Computação pela PUC de São Paulo. Atualmente é mestre em Engenharia da Computação na Escola Politécnica da Universidade de São Paulo; pesquisador pelo CEST.*

Jornalista Responsável: Edson Perin
Coordenador: Edison Spina

Este artigo resulta do trabalho de apuração e análise do autor, não refletindo obrigatoriamente a opinião do CEST.