Segurança em Foco

CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial

Engenharia SOCIAL

Edição nº16
Outubro/2021

Engenharia social, é a habilidade de conseguir acesso a informações confidenciais pessoais ou de áreas importantes de uma instituição, mediante habilidades de persuasão.

Muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou dados.

A engenharia social pode utilizar meios computacionais ou não.

Uma de suas formas mais comuns se apresenta através do envio de e-mails, cujo remetende se passa por uma pessoa ou empresa conhecida pelo usuário.

A busca de informações pode ocorrer também nos locais mais simples, como mesas de trabalho e lixeiras, e pela atenção às conversas alheias em locais sociais.

De modo geral, os ataques de engenharia social acontecem em uma ou mais etapas.

Primeiramente, o criminoso investiga a vítima em potencial para obter as informações necessárias para o ataque, como pontos de entrada e protocolos de segurança fracos, essenciais para prosseguir com a prática.

Em seguida, ele busca conquistar a confiança da vítima e fornecer estímulos para atividades subsequentes que violam as práticas de segurança, como revelar dados confidenciais ou conceder acesso a recursos críticos, por exemplo.

Nesse sentido, o ataque de engenharia social é baseado no erro humano e não na vulnerabilidade de softwares ou sistemas operacionais.

Por isso, como não envolve nenhuma questão técnica que possa ser reconhecida pelos dispositivos de segurança tradicionais, esses ataques estão entre os maiores riscos cibernéticos às empresas atualmente e requer diversos cuidados básicos para prevenção contra os golpes.

As principais técnicas utilizadas nesse tipo de ataque são:

- ***Spam*** **de e-mail: conforme já mencionado em outro informativo, o *spam* é uma das formas mais antigas de engenharia social, utilizadas para obter informações pessoais;**
- ***Phishing*****: conforme já mencionado em outro informativo, no qual os e-mails são disfarçados como fonte confiável e, na verdade, são projetados para enganar as vítimas, levando-as a fornecer informações pessoais ou financeiras;**
- ***Baiting*****: se refere a quando um invasor deixa um dispositivo infectado por *malware*, como um *pendrive USB*, em um local onde é provável que alguém o encontre; esses dispositivos são frequentemente etiquetados de forma provocativa para atrair a curiosidade; se alguém conectar o pendrive no computador, ele poderá infectá-lo com *malware;***
- ***Vishing*****: o criminoso liga para a vítima fingindo ser uma pessoa confiável ou um representante do seu banco ou de uma instituição parceira da empresa em que você trabalha e tenta, durante a conversa, obter informações da vítima;**
- ***Farming*****: o criminoso procura uma maneira de estabelecer um relacionamento com a vítima.**

Normalmente ele analisa o perfil das vítimas em mídias sociais e tenta estabelecer um relacionamento com ela, com base nas informações obtidas em sua pesquisa.

O criminoso tenta enganar a vítima pelo máximo de tempo que for possível, a fim de extrair o máximo de dados possíveis.

Seguem algumas dicas para se proteger desse tipo de ataque:

- **Adotar uma certa desconfiança e manter-se vigilante; saber que esse tipo de ataque pode acontecer é o jeito mais eficaz de garantir segurança, principalmente quando informações sensíveis fazem parte de um determinado assunto;**
- **Fique atento às mensagens ou ligações, em nome de alguma instituição, que tentem induzí-lo a instalar/executar programas ou clicar em *links*; elas podem ter sido enviadas de contas invadidas, perfis falsos ou podem ter sido forjadas;**
- **Não divulgue informações confidenciais sobre você ou sua empresa, seja por telefone, online ou pessoalmente;**
- **Proteja todos os dispositivos móveis e as máquinas, tanto pessoais quanto da empresa. Evite conectar *pendrive* ou qualquer outro tipo de mídia de origem desconhecida;**
- **Evite deixar visíveis informações como dados pessoais, senhas ou número de contas; o atacante pode ter acesso a essas informações simplesmente sentado ao seu lado em uma conversa;**
- **Sempre desconfie de interações que solicitem a divulgação de dados pessoais ou confidenciais, de cunho sigiloso ou de acesso à rede corporativa;**
- **Utilize um filtro *antiphishing*, a maioria vem integrado aos principais navegadores e antivírus, e serve para alertar os usuários quando uma página suspeita de ser falsa é acessada;**
- **Pense na sua presença digital, vivemos em uma época onde as pessoas compartilham muitas informações nas redes sociais, e isso pode ser perigoso. Alguns ataques de engenharia social tentam ganhar sua confiança usando eventos recentes compartilhados em redes sociais para chamar sua atenção;**
- **Sempre checar a privacidade das redes sociais, deixando as postagens configuradas para "apenas amigos" e tomar cuidado com o que está sendo publicado na internet; essa cautela deve ser expandida para várias outras situações online, como um currículo digital, onde é uma boa opção esconder endereço, número de telefone e data de nascimento, para que essas informações não sejam de acesso público.**

Fique ligado: no próximo mês, falaremos sobre *Vale a pena usar programa pirata?*

Tribunal Regional Eleitoral - RN