INSTITUTO FEDERAL
PIAUÍ

Engenharia Social

SEGURANÇA DA INFORMAÇÃO

Prof. Silvino Marques
silvinomarques@ifpi.edu.br

Introdução

Engenharia Social consiste no ato de obter informações das pessoas;

A engenharia social não se limita a meios computacionais;

Tipos de engenharia social

Baseado em pessoas:

- Nesse tipo, as técnicas utilizadas não necessitam do auxílio de programas computacionais;
- Ex: disfarces, vendedores, telemarketing e etc;

Baseado em computadores:

- As técnicas utilizadas necessitam do auxílio de programas computacionais;
- Ex: phishing, SET (*Social Engineering Tool*);

Introdução

Os engenheiros sociais são pessoas cultas, de um papo agradável e que conseguem fazer com que você caia em suas armadilhas.

Utilizando meios digitais, telefônicos e até pessoalmente, observam e estudam você sem que sejam percebidos.

E isso não é algo novo que surgiu com a informática, há décadas esses engenheiros vêm agindo.

- Por aqui, normalmente conhecemos essas pessoas por **estelionatários**.

Formas de ataque

Geralmente, existem três maneiras básicas de agir:

- Por e-mail:
  - O engenheiro envia um e-mail para seu alvo contendo informações que ele quer. Pode ser pedindo um documento importante ou fingindo ser da TI da empresa e requerendo uma mudança de senha. De qualquer maneira, seja a correspondência eletrônica ou real, quase sempre ela fica perfeita. Com o logotipo da empresa, marca d'água e e-mail de origem parecendo que vem mesmo da empresa. Tudo para gerar confiança.

Formas de ataque

- Pessoalmente:
  - É o método mais arriscado, mas também o mais eficiente. O engenheiro arruma um bom terno, um relógio com aparência de caro e uma maleta com um notebook. Pode se passar por um cliente, por um funcionário ou mesmo parceiro de negócios. As possibilidades são infinitas, já que as pessoas tendem a confiar mais em alguém muito bem vestido. Outra coisa que eles tendem a fazer pessoalmente: revirar o lixo de uma empresa em busca de informações importantes, como listas de empregados ou qualquer outra coisa que beneficie a Engenharia Social.

Formas de ataque

- Pelo telefone:
  - O engenheiro se passa por alguém importante, finge precisar de ajuda ou mesmo se oferece para ajudar. O interesse dele é mexer com o sentimento das pessoas, fazendo com que elas acabem entregando o que ele deseja sem, muitas vezes, nem saberem disso.

Manipulando os Sentimentos

Como já deve ter dado para perceber, o forte do Engenheiro Social é manipular os sentimentos das pessoas, levando-as a fazerem o que ele quer.

Vamos dar uma olhada nos casos mais comuns de manipulação, que são:

- **Curiosidade, Confiança, Simpatia, Culpa e Medo**.

Curiosidade

Muitos dizem que a curiosidade é a mãe do conhecimento.

Sabendo disso, o engenheiro social vai tentar atiçar de todas as maneiras a curiosidade dos empregados da empresa-alvo.

Existem várias técnicas para se fazer isso, desde o envio de um falso cartão por e-mail (o que é geralmente barrado antes de chegar nos funcionários) até técnicas que parecem absurdas à primeira vista, mas que funcionam.

Confiança

A confiança também é um fator muito manipulado pelos engenheiros sociais.

Ela pode ser gerada de várias maneiras:

- Você pode se passar por um funcionário de outra filial, citar procedimentos técnicos do manual da empresa ou, simplesmente, oferecer-se para ajudar com algum problema.
- Outra coisa comum é você receber um e-mail com o endereço de origem de um amigo ou colega de trabalho e esse e-mail vir com um anexo. **E-mails podem facilmente ser forjados!!**

No geral, todos esses fatores fazem com que a sua "resistência" a entregar informações fique mais fraca.

Simpatia

Outro grande modo de manipulação. O melhor exemplo de simpatia é no caso das mulheres.

- É muito mais fácil um “mulherão” conseguir ser bem sucedida na Engenharia Social com os seguranças de uma empresa do que um homem. Isso vale para telefone também, afinal, se a pessoa que fala com você tem uma voz doce e meiga, inconscientemente você acaba descartando a possibilidade daquela pessoa tentar “lhe passar a perna”.

Culpa

Quando as pessoas se sentem culpadas por algum motivo, são mais propensas a ajudar. Isso não deixa de ser verdade no meio da Engenharia Social.

Inflita culpa em alguém e faça essa pessoa lhe ajudar no que você quiser.

Dentro de uma empresa, os funcionários mais vulneráveis a essa emoção são os novatos, que estão querendo mostrar serviço.

Medo

A manipulação do medo é uma das mais poderosas, pois tende a obter resultados muito rápidos.

- Isso porque ninguém consegue aguentar a pressão por muito tempo e acaba entregando as informações rapidamente.

Geralmente, as “ameaças” parecem vir de pessoas com uma hierarquia bem maior que a do alvo dentro da empresa.

- Afinal, se um colega lhe ordenasse alguma coisa, você riria dele. Mas, e o vice-presidente da empresa?

Dicas de um Engenheiro Social Anônimo

Seja profissional:

- Você não quer que a pessoa desconfie, já que está criando uma ilusão. Tente transparecer confiança.

Fique calmo:

- Dê a impressão que você pertence àquele local.

Conheça sua marca:

- Conheça seu inimigo. Saiba exatamente como ele irá reagir antes que o faça.

Não tente enganar alguém esperto:

- Isso resultará em desastre. Sempre existem pessoas mais ingênuas.

Planeje sua fuga:

- Se alguém suspeitou, não entre em pânico e corra. Salve a fonte.

Dicas de um Engenheiro Social Anônimo

Tente parecer uma mulher:

- Está provado que as mulheres dão mais confiança ao telefone. Use isso como vantagem. Use a ajuda de uma mulher se necessário.

Logomarcas:

- Aprenda a fazê-las. São importantes em e-mails e correios falsos.

Cartões de apresentação e nomes falsos:

- Use-os para impressionar e parecer profissional.

Use um time se for necessário:

- Não seja arrogante e autoconfiante. Se precisar de ajuda, consiga.

TÉCNICAS

Tipos

Pessoalmente:

- ***Shoulder Surfing;***
- ***Rush Autentication/Tailgating;***
- ***Identity Theft;***

Internet/Telefone:

- ***Phishing;***
- ***Pharming;***
- ***Identity Theft;***

Shoulder Surfing

Espiar sobre os ombros

- Este tipo de ataque ocorre quando uma das partes é capaz de olhar sobre o ombro de outro ou espionar a tela do outro.

Rush Authentication/Tailgating

Furto de identidade (Identity theft)

É o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas.

Exemplos:

- Se alguém abre uma empresa ou uma conta bancária usando seu nome e seus documentos.
- Na Internet isto também pode ocorrer, caso alguém crie um perfil em seu nome em uma rede social, acesse sua conta de *e-mail* e envie mensagens se passando por você.

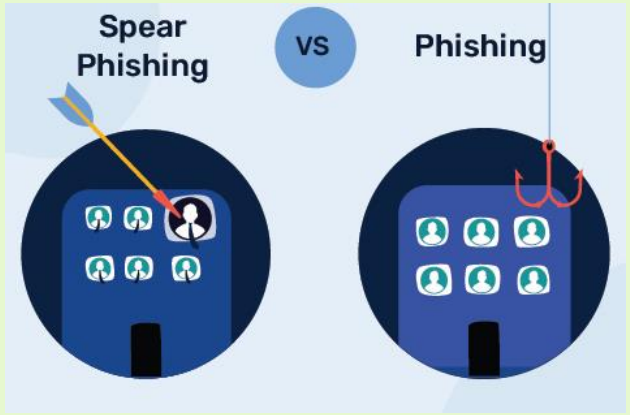
E-mail Phishing

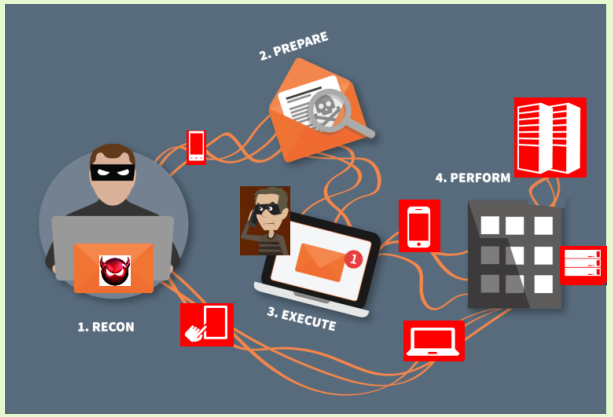
O mais comum é você receber um e-mail estranho, de alguém que você não conhece, com um arquivo anexado.

Spear Phishing – phishing direcionado;

Pretexting - criar uma falsa situação para induzir a vítima a disponibilizar acesso às informações do sistema, geralmente utilizando uma identidade falsa para coagir e intimidar;

Quid Pro Quo - "algo por algo", o *hacker* oferece para sua vítima algo em troca de uma informação;





E-mail Phishing

Esse tipo de técnica é a grande responsável pelos ataques de phishing (pescaria) hoje em dia.

Um ataque desses consiste em enviar um e-mail falso, geralmente para os clientes de algum banco ou instituição financeira, fazendo com que o e-mail pareça ter vindo do próprio banco (algo como <gerencia@meubanco.com.br>).

Alguns dos assuntos contidos nesses e-mails:

E-mail Phishing

“Prezado cliente, por motivos de segurança, pedimos que modifique sua senha de acesso. Clique aqui para fazê-lo.”

“Meus parabéns! O banco MeuBanco acabou de sortear um prêmio de 10.000 reais entre seus clientes e você foi um dos ganhadores. O MeuBanco lhe dá os parabéns, querido cliente. Entre na sua conta agora clicando aqui e receba o seu prêmio.”

E-mail Phishing

Nesses e-mails, existe um link para o site do banco, só que, na realidade, é um site falso, feito para se parecer exatamente como o original e ele realmente engana muita gente.

A seguir, uma imagem de um site clonado feito para se parecer exatamente com o original (o nome do banco foi removido da imagem para fins de resguardo).

Site Falso


- Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Bankline AGÊNCIA CONTA
Abra sua Conta Para Você Personnalité Private Bank Empresas
Conheça o Conta Corrente Investimentos Vida e Previdência Capitalização
PROMOÇÃO
SUAS CONTAS VALEM
PRÊMIOS
Pague suas contas no Caixa Eletrônico, no
contrate o Débito Automático e concorra a
até 14 carros
esperando por você.
VER DE NOVO
Aproveite melhor
Dicas de Segurança
Crédito Consciente
Aprenda a usar o crédito de forma consciente.
SUPERNOVAS
Plano de Pre
Garanta um fut
Invista Já!
Promoção A
Concorra a um
Cadastre-se a
Relações com Investidores Imprensa Notícias e Cotações Cultural Social Oportunidades de Carreira

Pharming

Pharming é um tipo específico de *phishing* que envolve a redireção da navegação do usuário para *sites* falsos, por meio de alterações no serviço de DNS (***D****omain* ***N****ame* ***S****ystem*).

- Neste caso, quando você tenta acessar um *site* legítimo, o seu navegador *Web* é redirecionado, de forma transparente, para uma página falsa.
- ***DNS Spoofing***

E-mail Falso

O e-mail falso ou simplesmente “fake mail” é uma técnica muito utilizada hoje na Internet para se enviar e-mail sem ser identificado.

Bom, pelo menos para o remetente, pois muitas vezes o endereço IP original ainda continua sendo mostrado no e-mail. Quais as vantagens disso para a Engenharia Social?

Como a maioria dos usuários é leigo e nunca iriam conferir o endereço para ver se bate, os engenheiros sociais podem fingir ter vindo de qualquer e-mail.

- https://emkei.cz/

Possíveis Soluções

As estratégias devem ser tanto no nível físico (meio pelo qual o engenheiro social age, seja telefone, pessoalmente ou Internet) quanto no nível psicológico (manipulando as emoções).

Possíveis Soluções

Seria um grande erro focar só no lado físico da coisa, o treinamento dos empregados é essencial.

Você tem que fazer os responsáveis entenderem que de nada adianta investir em softwares e hardwares, visando melhorar a segurança, se não for feito um plano contra a Engenharia Social.

Teste do Google

Verifique se você está apto a identificar casos de *phishing*:

https://phishingquiz.withgoogle.com

Referências Bibliográficas

Segredos do Hacker Ético. Marcos Flávio Araújo Assunção. São Paulo, SP, Brasil. 2008.

Introdução ao Pentest. Daniel Moreno. 1ª Ed. – São Paulo, SP. Novatec, 2015.