Engenharia Social

ALUNOS:

GUSTAVO PIMENTA

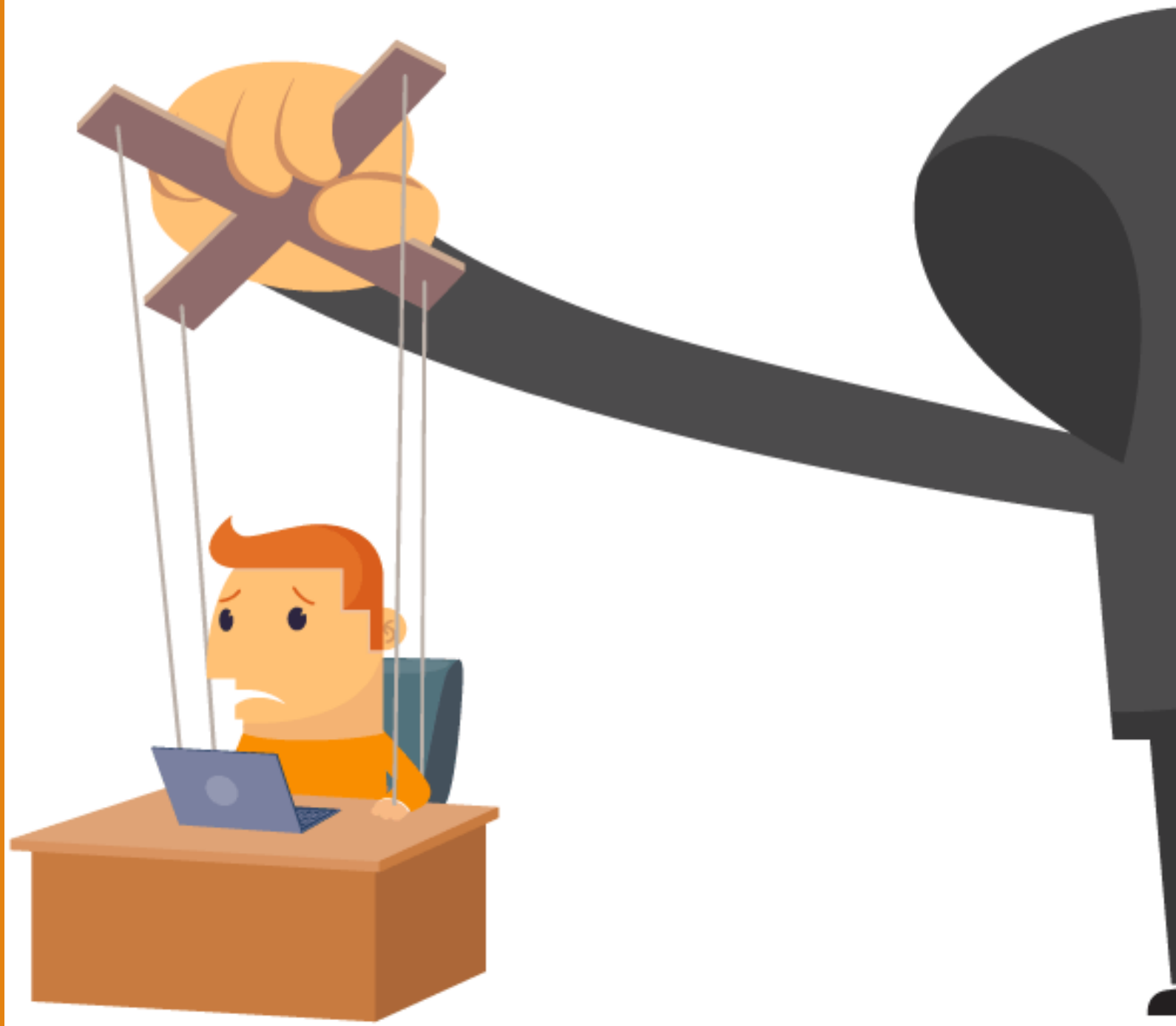
GUILHERME MACHADO

HORÁCIO SORIO

LEONARDO GOMES

MATHEUS MULINARI

MARCELLY COSTA



O que é?

A engenharia social é uma técnica de manipulação que explora erros humanos para obter informações privadas, acessos ou coisas de valor.

No crime cibernético, esses golpes de "hacking humano" tendem a atrair usuários desavisados para expor dados, espalhar infecções por malware ou dar acesso a sistemas restritos.

Como é executado?

A engenharia social só é bem-sucedida por apostar que o usuário vai ficar tentado a clicar em um link ou realizar uma determinada ação. Ou seja, o erro humano é explorado por novas técnicas de ataques. De modo geral, esses ataques acontecem de diversas formas e podem ser realizados em qualquer lugar em que a interação humana esteja envolvida. Confira a seguir os principais tipos de ataques cometidos na Engenharia Social.

Como é executado?

1- Phishing

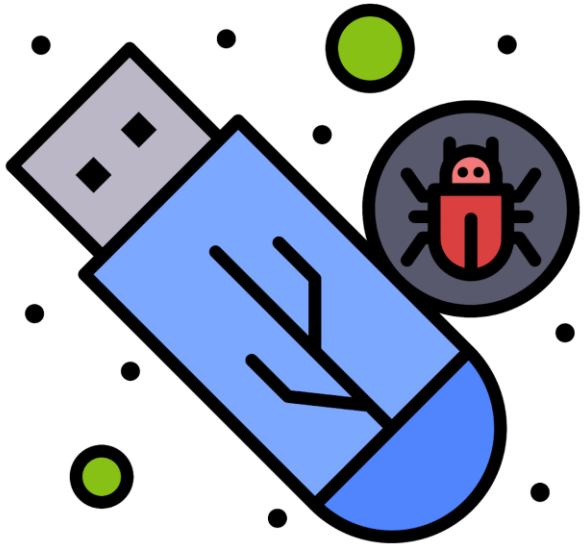
O phishing é o tipo mais comum de ataque de engenharia social, e também o mais simples e eficaz. O golpe consiste em convencer o usuário a abrir e-mails, clicar em anexos e links maliciosos e, com isso, coletar credenciais, dados privados e espalhar malware pelas redes. E-mails solicitando que os usuários troquem suas senhas ou afirmando que uma sua conta será cancelada se não realizar uma atualização são alguns dos exemplos de mensagens supostamente legitimas, mas cada vez mais difíceis de serem detectadas.

Como é executado?

2- Baiting

Essa técnica costuma acontecer com mais recorrência em ambientes de trabalho. Nela, o criminoso infecta um dispositivo(geralmente um pen-drive) com um malware e o deixa em algum lugar aleatório.

Um colaborador encontra o dispositivo e o conecta, por curiosidade, em algum PC ou notebook para conferir o conteúdo. Geralmente, a vítima também instala os arquivos do pen-drive em seu dispositivo para saber do que se trata. Fazendo isso, o criminoso passa a ter acesso a praticamente todos os sistemas do dispositivo infectado.



Como é executado?

3 - Quid pro quo

O ataque de quid pro quo acontece quando um hacker solicita informações confidenciais de alguém em troca de algo. O próprio termo é traduzido como “isso por aquilo”, pois o cibercriminoso oferece à vítima algo em troca desses dados sensíveis.

Isso pode acontecer, por exemplo, com o criminoso se passando por alguém do setor de tecnologia para abordar vítimas que tenham problemas relacionados aos seus sistemas ou equipamentos.

Como é executado?

4 - Spear-phishing

O spear-phishing é uma versão mais direcionada do phishing, focada em indivíduos e empresas específicas. Nesse tipo de ataque, o criminoso se passa por algum executivo ou membro da organização para cometer a fraude.

Ele se aproxima dos colaboradores com o objetivo de obter informações sensíveis. Pode fazer isso por meio de uma demanda urgente, por exemplo, exigindo uma transação financeira imediata para uma conta específica.

Caso Target (EUA)

Em 2013, a Target, segunda maior rede de lojas de departamento dos EUA, sofreu um ataque deixando 40 milhões de informações de pagamentos de seus clientes vulneráveis aos hackers.

Primeiramente, os atacantes enviaram um e-mail de *phishing* – *que tem o objetivo enganar usuários para obter informações confidenciais como nome de usuário e senha* – aos funcionários de uma empresa parceira da Target. Assim, os criminosos conseguiram instalar um *malware* – *um programa de computador destinado a infiltrar-se em um sistema de computador com o intuito de causar danos, alterações ou roubo de informações* – para que conseguissem acessar a rede da Target.

O acesso a rede, permitiu que os criminosos instalassem outro *malware* no sistema da Target com o objetivo de copiar informações de cartões de crédito e débito dos clientes.

Como os usuários podem se proteger?

Você viu que a Engenharia Social explora a confiança e as emoções das vítimas. Sendo assim, é essencial treinar os colaboradores e os clientes nas melhores práticas de segurança da informação, para que conheçam e adotem cuidados indispensáveis no dia a dia. A seguir, listamos algumas práticas e ações importantes para saber como se proteger dos engenheiros sociais.

- Adotar certa confiança e manter-se vigilante;
- Sempre desconfie de interações que solicitem a divulgação de dados pessoais ou confidenciais;
- Nunca se deixe levar pela pressão que criminosos tentam impor quando querem informações;
- Evites cliques com risco potencial;
- Tenha cuidado com anexos;
- Proteja as máquinas e equipamentos com bons protocolos de segurança.