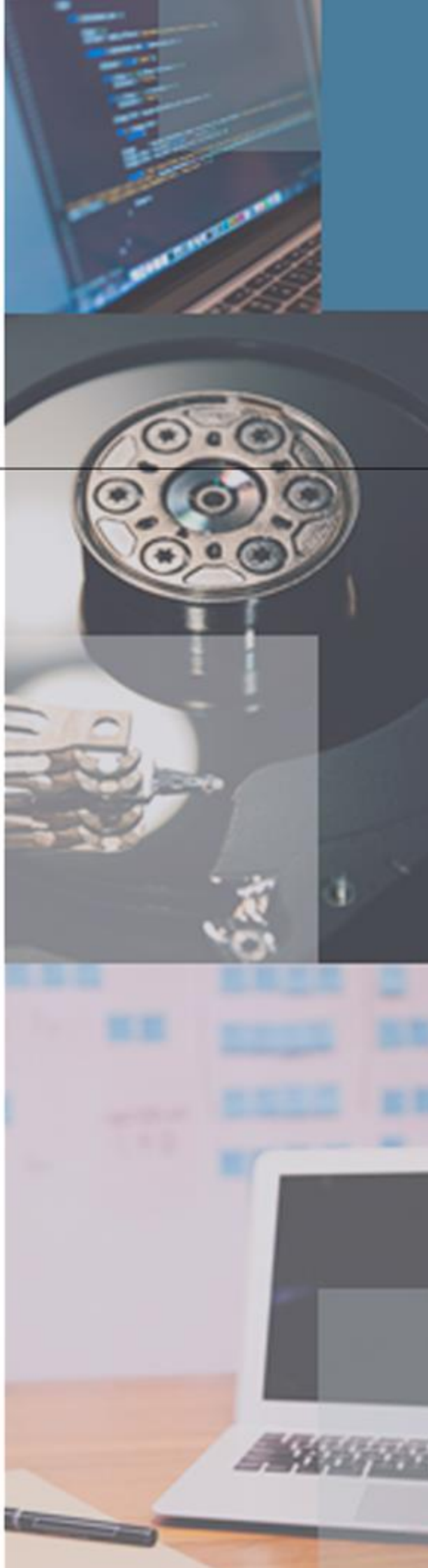
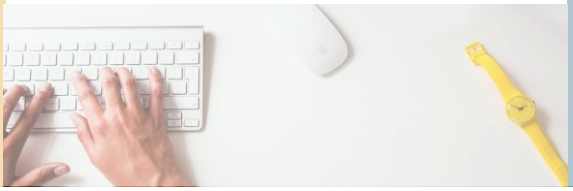
FUNDAMENTOS
DE ETHICAL HACKING

MATERIAL COMPLEMENTAR

Engenharia Social



marcosflavio.com.br



1. Engenharia Social

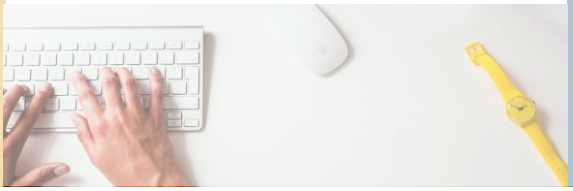
Os engenheiros sociais são pessoas cultas, de um papo agradável e que conseguem fazer com que você caia em suas armadilhas. Se utilizando de meios digitais, telefônicos e até pessoalmente, essas pessoas lhe observam e estudam sem que você perceba. E isso não é algo novo que surgiu com a informática, a décadas os engenheiros sociais vem agindo.

Geralmente existem 3 maneiras básicas de agir:

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

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 os engenheiros 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.

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.



2. Manipulação das sensações

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 e-mail com assuntos bem atrativos como um cartão dizendo “eu te amo”, fotos de supostos amigos esquecidos, informações afirmando que seu e-mail será cancelado, etc.

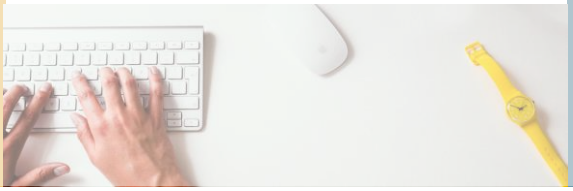
Confiança

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 se oferecer para ajudar um 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 vier com um anexo. Sempre passe o anti-vírus antes. Isso porquê e-mails podem facilmente ser forjados, tome muito cuidado pois é uma das maiores formas de engenharia social. No geral, todos esses fatores fazem com que a sua “resistência” a entregar informações fique mais fraca. Um exemplo abaixo:

Simpatia

Outro grande modo de manipulação. O melhor exemplo de simpatia é no caso das mulheres. É muito mais fácil uma mulher 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 te passar a perna. Abaixo você vê um exemplo:

Culpa

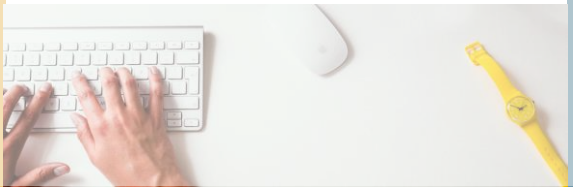
Quando as pessoas se sentem culpadas por algum motivo, são mais propensas a ajudar. Isso não deixa de ser verdade no meio da Engenharia Social. Inflija culpa em alguém e faça essa pessoa lhe ajudar no que você quiser. Dentro de uma empresa, os funcionários mais vulneráveis a essa emoção são os novatos, que estão querendo mostrar serviço.

Medo

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

3. Truques aplicados na informática

Os engenheiros sociais também aplicam vários truques se utilizando da informática, visando obter informações e dados importantes que normalmente não seriam tão facilmente entregues. Ou mesmo fazer com que alguma pessoa pense que está recebendo e-mail de um amigo qualquer com um anexo, quando na realidade é uma ferramenta de invasão (uma porta dos fundos por exemplo) que se for instalada, dará acesso total ao sistema para o invasor. Se você recebesse um e-mail assim de um amigo e seu antivírus nada detectasse (já vimos que é fácil esconder dele esses programas), você executaria o anexo? Pense nisso. Veremos algumas artimanhas desse tipo aqui.



E-mail *Phishing*

A ferramenta mais utilizada da Internet hoje é de longe o e-mail. Nos correspondemos instantaneamente com quem quisermos, na hora que desejarmos.

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:

"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 diretamente na sua conta corrente"

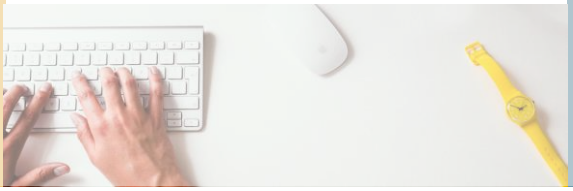
Atualmente muitos bancos não enviam e-mails para os clientes, apenas se esses solicitarem. Os engenheiros sociais são tão caras de pau que muitas vezes colocam isso nos e-mails de *phishing* para gerar confiança. Muitas vezes o cliente não se lembra se ativou ou não o serviço. Nosso primeiro exemplo modificado abaixo mostra isso.

"Prezado cliente, por motivos de segurança pedimos que modifique sua senha de acesso. Clique aqui para fazê-lo. O MeuBanco não envia e-mails aos usuários sem autorização. Se você não deseja mais receber o E-Banking, clique aqui para acessar sua conta e desabilitar o serviço"

Nesse e-mail existe um link para o site do banco, só que na realidade é um site falso. Feito para se parecer exatamente com o original, 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).

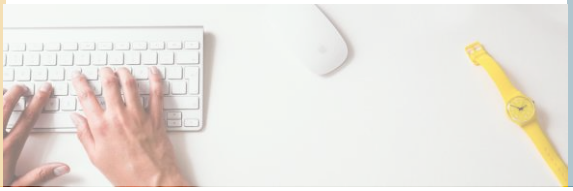
Fonte: *Print Screen* feito por Marcos Flávio A. Assunção.

Esse como muitos outros sites falsos de instituições financeiras, enganam facilmente as pessoas. A mídia muitas vezes se refere aos realizadores de Phishing como hackers. Isso é errado, já que não é necessário um conhecimento técnico para se mandar um e-mail falso e enganar alguém. O que temos aqui simplesmente são engenheiros sociais com péssimas intenções. Veremos como eles conseguem enviar o e-mail de forma anônima, tentando se passar por quem não são.



Assuntos mais comumente utilizados nos e-mails de *Phishing*

TEMA	TEXTO DA MENSAGEM
Cartões virtuais	UOL, *Voxcards*, Humor Tadela, O Carteiro, *Emotioncard*, Criança Esperança, AACD/Teleton.
SERASA e SPC	Débitos, restrições ou pendências financeiras.
Serviços de governo eletrônico	CPF/CNPJ pendente ou cancelado, Imposto de Renda (nova versão ou correção para o programa de declaração, consulta da restituição, dados incorretos ou incompletos na declaração), eleições (título eleitoral cancelado, simulação da urna eletrônica).
Álbuns de fotos	Pessoa supostamente conhecida, celebridades, relacionado a algum fato noticiado (em jornais, revistas, televisão), traição, nudez ou pornografia, serviço de acompanhantes.
Serviço de telefonia	Pendências de débito, aviso de bloqueio de serviços, detalhamento de fatura, créditos gratuitos para o celular.
Antivírus	A melhor opção do mercado, nova versão, atualização de vacinas, novas funcionalidades, eliminação de vírus do seu computador.
Notícias/boatos	Fatos amplamente noticiados (ataques terroristas, *tsunami*, terremotos, etc.), boatos envolvendo pessoas conhecidas (morte, acidentes ou outras situações chocantes).
Reality shows	*BigBrother*, Casa dos Artistas, etc. -- fotos ou vídeos envolvendo cenas de nudez ou eróticas, discadores.
Programas ou arquivos diversos	Novas versões de *softwares*, correções para o sistema operacional Windows, músicas, vídeos, jogos, acesso gratuito a canais de TV a cabo no computador,

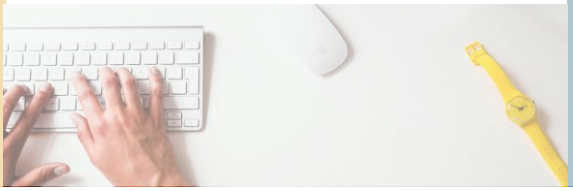


	cadastro ou atualização de currículos, recorra das multas de trânsito.
Pedidos	Orçamento, cotação de preços, lista de produtos.
Discadores	Para conexão Internet gratuita, para acessar imagens ou vídeos restritos.
***Sites* de comércio eletrônico**	Atualização de cadastro, devolução de produtos, cobrança de débitos, confirmação de compra.
Convites	Convites para participação em *sites* de relacionamento (como o *Facebook, Instagram*) e outros serviços gratuitos.
Dinheiro fácil	Descubra como ganhar dinheiro na Internet.
Promoções	Diversos.
Prêmios	Loterias, instituições financeiras.
Propaganda	Produtos, cursos, treinamentos, concursos.
FEBRABAN	Cartilha de segurança, avisos de fraude.
IBGE	Censo.

Fonte*: nic.br*

4. Combatendo a Engenharia Social

Existem algumas recomendações de como se proteger contra os ataques de engenharia social, especialmente no ambiente corporativo. Para começar, as estratégias devem ser tanto no nível físico (meio o qual o engenheiro social age, seja telefone, pessoalmente ou Internet) quanto no nível psicológico (manipulando as emoções). 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 melhora a segurança se não for feito um plano contra a engenharia social.



Você pode criar novas políticas de segurança e um controle maior do contato feito com os funcionários, mas se pegar muito pesado, deixará essas pessoas frustradas e a solução não é 100% eficiente.

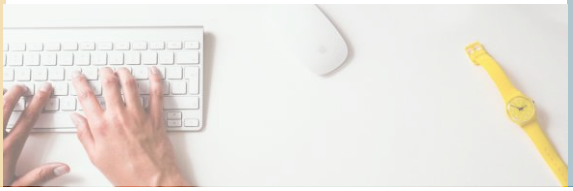
A melhor solução então seria simplesmente treinamento!

Todas as pessoas de uma empresa que lidam com informações importantes então devem passar por um treinamento no qual irão aprender a identificar os tipos de ataques e como reagir a cada um deles. Uma outra ideia interessante é mandar uma espécie de artigo todo mês para os funcionários mostrando novos exemplos de engenharia social e qual a técnica para se proteger deles. Isso vai lembrá-los sempre do perigo.

Combatendo o *Phishing*

Além de combater a Engenharia Social como "um todo", utilizando um escopo mais global, algumas dicas simples podem ajudar fazer com que os usuários não caiam facilmente nos ataques de *Phishing*.

- *Leia atentamente a mensagem. Normalmente, ela conterá diversos erros gramaticais e de ortografia;*
- *Os engenheiros sociais utilizam técnicas para ofuscar o real link para o arquivo malicioso, apresentando o que parece ser um link relacionado à instituição mencionada na mensagem. Ao passar o cursor do mouse sobre o link, será possível ver o real endereço do arquivo malicioso na barra de status do programa leitor de e-mails, ou browser, caso esteja atualizado e não possua vulnerabilidades. Normalmente, este link será diferente do apresentado na mensagem;*
- *Qualquer extensão pode ser utilizada nos nomes dos arquivos maliciosos, mas fique particularmente atento aos arquivos com extensões ".exe", ".zip" e ".scr", pois estas são as mais utilizadas. Outras extensões frequentemente utilizadas por fraudadores são ".com", ".rar" e ".dll";*
- *Fique atento às mensagens que solicitam a instalação/execução de qualquer tipo de arquivo/programa;*



- *Acesse a página da instituição que supostamente enviou a mensagem, seguindo os cuidados apresentados e procure por informações relacionadas com a mensagem que você recebeu. Em muitos casos, você vai observar que não é política da instituição enviar e-mails para usuários da Internet, de forma indiscriminada, principalmente contendo arquivos anexados.*