UNISA - UNIVERSIDADE DE SANTO AMARO

SISTEMAS DE INFORMAÇÃO

DIEGO ESPINOZA

JEAN ALBUQUERQUE

LUIZ FERNANDO SANTANA

MARCIO JUNIO

ENGENHARIA SOCIAL

SÃO PAULO

2013

DIEGO ESPINOZA

JEAN ALBUQUERQUE

LUIZ FERNANDO SANTANA

MARCIO JUNIO

ENGENHARIA SOCIAL

Trabalho de Conclusão de Curso apresentado para obtenção do título de Bacharel em Sistemas de Informação da Universidade de Santo Amaro, sob a orientação do Prof. Marcos Antônio.

SÃO PAULO
2013

DIEGO ESPINOZA

JEAN ALBUQUERQUE

LUIZ FERNANDO SANTANA

MARCIO JUNIO

ENGENHARIA SOCIAL

Trabalho de Conclusão de Curso apresentado para obtenção do título de Bacharel em Sistemas de Informação da Universidade de Santo Amaro – UNISA sob a orientação do professor Marcos Antônio.

Data de Aprovação: ____/____/____

BANCA EXAMINADORA

_____

(Nome do orientador e Titulação)

_____

(Nome do professor e Titulação)

CONCEITO FINAL: _____

Dedicamos este trabalho aos nossos familiares e amigos, que nos deram apoio desde o princípio para que avançássemos em nossa vida pessoal e profissional.

Ao nosso professor orientador Marcos Antônio, que nos ajudou e incentivou, contribuindo muito para o nosso aprendizado.

A todos os professores que dividiram conosco seus ensinamentos.

E acima de tudo a Deus, que nos capacitou para a conclusão desde trabalho e de nossa graduação.

AGRADECIMENTOS

Agradecemos primeiramente a Deus, por nos dar forças para buscarmos nossos sonhos e sabedoria para concluirmos este trabalho e nos manter firmes e confiantes durante o período de Curso.

Aos nossos pais por todo o sacrifício e apoio para a nossa formação, estando sempre presentes ao nosso lado, por nos ensinarem a lutar pelos nossos objetivos e o significado das palavras perseverança e humildade, pois estas serviram como base para que fôssemos capazes de chegar aos nossos objetivos.

Aos nossos Irmãos e colegas de sala, que sempre nos respeitaram e caminharam juntos até o fim desta, que é a primeira de muitas conquistas profissionais que virão.

A todos os professores que fizeram parte desta turma e principalmente ao professor e orientador Marco Antônio por toda a paciência, colaboração, pelo aprendizado, pelas aulas ministradas e principalmente por toda motivação e auxilio.

Agradecemos também a Erica Silva Domingues e Titiane Chamorro pela ajuda na revisão e correção do trabalho.

Obrigado a todos por terem cruzado nosso caminho!

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

EUA	Estados Unidos da América
RG	Registro Geral
CPF	Cadastro de Pessoa Física
CNPJ	Cadastro Nacional de Pessoa Jurídica
OMPI	Organização Mundial de Propriedade Intelectual
ONU	Organização das Nações Unidas
DNS	Domain Name System
TI	Tecnologia da Informação
SPF	Sender Policy Framework
ID	IDentification
IVR	Interactive Voice Response
URL	Uniform Resource Locator
HTML	Hyper Text Markup Language
OCR	Optical Character Recognition
IWR	Information World Review
NET	Forma informal para referenciar Internet
BR	Brasil
SSID	Service Set IDentifier
SAC	Serviço de Atendimento ao Consumidor
IP	Internet Protocol
CD	Compact Disc
DVD	Digital Versatile Disc
HD	Hard Disk
CEO	Chief Executive Officer
ART	Antigo
SOC	Security Operations Center
USB	Universal Serial Bus
TV	Televisão
SE	Social Engineer
PNL	Programação Neurolinguística

CFTV	Circuito Fechado de TV
PLS	Projeto de Lei do Senado
PMDB	Partido do Movimento Democrático Brasileiro
CE	Ceará
PT	Partido dos Trabalhadores
AC	Acre
PDT	Partido Democrático Trabalhista
MT	Mato-Grosso
TLD	Top-Level-Domain
SET	Social Engineer Toolkit

SUMÁRIO

RESUMO

O presente trabalho de conclusão de curso aborda a engenharia social e explicar detalhadamente algumas das ferramentas, os meios de aplicação, as fontes de coleta de informações, as técnicas e os indivíduos que fazem o uso destas técnicas, que tem como objetivo comprometer a segurança da informação de organizações e de pessoas comuns.

Empresas investem constantemente na implantação e modernização de sistemas de segurança, com softwares e hardwares cada vez mais avançados, mas quase não há investimento no fator humano, deixando assim grandes vulnerabilidades para as práticas da engenharia social. Não existe uma forma cem por cento efetiva de proteção para a engenharia social, porém, pontos como treinamento de funcionários, elaboração e implantação de um plano de segurança, cuidado e atenção com informações confidenciais, etc. ajudam a minimizar os riscos.

No Brasil, não existe uma legislação especifica para as práticas ilegais da engenharia social, mas grande parte das atividades ilícitas se enquadram em algum artigo da constituição.

ABSTRACT

The following thesis talks about the social engineering and explain in details some of the tools used, means used, source of information, techniques and who uses it, with the goal of compromise the company's and people's information security.

Companies invest constantly in the implantation and modernization of security systems, with more advanced software and hardware, but the human factor is almost always forgot, letting vulnerabilities that can be explored with social engineering. There is not a 100% effective way to prevent social engineering attacks, but is possible to minimize the risks with employee trainings, security plans and more attention with the confidential information.

In Brazil, there is not specific laws that can be applied to the social engineering activities, but almost all of the illicit activities are applied to some existing law.

OBJETIVO

O trabalho foi elaborado com o objetivo de despertar o interesse e a conscientização das pessoas e organizações para as práticas de engenharia social, através de uma abordagem simplória onde não serão aprofundados códigos e protocolos técnicos, mas partindo do princípio de que a maioria dos usuários não compreende ou são leigos neste assunto, visando que assim o leitor possa reconhecer os perigos eminentes desta metodologia e não ser mais uma vítima dessas pratica tão comum nos dias de hoje, apreendendo também algumas maneiras de prevenção.

INTRODUÇÃO

Antes de começar um estudo aprofundado em engenharia social, que será o tema central, é necessário um estudo básico sobre um assunto muito importante:
O que é segurança da informação?

A informação pode existir em diversos formatos, pode ser impressa, escrita, armazenada e transmitida eletronicamente, exibida em filmes ou falada em conversas. Seja qual for a forma em que é apresentada, compartilhada ou armazenada, é recomendado que a mesma fosse sempre protegida adequadamente.

Segurança da informação é a proteção da informação contra vários tipos de ameaças e ataques, para garantir a continuidade de um negócio, minimizar possíveis riscos, maximizar retornos sobre os investimentos entre outros objetivos, e pode ser obtida com a adoção de um conjunto de controles, incluindo políticas de segurança, processos, procedimentos, estruturas organizacionais, software e hardware.

Esses controles precisam ser estabelecidos, implantados, monitorados, analisados e melhorados onde e sempre que necessários, para garantir os três pilares da segurança da informação, que são a confidencialidade, integridade e a disponibilidade.

Visando uma melhor compreensão do tema abordado, o trabalho de conclusão de curso foi divido em oito capítulos. No primeiro capitulo são abordados temas como a discussão geral de engenharia social, os fatores motivacionais para a prática desta ciência e as categorias de engenheiros sociais. O segundo apresenta as diferentes fontes e formas para se coletar informações para a realização de ataques futuramente. Já os capítulos três e quatro, demonstram as principais técnicas e suas formas de aplicação, além de exemplos de ataques reais, formas de como se prevenir dos mesmos. Seguindo com o raciocínio o capitulo cinco, são tratados os aspectos psicológicos envolvidos com engenharia social, onde são vistos fatores como persuasão, autoridade e amizade. Por fim os capítulos seis, sete e oito, irão tratar respectivamente de temas como as ferramentas usadas para realizar ataques, as leis e aplicações em caso de uso mal-intencionado da engenharia

social, e por fim são apresentadas algumas prevenções e dicas para do que ser feito para combater se proteger e reagir mediante a um ataque.

1 Discussão Geral

1.1 Definições de Engenharia Social

Engenharia Social pode ser definida como o ato de influenciar, manipular ou enganar uma pessoa ou um grupo de pessoas para alcançar uma meta. Essa meta pode ser dar acesso a lugares restritos ou passar informações confidenciais. Pode ser descrita também como uma forma de conduzir o “indivíduo alvo” a fazer algo, que ele normalmente não faria sem a influência do engenheiro social, como obter informações que podem ou não ser confidenciais, ganhar acesso a lugares restritos, realizar fraudes, invadir computadores ou entrar em locais sem autorização.

Geralmente tido pela sociedade como algo ruim ou de cunho duvidoso, a engenharia social pode e é utilizada de maneira positiva por pessoas comuns como pais, cônjuges, terapeutas, psicólogos, professores, líderes, palestrantes, políticos, vendedores, etc. Os princípios da engenharia social são vistos e utilizados na vida pessoal, mesmo que sem consciência ou vontade. O termo normalmente é entendido como base para invasões a locais e computadores, coletar informações, trapaças e fraudes.

1.2 Fatores motivacionais para praticas em engenharia social

Seis fatores principais motivacionais podem ser listados para realização de crimes cibernéticos, onde também estão inclusos as práticas de engenharia social.

As seis principais motivações são:

Fatores monetários (dinheiro);
Entretenimento;
Ego;
Impunidade;
Entrada em um grupo social;
Manter status dentro de um grupo.

Algumas destas motivações são comuns em quaisquer sociedades, pois pessoas geralmente querem ganhar mais dinheiro e serem aceitas em grupos. É

possível acrescentar a esta lista aspectos como conhecimento, vingança ou até curiosidade.

Segundo uma divisão de necessidades proposta pelo psicólogo americano Abraham Maslow, que ficou conhecida como a pirâmide de Maslow, onde é apresentado um conjunto de cinco necessidades que todos os indivíduos buscam ao longo de suas vidas. Maslow defendia a ideia de que, os indivíduos deveriam "escalar" a hierarquia para a sua auto-realização.

Os fatores motivacionais mais comuns para as práticas de engenharia social podem ser encontrados na Pirâmide de Maslow.

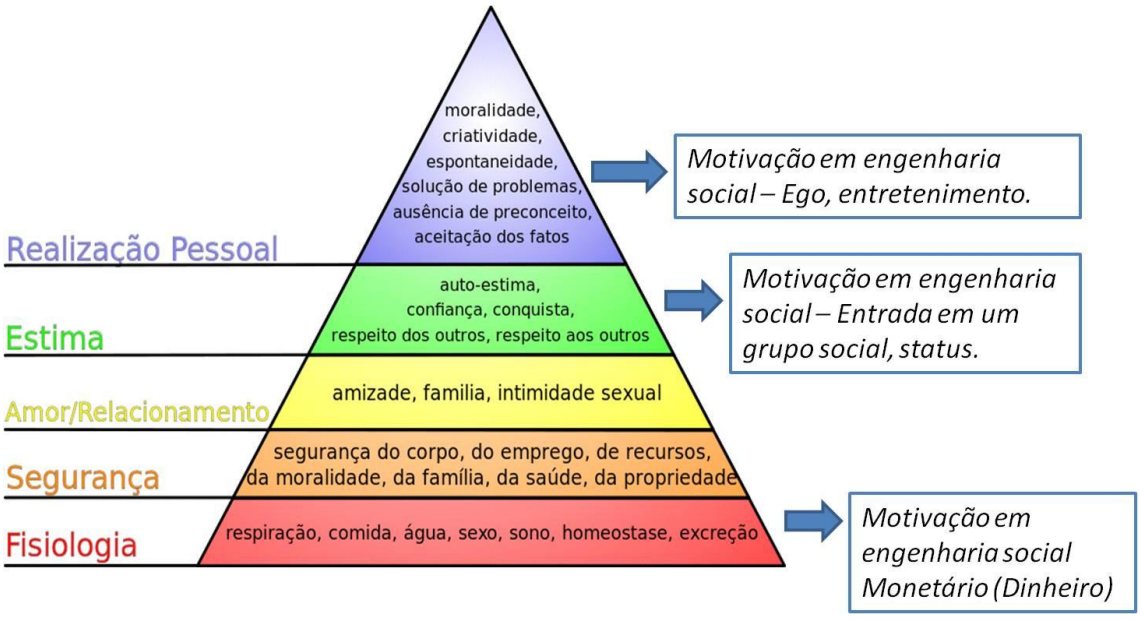

Figura 1: Pirâmide de Maslow. Fonte: Wikipedia Commons.
http://commons.wikimedia.org/wiki/File:Maslow%27s_hierarchy_of_needs.png

Outras motivações primordiais para o uso da engenharia social que não foram enquadradas na pirâmide de Maslow são: eficiência dos ataques e impunidade.
Segundo Carlos Arruda, gerente de pesquisas, desenvolvimento e operações da In2Sec[1], a alta probabilidade de sucesso no uso de engenharia social se torna um fator motivacional importante para uso desta pratica.

[1] In2Sec. Empresa brasileira especializada em inteligência aplicada à segurança da informação.

Segundo o site trustsign[2] "O *ser humano é um mix de experiência, motivação, crença e conhecimento, com tudo isso podemos ter ou não pessoas suscetíveis à engenharia social, e hoje mais de 95% o são[...]*".

1.3 Categorias de engenheiros sociais

Engenheiro social é o termo dado, voluntariamente ou não, às pessoas que utilizam técnicas da engenharia social. Existem diferentes técnicas para aplicação de ataques e diferentes tipos de engenheiros sociais, que podem ser divididos em diferentes categorias.

1.3.1 Hackers

O hacker é um profissional da área de Segurança de Informação que utiliza seu amplo conhecimento técnico para identificar e explorar vulnerabilidades em um sistema ou rede, visando a melhoria dos mesmos.

O cracker, diferentemente do hacker, utiliza seus conhecimentos técnicos com o intuito de invadir e danificar sistemas e redes e para seu próprio benefício. Crackers quebram códigos e senhas e invadem redes ou sites para roubar ou alterar informações, sempre com um objetivo malicioso.

Ambos podem ser considerados engenheiros sociais, pois utilizam técnicas de engenharia social para a realização de ataques, aumentando as chances e potencializando os danos. Muitas pessoas não sabem a diferença entre hacker e cracker, rotulando ambos como criminosos.

1.3.2 Penetration Testers

Penetration Testers(Testadores de Penetração, em tradução literal) são profissionais da área de segurança que realizam testes e procuram invadir a rede alvo, tanto pelo acesso físico quanto como pelo acesso virtual. Normalmente são contratados por empresas para que seja feita uma avaliação do nível de segurança de seus sistemas.

---

2 Disponível em: http://www.trustsign.com.br/blog/95-das-pessoas-sao-suscetiveis-a-engenharia-social/

Para que estes profissionais alcancem seus objetivos, eles realizam testes de penetração que simulam um ataque real, visando encontrar e explorar falhas na rede. Para estes ataques são utilizadas ferramentas especializadas em encontrar e explorar vulnerabilidades, como o Veracode (Ferramenta de análise estática e analise dinâmica usada em testes de penetração).

Estes profissionais também podem ser considerados engenheiros sociais porque utilizam técnicas e ferramentas de engenharia social para tentar acessar fisicamente o local.

1.3.3 Espiões

Através do treinamento recebido, espiões são capazes de se infiltrar em lugares, se passar por pessoas e invadir sistemas a fim de descobrir as informações que desejam.

Técnicas e ferramentas de espionagem também podem ser utilizadas através da internet ou telefone. Ferramentas como escutas telefônicas, rastreadores via satélite, softwares como Spymaster, BRMonitor e KidLogger são utilizados para coletar informações.

1.3.4 Ladrões de identidade

O roubo de identidade em engenharia social envolve a utilização de RG, CPF, CNPJ, números de conta bancaria endereço, datas de nascimento e qualquer outra informação pessoal que possa ser utilizada para se passar por outra pessoa ou instituição. Os ladrões de identidade são engenheiros sociais especializados nas técnicas pretexting, phishing e personificação.

Segundo a OMPI[3], o roubo de ciberidentidade, ou também conhecida como identidade virtual, "aumentou 5% em 2012, chegando ao registro sem precedentes de 2.884". Os números foram anunciados pelo diretor Francis Gurry, na agencia da ONU[4] em Genebra, Suíça em 28 de fevereiro de 2013.

[3] OMPI: Organização Mundial da Propriedade Intelectual
[4] ONU: Organização das Nações Unidas

Francis Gurry revela que "as áreas nas quais o roubo de ciberidentidade é maior, de acordo com os casos, são as de vendas varejistas, de moda, de bancos e finanças".

1.3.5 Funcionários Insatisfeitos

Funcionários insatisfeitos também podem ser classificados como uma categoria de engenheiro social. Isso porque um funcionário descontente, pode usar o seu conhecimento interno sobre a empresa para acessar dados confidencias enquanto trabalha, podendo assim usar as informações contra a empresa futuramente ou abrir vulnerabilidades para que outros engenheiros sociais possam realizar ataques.

Os principais motivos para que o funcionário fique descontente com a organização onde ele trabalha é a desvalorização, má remuneração e acumulo de funções.

Normalmente quando um funcionário está descontente com a organização, o mesmo procura desestimular os demais funcionários, causando um mal estar no ambiente de trabalho. Algumas vezes isso pode ocorrer involuntariamente, porém o simples fato de procurar e compartilhar a sua insatisfação com os colegas de trabalho pode acabar gerando o desconforto interno.

Características como baixa produtividade, mau comportamento, foco nos pontos negativos, postagens negativistas com relação ao trabalho em redes sociais e até mesmo roubo podem ser pontos a serem observados para identificar funcionários descontentes.

As empresas possuem informações confidenciais que não podem ser reveladas para toda a organização. Algumas destas informações incluem propriedade intelectual, organogramas e eventos da empresa, mediante isso, um dos grandes problemas de funcionários descontentes, é que por muitas vezes como forma de protesto a insatisfação com a organização, eles acabam se apropriando ou compartilhando estas informações com pessoas que não são funcionários.

1.3.6 Governos

A engenharia social é utilizada por governos para diversos objetivos, como influenciar a opinião pública, sendo feito por políticos ou agências governamentais.

Estas técnicas de engenharia social visam manipular o maior número de pessoas, através de leis, regulamentos e campanhas de marketing, fazendo com que o cidadão esteja dentro de um padrão.

1.3.7 Pessoas Comuns & Profissionais

Como citado anteriormente na definição geral de engenharia social, o uso das técnicas de engenharia social não se restringe apenas aos especialistas no assunto, todos já fizeram uso de alguma destas técnicas.

Crianças utilizam técnicas para manipular as emoções de seus pais, conseguindo o que desejam, no momento que desejam.

Os pais por sua vez, fazem o uso da engenharia comparando e despertando em seus filhos um sentimento de vergonha ou culpa. Exemplos clássicos como “homem não chora” ou “azul e cor de menina e rosa é cor de menina”, são frases que normalmente são ditas as criança e influenciam diretamente nas atitudes e pensamentos das crianças.

Profissões como advogados, engenheiros, diretores, médicos, psicólogos, professores, entre outras profissões, utilizam uma ou mais técnicas de engenharia social, como por exemplo, persuasão e influência.

2 Coleta de informações

Existem várias formas de conseguir informações de uma empresa ou pessoas, as mais utilizadas são o uso do telefone, buscas na internet ou até uma invasão física ou aos sistemas de uma empresa ou residência.

Para o engenheiro social quaisquer informações são uteis, não importando como elas foram obtidas.

Assim como as informações são recursos ilimitados, as fontes de coletas utilizadas por engenheiros sociais para obtê-las também são.

Existem duas fontes de coleta de informações, que podem ser descritas como tradicionais e não tradicionais.

2.1 Fontes de informações Tradicionais

As fontes tradicionais são fontes de informações que estão disponíveis publicamente na internet. Podendo ser obtidas a partir das seguintes fontes:

2.1.1 Pesquisas

Uma pesquisa é uma maneira muito fácil e útil de conseguir boas informações. Assim como uma pesquisa para um trabalho escolar, os engenheiros sociais realizam pesquisas sobre seus alvos antes de atacá-los. Como toda boa pesquisa, é necessário definir o objetivo central a fim de manter a mesma focada. Ter um objetivo claro ajuda a determinar quais informações serem relevantes e quais deveram ser ignoradas.

2.1.2 Telefone

Pode ser considerado uma “arma” muito perigosa se utilizada por um engenheiro social, pois proporciona o anonimato. Mesmo com toda tecnologia de rastreamento e identificadores de chamadas, é muito comum ataques de engenharia

social utilizando o telefone. Com apenas um telefonema, pode se conseguir informações valiosíssimas sobre uma empresa, pessoa ou entidade.

2.1.3 Sites corporativos

Podem oferecer grande variedade de informações de uma empresa. Nestes sites é possível encontrar informações do histórico da empresa, sua linha de produtos e serviços, links para sites internos ou externos, quantidades de funcionários, vagas em aberto, faturamento, telefones de contato e em alguns casos é possível até conseguir informações para contato com diretores.

2.1.4 Redes sociais ou Blogs

Redes sociais são utilizadas pelas empresas e pessoas para interagirem com amigos, clientes e fornecedores, porém por meio das informações postadas pessoas mal intencionadas conseguem dados que podem ser utilizados para cometer atos criminosos.

Nas redes sociais são divulgadas informações do seu cotidiano, eventos, lançamentos de novos produtos ou até mesmo informações de ferramentas utilizadas.

Usando técnicas de Engenharia Social, desenvolvedores de malwares [5] usufruem das redes sociais para disseminar códigos maliciosos.

Um exemplo conhecido é o cavalo de tróia chamado Koobface, que tem utilizado mensagens atrativas para chamar a atenção dos usuários do Facebook, infectando os usuários e criando uma rede zumbi de computadores que podem ser controlados de qualquer lugar do planeta pelos criminosos. Outra ameaça conhecida é o Boonana, que consegue se propagar por aplicativos Java quando o usuário visita uma página maliciosa executa o programa.

Abaixo se encontram cinco razões para as redes sociais serem fontes de informações muito valiosas.

[5] Palavra em inglês derivada de Malicious Software, que significa software malicioso em tradução literal.

- Pesquisas pelo nome da empresa podem trazer nomes de funcionários, cargos e telefone.
- Postagens de funcionários podem dar pistas para criminosos descobrirem suas senhas, atividades e cargo.
- A utilização de localização em aplicativos ou redes sociais torna público o local que a pessoa está e os locais que a pessoa que costuma frequentar. Utilizando estas informações o engenheiro social poderá se passar por um conhecido da pessoa ou procurar uma forma para entrar na empresa que ela trabalha.
- Concursos ou postagens falsas que circulam no Facebook e solicitam vários dados ou postagens de funcionários podem ser usadas para redefinir senhas por meio de perguntas como: qual o nome da sua mãe, qual o nome do seu animal de estimação, qual sua data de nascimento, entre outras.
- Por meio das páginas da empresa nas redes sociais o engenheiro social pode descobrir quando surgir uma vaga e se candidatar para conseguir informações sobre a empresa e até se infiltrar.

2.1.5 Dados de domínio público

Outra forma de coleta de informações tradicionais são os dados de domínio público. Regulamentada em novembro de 2011 a Lei Federal 12.527, é conhecida como a Lei de Acesso à Informação, que tem como objetivo garantir aos cidadãos o acesso à informação sobre as ações públicas. Desta forma, todas as informações de projetos, gastos, receitas, balancetes entre outros ficam à disposição de todos, visando uma administração clara e honesta. Essas informações podem ser obtidas pelo site da prefeitura, ou até mesmo o site do governo federal.

2.2 Fontes de informações Não tradicionais

Fontes de informações não tradicionais são aquelas que aparentemente não tem importância ou não são públicas:

- Essas fontes de informações não tradicionais podem ser por meio de uma conversa com um especialista da atividade ou do assunto da empresa que o engenheiro social irá atacar.
- Outra fonte de informações não tradicionais pode ser frequentar os mesmos lugares que os funcionários da empresa frequentam ou realizar atividades iguais ou parecidas com eles, visando coletar informações e aprender costumes. Esta aproximação oferecerá oportunidades para escutar diálogos entre os funcionários, conversar com eles ou até mesmo copiar sua identificação de acesso a empresa.
- Dumpster diving (Mergulhar no lixo, em tradução literal): Técnica utilizada para vasculhar o lixo, visando também à coleta de informação.

3 Técnicas de Engenharia Social e Coleta de Informações

3.1 Definição de Elicitação

Elicitação é a técnica de obtenção de informações, usada para a análise e construção ou para melhorar um sistema, um produto, um processo de trabalho entre outros exemplos. Na área da engenharia social e espionagem, elicitação é extração sutil de informações durante uma conversa aparentemente normal e inocente.

É usada para conhecer melhor as pessoas, avaliar e verificar como desenvolver relacionamentos. Pessoas usam elicitação a todo o momento, analisando as possibilidades, se podem e como podem criar um relacionamento com outra pessoa. Isso é feito diariamente por todos ao conversar, ouvir e fazer perguntas e também é conhecido como socialização.

Na engenharia social a elicitação assume o papel de extrair informações significativas e relevantes do indivíduo alvo, sem transparecer que a coleta de informações está sendo feita ou mesmo o desejo por aquelas informações, melhorando assim as chances de sucesso no seu objetivo final. A experiência com socialização, principalmente com pessoas desconhecidas, melhora as habilidades e aumenta o conhecimento do processo de elicitação, ajudando a levantar melhor as informações desejadas.

O simples ato conversar, compartilhar informações e fazer perguntas bem colocadas, se feitas de forma correta, parecendo inocente e casual, não deve provocar uma reação defensiva ou negativa no indivíduo alvo. Isso permite uma melhor investigação, aumentando também a chance de obtenção de informações mais especificas.

Não há maneiras simples de se prevenir contra a elicitação, deve-se sempre estar atento a qualquer resposta dada e pergunta feita, principalmente por desconhecidos e nunca falar, escrever ou divulgar de qualquer maneira informações confidenciais, mesmo que para pessoas de confiança.

3.1.1 Meios de Elicitação

Existem alguns meios de elicitação conhecidos e utilizados por engenheiros sociais, abaixo se encontram alguns deles:

3.1.1.1 Internet

Adquirir informações por meios eletrônicos é uma forma de ataque viável e eficaz. E-mails falsos e sites mal-intencionados que enganam os usuários e os fazem fornecer suas informações pessoais, como credenciais, número de conta bancária ou RG/CPF são excelentes exemplos de como extrair informações utilizando a internet.

E-mails com domínio forjado com técnicas de E-mail Spoofing(e-mail forjado, em tradução literal) ou criado para parecer com outro domínio verdadeiro aumentam a credibilidade com o alvo.

3.1.1.2 SMS, e-mails e aplicativos de mensagens instantâneas

Mensagens instantâneas podem ser utilizadas por pessoas sem experiência em atuação ou que mentem sobre sua identidade, aparência ou localização. A abordagem pode ser feita de várias maneiras diferentes e com diferentes pretextos, como amizade ou relacionamento, possibilitando esconder de maneira melhor o objetivo final, que é de coletar informações. A vantagem da não rastreabilidade e velocidade das mensagens permitem ao engenheiro social se comunicar com vários alvos ao mesmo tempo e que estão à grande distância. O anonimato permite e ajuda na utilização de pretextings, sendo possível até enviar fotos editadas ou de outras pessoas para aumentar a credibilidade. Aplicativos de mensagens instantâneas são utilizados em larga escala, a maioria está disponível para celulares (Skype, Whatsapp, WeChat, etc.) e alguns possibilitam até encontrar usuários próximos(WeChat).

3.1.1.3 Pesquisas de opinião

A utilização de pesquisas de opinião é uma ótima maneira de elicitação. Pesquisas são utilizadas para saber opiniões, gostos, profissões e outras informações de pessoas que trabalham ou frequentam um local, permitindo levantar um perfil de personalidade dos frequentadores e muitas vezes dos funcionários de uma empresa ou estabelecimento. A abordagem deixa explícito que se deseja saber informações daquela pessoa, fazendo com que experiência e habilidades de atuação não sejam necessárias, permitindo assim um bom resultado apenas com uma prancheta para anotação. Pesquisas podem ser feitas, por exemplo, em frente de empresas alvo para descobrir os gostos comuns ou locais frequentados pelos funcionários, que será utilizado futuramente para planejar um ataque mais efetivo.

3.1.1.4 Conversas

Conversas onde se é utilizado elicitação devem ser totalmente descontraídas. É extremamente importante não deixar, em momento nenhum, que o alvo perceba ou suspeite do desejo por suas informações ou da finalidade daquela conversa. Quando não existe um relacionamento com o alvo, a abordagem e as perguntas devem ser realizadas de forma mais sutil, evitando uma reação defensiva ou negativa, não desejada.

Exemplo: Para iniciar uma conversa com uma secretária desconhecida, ao se olhar para a foto dela com seu filho. Uma pergunta do tipo “Qual o nome do seu filho?” pode parecer muito intrusiva e causar uma reação defensiva.

Recomenda-se uma pergunta menos invasiva, normalmente seguida de um elogio, como por exemplo: “Este é seu filho mais novo? Muito bonito!”. Esta pergunta tem mais chances de causar uma resposta mais completa que pode levar a continuidade da conversa e adquirir mais informações.

3.1.2 Preloading

O preloading (Pré-Carregamento, em tradução literal) é uma parte de um ataque de engenharia social. É o ato começar a influenciar o alvo antes de

realmente tentar coletar as informações, aumentando a confiança e tornando-o mais propenso a lhe fornecer as informações necessárias. Pode ser comparado com um teaser (trailer de 15 segundos) ou um vídeo promocional de um filme, que mostra cenas pré-selecionadas usadas para influenciar a opinião da audiência sobre o filme, com palavras como “O melhor filme já feito!”.

3.1.3 Tipos de perguntas

Existem diferentes tipos de perguntas que devem ser usadas no momento certo.

Comparando as perguntas: "Hoje está quente, não acha?" e "O que você acha do tempo hoje?". Pode-se notar facilmente a grande diferença entre elas. A segunda pergunta obriga uma resposta do alvo que vai fornecer informações muito mais detalhadas sobre essa pessoa, como "Acho que hoje muito quente, mas gosto assim".

A primeira quase obriga o indivíduo alvo a dizer apenas "Sim" ou "Não está tão ruim” enquanto a segunda pode provocar uma resposta muito mais valiosa.

3.1.3.1 Perguntas Abertas

Perguntas abertas são perguntas formatadas especialmente para exigir mais diálogo e explicação sobre o assunto e não podem ser respondidas com um simples “sim” ou “não”, estas perguntas criam um sentimento de proximidade e relacionamento devido a necessidade de mais ações por parte do alvo, facilitando no processo de coleta de informações. Algumas vezes também são elaboradas de maneira que se parece com uma afirmação que precisa de resposta.

Quando feitas de maneira correta, aprende-se muito sobre as perspectivas, valores e metas de uma pessoa, bem como pequenos pedaços de informações interessantes sobre eles que podem ser usados mais tarde, para formar uma idéia ou uma informação que não foi dita por completo.

Apesar de tudo, pessoas podem se sentir desconfortáveis quando são alvo de uma pergunta aberta, muitas vezes por não entender aonde se quer chegar ou simplesmente por não querer responder por ser uma informação pessoal ou de um

assunto onde o alvo não quer se aprofundar. Também podem resultar em respostas longas e inúteis no ponto de vista de um engenheiro social. As perguntas abertas devem ser específicas, mas sem demonstrar as reais intenções por trás dela.

3.1.3.2 Perguntas Fechadas

Perguntas fechadas são tipos de perguntas elaboradas de uma maneira que garante um maior controle da conversação, permitindo a pessoa direcionar a conversação de maneira mais efetiva. Basicamente são perguntas onde o respondente deve escolher a resposta entre as opções fornecidas pelo questionador. Normalmente são utilizadas para testes e quando respostas diretas e focadas são desejadas.

Exemplos:

- O câmbio do seu carro está com problemas?
- Você conseguiu chegar a tempo de embarcar no seu vôo?
- Seu filho já tem 18 anos?

Algumas perguntas fechadas podem causar respostas confusas ou errôneas devido à falta de alternativas para resposta, isto acontece quando a pergunta faz uma suposição injustificada ou controversa limitando a resposta.

Exemplo: Você já parou de roubar dinheiro da sua empresa?

Esta pergunta pressupõe que o respondente já roubou dinheiro da sua empresa no passado e questiona com uma pergunta fechada se você já parou ou não de roubar.

3.1.3.3 Perguntas Neutras

Perguntas Neutras são perguntas onde não há direcionamento ou orientação para um assunto ou caminho específico e permite ao respondente criar e seguir sua própria linha de raciocínio, podendo ser respondida de qualquer maneira.

3.1.3.4 Perguntas Influentes / sugestivas

Perguntas Influentes ou sugestivas como também são conhecidas, são perguntas que fazem uma suposição ou insinuam que uma situação ou acontecimento, seja ela real ou irreal e que favoreça o questionador, de forma explicita com o objetivo de levar o indivíduo alvo a responder da maneira desejada pelo questionador. É uma das técnicas utilizadas em um interrogatório sugestivo e, devido a sua natureza manipulativa, este tipo de pergunta é proibida em julgamentos com testemunhas em vários países do mundo. Algumas vezes também podem ser respondidas com um “sim” ou “não”.

No escopo de engenharia social, são usadas para confirmar informações sobre o indivíduo alvo, como seus gostos, o que faz ou fez em certa data e hora, sua personalidade, etc. Perguntas influentes só devem ser feitas após um bom relacionamento com o indivíduo alvo ter sido criado, caso contrário existe o risco de finalização do contato por parte do respondente.

3.1.3.5 Perguntas Pretensiosas

Perguntas pretenciosas são uma ótima ferramenta para deixar uma pessoa a vontade ao se presumir coisas sobre ela, sobre suas ações ou seus pensamentos. Exemplo: “Quantos documentos você já roubou de sua empresa de uma vez só?” Essa pergunta presume que a pessoa já roubou algum documento ou outras coisas e a deixa mais à vontade na situação, pois ela não tem que admitir que fizesse aquilo. Para evitar que o alvo perceba independentemente da resposta, o questionador precisa agir com naturalidade.

3.1.4 Pontos Importantes

Para ter sucesso com a elicitação, devem-se levar em consideração alguns pontos importantes:

- É essencial saber como se comunicar e entender o funcionamento da comunicação interpessoal.
- Criar um vínculo ou um relacionamento com o "indivíduo alvo" é fundamental.

- Saber fazer perguntas inteligentes que trarão respostas utilizáveis. Perguntas que podem ser respondidas com um simples "Sim" ou "Não" não são boas perguntas e devem ser evitadas.
- Muitas perguntas podem fazer com que o alvo interrompa a conversa ou interação e poucas perguntas podem fazer a pessoa se sentir desconfortável;
- Sempre usar as respostas dadas para formular as próximas perguntas de maneira mais eficiente.
- Usar uma abordagem que leve a perguntas diretas e restritas, para obter mais informações

Exemplo: Perguntas Neutras -> Perguntas Abertas -> Perguntas Fechadas -> Perguntas muito direcionadas (como último recurso).

- Perguntas com "por que" normalmente colocam o indivíduo alvo numa posição defensiva pois exigem explicações e motivos mais aprofundados, isto diminui as chances de sucesso na aquisição da informação desejada. Por outro lado, caso se esteja em uma posição em que é necessário enfrentar o alvo de maneira mais direta, perguntas deste tipo são muito úteis.
- Deve-se aprender a ser adaptável ao ambiente, a comunicação deve ser feita para se ajustar ao ambiente e situação em que se encontra.
- A comunicação deve coincidir com o pretexto usado, para evitar parecer suspeito ou até mentiroso. Por exemplo: Se o alvo é um membro da equipe de TI e você diz ser da área de TI, então você precisa conhecer entender e ser capaz de conversar sobre o assunto.

3.2 Pretexting

O Pretexting (Pretexto, em tradução literal) pode ser descrito basicamente como um álibi, um contexto ou um cenário que seja, de preferência, complexo e bem embasado, criado pelo engenheiro social para apoia-lo em um ataque. Para que o “ataque” de engenharia social seja feito de maneira eficiente é necessário, antes de tudo, que o Pretexting seja criado.

Na criação do Pretexting, são necessárias várias informações, sendo que algumas delas não podem ser criadas ou inventadas e devem ser coletadas diretamente do ambiente real onde o ataque ou a infiltração irá ocorrer. Informações

como nome, profissão, cargo, tempo e colegas de trabalho, telefones para contato, cartão de apresentação, vestimenta, endereço da empresa, contato do gerente ou supervisor, horários e nomes de funcionários do local, horários de troca de turno de seguranças, locais vigiados por câmeras, entre outras informações, são necessárias para a criação de um Pretexting bem sucedido.

Para coleta das informações deve haver uma investigação de toda a estrutura de recursos físicos e humanos, além de habilidades de atuação para garantir a postura de uma pessoa que é quem diz ser. Deve-se também planejar planos de fuga e desculpas caso algum problema ocorra ou alguém descubra a farsa.

O Pretexting não é uma técnica exclusiva de engenheiros sociais, é utilizada por profissionais de várias áreas como vendas, medicina, advocacia, terapêutica e principalmente psicológica. Essas profissões tendem a criar um pretexting para que seus clientes se sintam mais confortáveis para expor seus problemas e necessidades.

Não é possível se prevenir contra um pretexting bem feito sem a utilização de tecnologia e processos de segurança de acesso rigorosos. Registro de RG ou CPF, fotos, equipamentos, impressões digitais, reconhecimento ocular, etc. são meios eficientes de segurança, mas não são impossíveis de burlar.

3.2.1 Princípios Básicos

Princípios básicos na utilização do Pretexting:

- Quanto mais pesquisa for realizada maior será a chance de sucesso;
- O Pretexting deve envolver atividades e interesses do alvo;
- Todos os cenários possíveis devem ser planejados cuidadosamente;
- Treinar e praticar todas as abordagens que serão aplicadas;
- Nunca limitar as investigações em áreas ou pessoas específicas, deve-se saber de tudo que ocorre no local alvo;
- Naturalidade e simplicidade aumentam a chance de sucesso do Pretexting/ Atuação é essencial, todas as atitudes devem ser totalmente naturais durante o ataque;
- Os pretextos e explicações devem passar segurança. A desconfiança pode destruir todo o plano;

- É necessário conhecer o nível de conhecimento e experiência que o indivíduo alvo possui;
- Saber das leis e legislações locais ajuda a evitar problemas com a justiça;
- Gravar o Pretexting ou a tentativa para análise futura é uma ótima ferramenta de aprendizado, principalmente em ataques com ligações telefônicas;
- Utilizar disfarces que se encaixem com a situação, horário ou época.

Exemplo: Repórteres em operações policiais ou acidentes.

Pontos que se deve evitar:

- Não repetir os pretexting muitas vezes ou em alvos relacionados. Ferramentas, argumentos, profissão, perguntas e respostas, não devem ser repetidas. São recomendados juntos vários aspectos de diferentes pessoas todas as vezes que um Pretexting estiver sendo criado;
- Quando o telefone é usado, não se deve desligar caso o indivíduo alvo suspeite ou não se consiga a informação que queria. A melhor opção é planejar os possíveis erros que podem acontecer e estar preparado para qualquer tipo de problema que, ao telefone, é utilizar uma desculpa educada para poder desligar e talvez até dizer que ligará novamente.

3.2.2 Importância da Pretexting/Confiança/Relações de Confiança

A confiança é a crença na honestidade ou capacidade de algo ou alguém. Pessoas tem confiança em parentes, conjugues amigos, colegas de trabalho, superiores, empresas, personalidades, etc. Esta confiança pode, deve e, nos melhores casos, será utilizada em ataques que usam engenharia social e recomenda-se que seja levada em conta na criação de um Pretexting. Ao se explorar uma relação de confiança, as chances de sucesso são aumentadas e tempo de execução necessário é menor, o que diminui o risco do engenheiro social ser descoberto.

Um engenheiro social deve construir um cenário e ter segurança nas informações que possui e nas perguntas que serão feitas, sempre passando confiança e credibilidade total durante a execução de seu plano, não correndo o risco de perder o controle da situação ou a confiança das pessoas ao seu redor, impactando todo o objetivo. Limitar as perguntas até onde é necessário para não

transparecer o desejo pela informação e fazer com que o alvo seja influenciado a passar informações ou fazer algo de maneira desejada.

Durante a fase de pesquisa de informações sobre a área e o alvo, deve-se prestar atenção nas pessoas que interagem e que já possuem a confiança do alvo e daqueles ao seu redor, todos os detalhes sobre estas pessoas ou empresas devem ser anotados para que o engenheiro social possa usufruir desta confiança durante seu ataque.

Um exemplo de utilização da confiança em ataques de engenharia social é o de Mati Aharoni “muts”[6], do Offensive Security[7](Segurança Ofensiva, em tradução literal), que contou como foi capaz de convencer um funcionário de uma empresa a visitar um site para ver sua coleção de selos. Mati descobriu que o funcionário tinha um hobby de colecionar selos numa rede social e usou a confiança obtida ao dizer que também era um colecionador de selos e um site real como Pretexting para instalar um software malicioso no computador da empresa.

3.2.3 Planejamento

Para conseguir o sucesso, é indispensável um ótimo planejamento. Sem um planejamento correto, o engenheiro social pode ser descoberto e todo o plano irá fracassar e dependendo da situação, poderá ser preso. Para evitar problemas, a pesquisa deve ser embasada em informações claras e confiáveis, porém conseguir esta informação também é muito difícil. Para se coletar informações, deve-se utilizar as técnicas de engenharia social como um costume. Elicitação, pesquisas na internet, Dumpster Diving (Vasculhar o lixo), Redes sociais, programas de pesquisa em redes sociais (Social Network Mining, Exemplo: Maltego).

O Pretexting é conhecido como uma das maneiras mais rápidas de se conseguir informações através da engenharia social. Sua utilização ocorre em muitas áreas, profissões como repórteres, detetives, delegados o utilizam para chegar ao seu objetivo.

Na escolha e desenvolvimento do Pretexting, é necessário considerar alguns pontos:

---

[6] Mati Aharoni "Muts", Profissinal de segurança de informação. http://www.offensive-security.com/about-us/
[7] Offensive Security, empresa de segurança de informação. http://www.offensive-security.com/

- Qual problema você está tentando resolver?
- Quais perguntas estou tentando responder?
- Quais são as informações que procuro?
- A personalidade da pessoa com que se irá interagir.

A utilização de termos técnicos, sotaques, frases de efeito, expressões e gírias locais deve ser feita apenas quando o engenheiro social possui amplo conhecimento e experiência na área de atuação e da cultura local. Isto não se limita apenas ao sotaque, é necessário ter ciência completa do uso de qualquer palavra, termo ou gíria que são usadas na área ou região, além da necessidade de um ótimo nível de atuação para falar e convencer uma pessoa local.

Ao se usar Pretexting, deve-se levar em conta que o planejamento é tão importante quanto a execução do plano. Deve-se saber o que dizer, o que o alvo pode dizer as possíveis opções de resposta, possíveis reações, qual a informação necessária e uma maneira do alvo entregar a informação sem que perceba.

3.2.4 Criação de Personagem

Na criação do personagem para o Pretexting, a complexidade dos detalhes é determinada pela interação que o engenheiro social teve e conhecimento que possui das pessoas que fazem parte do “círculo local alvo”.

O cenário criado pode ser altamente complexo com identidades falsas (ou até verdadeiras), registros em sistemas, crachás, noção de personalidades (adquiridas em redes sociais, postagens em blogs, etc.) e conhecimento pessoal ou pode ser muito simples, utilizando apenas simpatia e o pensamento rápido necessário para criar o cenário durante uma conversa.

Em casos mais complexos e perigosos, onde geralmente tanto o “prêmio” quanto o risco é maior, a expressão “Quanto mais simples, melhor” não é válida e pode ser substituída por “Quanto mais detalhes, melhor”. O personagem criado pelo engenheiro social deve se vestir, agir, atuar, ter o conhecimento e as ferramentas da pessoa que diz ser.

Exemplo: Caso esteja disfarçado como um vendedor de software, é necessário ter valores, contratos de vendas, datasheets[8], cartões de visita, conhecer concorrentes e colegas de trabalho, etc.

Para aumentar a chance de sucesso, devem-se usar mais detalhes e possuir mais informações sobre a profissão. Recomenda-se utilizar disfarces onde já se possui grande experiência.

Exemplo: Se o engenheiro social tem experiência real como corretor de imóveis e atua como um, as chances de sucesso são maiores do que se o mesmo atuasse como um vendedor de software.

A comunidade de teatro possui processos bem definidos, documentados e praticados com inúmeras técnicas que podem ser utilizadas na criação de personagens para o Pretexting.

3.3 Phishing

Phishing pode ser definido como o roubo de identidade online de forma automatizada, por meio de mensagens e sites fraudulentos. O emissor do ataque, conhecido como Phisher, envia várias (milhares e até milhões) de mensagens falsas, o phishing, para um grande número de pessoas sob o pretexto de uma grande empresa, governo ou instituição conhecida. Esta mensagem solicita em algum momento, que o usuário passe as informações confidenciais como senhas, contas de banco, números de cartão de crédito, RG e CPF, etc. A chance de sucesso é baixa, mas uma pequena porcentagem dos alvos irá acreditar que a mensagem é real e cairá no golpe.

Na engenharia social, o phishing é usado como forma de coleta de informações para facilitar e potencializar ataques futuros.

A palavra phishing é uma evolução da palavra inglesa fishing, que significa pescaria em tradução literal. A letra f normalmente é trocada por “ph” no dialeto usado por hackers. A associação vem do fato de usuários, considerados Phishs/Fishs(peixes), serem atraídos pelos e-mails e sites falsos até uma armadilha, para terem suas informações coletadas.

[8] Planilhas com informações sobre o produto.

Quase 100% das pessoas já receberam um e-mail de phishing em algum momento. Estes e-mails e sites são formatados e algumas vezes até clonados para se parecer com um e-mail ou site legítimo de uma empresa que atua na internet, para tentar enganar o usuário a digitar informações pessoais e até confidenciais. Normalmente estas informações são nomes de usuários e senhas de vários serviços, conta e agencia de internet banking, dados de cartão de crédito, RG e CPF, número de seguro social (EUA), etc. Phishers sabem que o jeito mais fácil de se conseguir uma informação é pedindo.

O phishing também pode ser realizado através de malwares e também por ataques baseados em DNS[9], que redirecionam o site solicitado para um servidor falso.

Normalmente os phishing são associados a e-mails, mas também podem ser feitos por qualquer forma de comunicação, como por carta, telefone, web chat ou aplicativos de mensagens instantâneas e vários outros métodos. Devido à facilidade de criação e rapidez na entrega, além de ser fácil embutir um link para um website malicioso, o e-mail são o meio mais usado para propagação de ataques.

Até mesmo pessoas com experiência na internet e conhecimentos de TI podem ser pegas com técnicas de phishing, devido ao uso descuidado na realização de atividades rotineiras.

3.3.1 Prejuízos

Em setembro de 2008, o Gartner Inc, empresa americana de pesquisas tecnológicas e assessoria, entrevistou 3,985 americanos que utilizam a internet para determinar o número de pessoas que foram vítimas de ataques com phishing, além do método utilizado pelos criminosos.

A média de prejuízo foi de 351 dólares por pessoa, valor 60% menor que o do ano anterior. Os consumidores recuperaram em média 56% de suas perdas.

Mais de cinco milhões de pessoas tiveram prejuízos financeiros relacionados ao phishing entre setembro de 2007 e setembro 2008, um aumento de 39.8% sobre o ano anterior.

[9] Domain Name System, sistema de nome de domínio, em tradução literal.

Dados de pesquisas anteriores informam que em 2003 foram 1.2 bilhões de dólares em prejuízo, em 2004 foi estimado 1.78 bilhões, e em 2007 o prejuízo foi de três bilhões de dólares.

Os valores relacionados a perdas indiretas são muito maiores devido as despesas com SAC[10], reposição de valores perdidos, processos judiciais, perda de confiança nas organizações e diminuição do uso de transações online.

3.3.2 Fluxo de ataque

Normalmente os ataques relacionados com phishing seguem um padrão já conhecido.

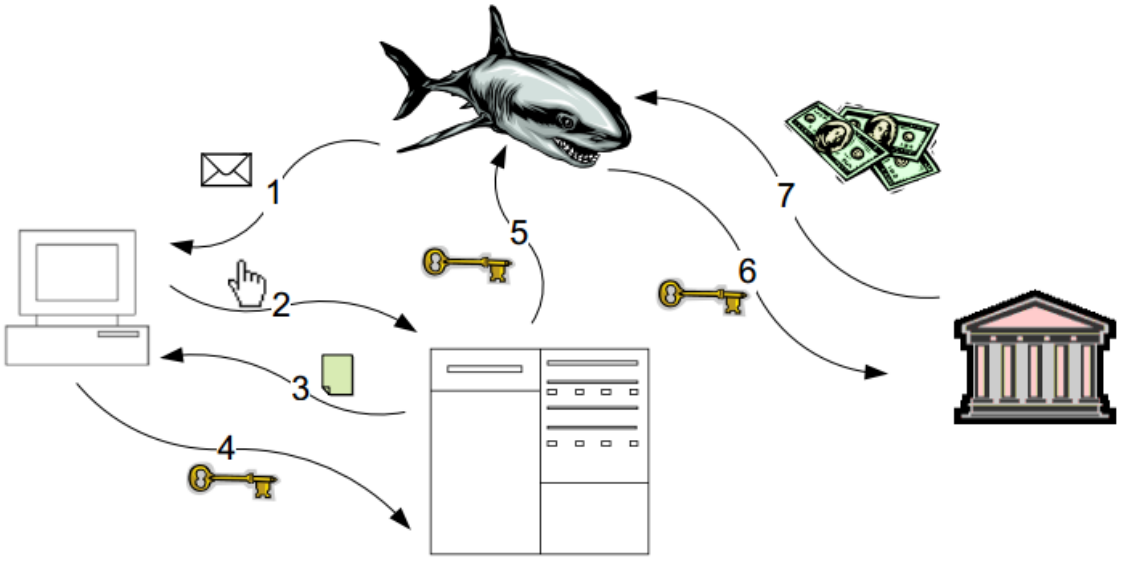

Figura 2: Diagrama de um ataque de Phishing

Fonte: Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures
Aaron Emigh, Radix Labs, ate@radixlabs.com, Revision 1.3, October 3, 2005

1. O phisher prepara o ataque, desenvolvendo o texto e as imagens utilizando técnicas para dificultar a detecção por sistemas de prevenção e melhorar o visual, fazendo-o parecer legítimo e aumentando a chance de sucesso.
2. O phishing é entregue ao alvo por qualquer meio de propagação.

[10] Serviço de Atendimento ao Cliente

Exemplo: O usuário recebe uma mensagem de um banco informando que é necessário validar as credenciais de acesso a conta devido a “atividades suspeitas” que foram detectadas na conta. O alvo se assusta com a mensagem e pensa que alguma outra pessoa estava tentando acessar sua conta.

3. O usuário toma alguma ação, como abrir e ler a mensagem, clicar no link e abrir o site ou até instalar malwares no computador, tornando-o vulnerável a perda de informações.

Exemplo: O alvo clica no link de login para o site, que na verdade o redireciona para um website malicioso que é criado e formatado para ser exatamente igual ao site legítimo. Por exemplo, www.bnaco.com.br em vez de www.banco.com.br.

4. O usuário recebe a solicitação da informação confidencial, em forma de login em um website falso ou tem as credenciais coletadas por um Trojan instalado localmente na máquina.

- O usuário digita suas informações.

Exemplo: O usuário digita o nome de usuário e senha e clica em login, enviando as informações.

5. A informação é transmitida do servidor de phishing para o phisher.

6. A informação é utilizada pelo Phisher para se autenticar nos serviços do usuário

(banco, e-mail, redes socais, etc.).

7. O phisher realiza uma ou mais fraudes utilizando a informação roubada.

3.3.3 Variações de Phishing

Como definido anteriormente, phishing é a tentativa de adquirir informações confidenciais com meios fraudulentos, mascarando-se como uma entidade eletrônica confiável.

Esta técnica pode ser dividida em algumas formas, conforme lista abaixo:

3.3.3.1 Spear phishing

Spear Phishings são ataques de phishing direcionados especialmente a pessoas ou empresas específicas. Normalmente são enviados para alvos dentro uma certa área de atuação.

3.3.3.2 Clone phishing

Variante de ataque de phishing onde é usado um e-mail legítimo enviado pela empresa para criar um e-mail quase idêntico ao original ou até mesmo cloná-lo. Os anexos ou links são substituídos por uma versão contendo anexos com malwares ou links com redirecionamento para sites falsos. Após o processo de clonagem, os Clones Phishing são enviados para os alvos por e-mail spoofing[11] (e-mail de fraude, em tradução literal) para parecer que e-mail veio da empresa real. Também são feitos ataques encaminhando e-mails originais editados ou atualizados.

Existem métodos de detectar e evitar os e-mails *spoofing*, dentre eles estão o SPF[12] ou Sender ID[13], porém nem todas as empresas possuem este tipo de medida de segurança.

3.3.3.3 Whaling

Whaling são ataques de phishing que são direcionados especialmente e exclusivamente para executivos e outras pessoas de alto cargo ou de alto poder aquisitivo.

O termo *Whaling* vem da palavra da língua inglesa *Whale*, que significa baleia. Por ter alvos de alto valor, em vez de phishing (peixe), o whaling é um ataque tenta “pescar” um peixe maior, uma baleia.

[11] E-mail Spoofing: Técnica utilizada para alterar informações do protocolo de envio de e-mail, alterando o endereço do remetente.
[12] Sender Policy Framework: Sistema de prevenção envio de fraudes de e-mail spoofing.
[13] Sender ID: Identidade do Remetente, em tradução literal. Número de identificação do remetente da mensagem.

3.3.3.4 Phone phishing

Phishing também pode ser feito por telefone. Mensagens gravadas são usadas em ligações telefônicas para influenciar os receptores a ligar em um número falso onde a coleta das informações será realizada.

Por exemplo: Um cliente do “Banco X” recebe uma ligação telefônica com uma mensagem gravada dizendo que o mesmo deve entrar em contato no número 1234-5678, que é mantido pelo phisher e utilizando normalmente um serviço de VoIP[14], para resolver problemas sobre sua conta. O número passado muitas vezes possui um sistema de atendimento IVR[15] idêntico ao do “Banco X”, levando os usuários a digitar suas informações. Esta técnica também é conhecida como *Vishing* (Voice Phishing).

3.3.4 Técnicas de Phishing

As técnicas de phishing não se limitam apenas na criação de cenários falsos. Através do phishing é possível alterar informações legítimas, comprometendo a integridade e legitimidade das mesmas.

As formas mais usadas para aplicação desta técnica são:

3.3.4.1 Manipular links

As técnicas de Phishing atuais normalmente enganam usuários alterando partes das mensagens enviadas, como links alterados que redirecionam o navegador a um *Spoofed Website* (Website falsificado, em tradução literal) que se parece ou é idêntico ao site verdadeiro da organização. URLs[16] (Localizador Padrão de Recursos, em tradução literal) erradas ou subdomínios são muito usados na criação dos Spoofed Websites.

[14] Voice Over IP: Voz sobre IP, em tradução literal. Tecnologia de conversação de voz pela Internet.
[15] IVR: Interactive Voice Response, sistema telefônico de atendimento automático.
[16] URL: Utilizado também para identificação na

Exemplo: A URL http://www.banco.exemplo.com.br/ parece que te levará a página “exemplo” do site do banco, enquanto na verdade irá levar a página “banco” do site exemplo.com.

Outro truque utilizado é editar o texto do link para levar a uma página diferente (Em HTML, pode-se fazer isto utilizando as Tags <A></A>).

Por exemplo: O link www.banco.com.br em um e-mail pode direcionar o usuário para o site www.exemplo.com.br. A maioria dos navegadores de internet exibe o site real que o link irá abrir no canto inferior esquerdo da tela quando o mouse é mantido em cima do link.

3.3.4.2 Enganar Filtros Anti-Phishing ou Anti-Spam

Para evitar filtros anti-phishing ou anti-spam disponíveis na maioria dos e-mails atuais, os phishers utilizam e-mails com imagens em vez de texto, impossibilitando a análise de formatação e conteúdo e diminuindo a chance de bloqueio antes de chegar à caixa postal dos alvos.

Porém, isto levou ao desenvolvimento de sistemas anti-phishing ou anti-spam mais avançados que fazem a leitura das imagens e o reconhecimento dos caracteres para analisar pelo filtro anti-phishing comum, impedindo que mensagens disfarçadas com imagens sejam repassadas ao usuário. Este tipo de sistema utiliza *OCR* [17] (Optical Character Recognition, em tradução literal) para fazer o reconhecimento dos textos nas imagens.

Sistemas anti-phishing ainda mais avançados utilizam *IWR* [18] (Reconhecimento Inteligente de Palavras, em tradução literal), que podem analisar e reconhecer letras escritas a mão, letras invertidas (de cabeça para baixo ou de traz para frente), letras distorcidas, com fundos coloridos, etc. Sistemas IWR não substituem totalmente os OCR, mas são um complemento a eles.

3.3.4.3 Typosquating

Typosquatting pode ser definido basicamente como comprar, registrar e utilizar domínios com nomes semelhantes a sites reais, esperando que usuários

[17] OCR: Aplicação de reconhecimento de caracteres por imagem para conversão em texto.

descuidados digitem o endereço errado e sejam redirecionados para os sites *Typosquatted,* onde sites falsos são publicados, usados para roubo de informações.

Normalmente a URL de typosquatting são de quatro tipos distintos, todas similares ao endereço de domínio de alguma empresa ou instituição.

1. Um erro de soletração ou de pronúncia, principalmente erros de pronuncia de estrangeiros como: www.exemple.com correto www.examplo.com.br
2. Erros de digitação do tipo www.eaxmplo.com.br ou www.uinsa.br
3. Um domínio correto e parecido com o real: www.exemplo**S**.com.br, em vez de www.exemplo.com.br
4. Um domínio de topo ou TLD (Domínio de alto nível), exemplo: com, .org. .net, .br, etc.) diferente. www.examplo.org em vez de www.exemplo.com.

.

3.3.4.4 Outras técnicas

Uma maneira de ataque por phishing é enviar o usuário para o site real da empresa e abrir uma janela pop-up[19], falsa solicitando as credenciais do usuário, levando a pensar que é o site da empresa real que está solicitando as credenciais.

- Outra técnica usada é o ***tabnabbing*** que utiliza a função de Abas dos navegadores atuais. Usando scripts e outros recursos é possível abrir novas abas com os sites maliciosos ou também carregar o site em abas previamente abertas, fazendo com que um usuário distraído digite suas credenciais na aba falsa.

- O Evil twins (Gêmeos do Mal, em tradução literal) é uma técnica de phishing muito difícil de ser detectado. O phisher cria uma rede wireless falsa com o SSID[20] que se parece ou é igual ao da rede wireless aberta disponível no local. Muitos lugares públicos como shopping, praças, cinemas, restaurantes, aeroportos, cafés, hotéis e outros estabelecimentos possuem redes wireless abertas. Quando o usuário se conecta a rede falsa, o phisher inicia uma captura de pacotes para coletar as credenciais ou outras informações das vítimas.

[19] Pop-Up: É uma janela extra que abre no navegador ao visitar uma página web ou acessar um link específico.
[20] Service Set IDentifer, é um conjunto de caracteres que diferencia uma rede sem fio de outra.

3.3.5 Prevenção

Phishing é um fenômeno complexo que inclui vários fatores sociais e também tecnológicos. Não existe nenhuma solução definitiva para prevenir o phishing, a melhor maneira de se evitar problemas é ter consciência e verificar todas as informações possíveis.

Alguns passos podem ser feitos para evitar problemas:

- URL de links - A URL pode ser verificada na parte inferior da página do navegador antes de clicar no link. A verificação deve ser feita porque o texto do link pode ser diferente da URL de destino no hyperlink.

- Números de telefone - Phishers também costumam enviar números telefônicos nas mensagens solicitando que o usuário ligue para resolver o problema ou ganhar algum prêmio. São usadas frases do tipo “Evite os riscos das transações pela internet e ligue para o número 0123-4567”. Muitos phishers possuem sistemas telefônicos IVR, que imitam de forma convincente qualquer central telefônica, com menus e gravações de voz idênticas as originais.

A veracidade dos números deve ser verificada antes de ligar, basta procurar pelo número do SAC da empresa na internet antes de ligar, olhando diretamente na página oficial.

Existem outras medidas de segurança que se aplicadas corretamente podem reduzir significantemente o risco de ataques com phishing, principalmente em empresas e instituições. Podem-se aplicar medidas de segurança em várias áreas, como:

- Monitorar atividades potencialmente maliciosas como uso de websites, registros de domínios, detectar e-mails de phishing antes de chegarem e bloquear os mesmos.
- Usar métodos para evitar o e-mail Spoofing de endereços, dentre eles estão o SPF (Sender Policy Framework), Sender ID, etc.
- Detectar o uso não autorizado de marcas, logos e outras informações proprietárias.

- Melhorar a infraestrutura e os processos e a frequência de patching[21], resolvendo possíveis falhas, diminuindo as chances de invasões.
- Detectar sites fraudulentos e alertar o usuário. Isto pode ser realizado desativando plugins do navegador, filtragem e categorias de proxy, etc.
- Estabelecer comunicação segura entre o usuário e o destino.
- Usar autenticação de dois níveis.
- Garantir que senhas sejam únicas para cada aplicação, site ou serviço.
- Codificar as credenciais e fazer o uso de chaves de criptografias assimétricas, e certificados digitais.

3.4 Dumpster Diving

A frase que descreve perfeitamente o Dumpster Diving é “One man’s trash, another man’s treasure”, traduzida como “O lixo de uns é o tesouro de outros”. Dumpster Diving, significa mergulhar na lixeira em tradução literal.

Pode ser definido como o processo de vasculhar o lixo para localizar itens de valor, úteis ou informações. Apesar do nome, não é feito somente em lixeiras, quando feito em sacos de lixo, fica conhecido como Garbage Picking, que significa Pegar lixo. A prática de Dumpster Diving vem crescendo rapidamente em países de primeiro mundo, onde as pessoas procuram por objetos para usar em casa como decoração e algumas vezes até comida e mobília.

Na engenharia social, Dumpster Diving é usado para coletar informações confidenciais que foram descartadas e que podem ser usadas para ataques futuros. Foi muito popular na década de 90 e usada por vários hackers, como Kevin Mitnick.

A única maneira de se prevenir do dumpster diving é, primeiramente, filtrar e descartar corretamente todo o conteúdo que será jogado no lixo. Não descartar documentos confidenciais em lixo comum. Deve haver processos e treinamentos corporativos que instruam os funcionários a prestar atenção no que descartam. Outra boa prática é manter o lixo em local não público e trancado em vez de ruas e calçadas.

[21] Patching: Da palavra Patch, significa correção, usado para referenciar a correção de uma ou mais vulnerabilidades de um sistema informático.

3.4.1 Itens de valor

Pessoas, empresas e organizações que não fazem filtragem ou reciclagem de lixo, acabam deixando que muitas informações sejam descartadas de forma incorreta, possibilitando uma coleta. Nas organizações, normalmente os funcionários não são devidamente treinados para descartar informações confidenciais de forma correta.

O descarte incorreto de documentos pode ser de grande valia ao engenheiro social para futuros ataques. Dados pessoais, como, números bancários, telefones, nome completo, data de nascimento, dentre outras informações sensíveis podem ser encontrados em lixos residenciais.

As empresas por sua vez, podem estar jogando incorretamente varias informações sobre seus funcionários no lixo, como nomes, departamento e gerentes estão entre os dados que podem ser encontrados.

É possível encontrar e-mails impressos que foram descartados. Estes e-mails podem revelar informações importantes como cadastros em outros serviços como redes sociais e até informações confidenciais, como documentos confidenciais e a estrutura de contas de e-mails da empresa.

Outro tipo de informação que pode ser coletado com o uso do Dumpster Diving são diagramas de rede, com informações de endereços de IP[22], hostname[23], roteadores, switchs, mapas de rede, que também são descartados como um lixo comum, apesar de serem informações confidenciais.

Um documento que pode ser encontrado nos lixos de uma empresa são notas fiscais que podem conter informações sobre a empresa, clientes, fornecedores, parceiros, entre outros. Este tipo de informação pode ser usado para descobrir que tipo de negócios a empresa faz e quais cenários uma invasão pode ser feita.

Outro aspecto que pode ser observado nas empresas é de que normalmente administradores de rede exigem que senhas sejam trocadas de três em três meses, ou menos. Para não se esquecer das senhas, muitos funcionários mantém estas informações de usuário e senhas anotados em post-its[24] ou arquivos de texto no computador, que muitas vezes são impressos e jogados no lixo.

---

[22] IP: Information Protocol, endereço de rede virtual de um computador numa rede.
[23] Hostname: Nome de um computador em uma rede.
[24] Post-It: Pedaço de papel utilizado para anotações.

Dispositivos como PenDrive, CDs, DVDs e até HDs também podem ser encontrados no lixo. Normalmente ninguém deleta informações ou quebra CDs/DVDs antes de descarta-los, permitindo que sejam coletados e analisados futuramente.

Um fator curioso e também importante a ser observado é que nos dias de hoje é muito raro a leitura de manuais de usuário que acompanham produtos ou sistemas, por falta de interesse e não necessidade, além do que a maioria desta documentação estar disponível na internet ou em arquivos digitais. Quando as documentações são atualizadas, as versões antigas vão para o lixo. Este tipo de documento engloba manuais de usuário e administrador, guias e procedimentos de operação e correção de problemas, que são descartados na maioria das vezes e por quase todos os funcionários da empresa. Muitas pessoas também jogam fora o CD/DVD oficial do produto que possuem as documentações e a até números de série e de licença.

Até mesmo assinaturas são de grande importância para um engenheiro social, pois podem ser usada para criar uma autorização de entrada ou saída falsa, falsificar um documento fiscal para obter ganhos financeiros, principalmente se estas assinaturas são de pessoas de alto cargo como diretores executivos ou até CEOs[25].

Uma prática comum em algumas empresas é o uso de máquinas de triturar papel para descartar documentos sigilosos. Porém isto pode não ser suficiente, pois algumas máquinas não misturam as laminas, apenas trituram o papel e deixam os pedaços ordenados, facilitando a reconstrução após a coleta. Existem softwares que fazem a reconstrução digital de documentos triturados. Um exemplo é o: Unshredder, http://www.unshredder.com/

3.4.2 Problemas Judiciais

Antes de praticar o Dumpster Diving, é de extrema importância verificar a legislação local para evitar problemas com a justiça.

No Brasil, não é crime coletar itens descartados no lixo, desde que esteja em uma lixeira ou em área pública. Porém o lixo que ainda está dentro de uma propriedade privada irá exigir a entrada no local para que a coleta seja feita e

[25] CEO: Chief Executive Officer, presidente da organização.

invasão de propriedade e pode ser enquadrada no artigo 150 e até furto no artigo 155.

- Invasão de Propriedade – “Art. 150”- Entrar ou permanecer, clandestina ou astuciosamente, ou contra a vontade expressa ou tácita de quem de direito, em casa alheia ou em suas dependências:
- Furto – “Art. 155” - Subtrair, para si ou para outrem, coisa alheia móvel.
- Pena - reclusão, de um a quatro anos, e multa.

4 Ataques Comuns

No mundo da engenharia social existem muitas formas de ataque, alguns envolvem muita tecnologia e outras nenhuma. O resultado final de qualquer ataque é quase sempre mesmo, perda de dados e até prejuízo financeiro.

A seguir uma pequena lista de algumas das mais comuns formas de ataque em engenharia social.

4.1 Ataques por Telefone

O telefone além de ser uma forma útil de coleta de informações conforme falado anteriormente, é um meio mais comum utilizado em ataques de engenharia social. O telefone é uma ferramenta altamente utilizada por sua facilidade, praticidade, velocidade e segurança. É possível realizar a tentativa de ataque mais rapidamente com um telefone, não há necessidade de se locomover até a empresa ou a casa do alvo, o risco de ser pego e de problemas legais é menor, não há necessidade de roupas e disfarces, o nível de atuação necessário é menor e a comunicação corporal pode ser desconsiderada. Ataques por telefone são feitos várias vezes até se encontrar alguém que caia no golpe. São usadas vozes do sexo masculino ou feminino, independente do sexo do atacante e normalmente o número de Caller ID[26] é restrito.

Ataques por telefone normalmente seguem duas vertentes:

1 - Ligar para o Suporte Técnico da empresa fingindo ser um funcionário;

2 - Ligar para um funcionário fingindo ser do Helpdesk/TI.

Analistas de Helpdesk são extremamente vulneráveis a ataques com engenharia social devido a natureza de seu trabalho. Sendo sua principal função ajudar os usuários, um engenheiro social tem a disposição toda a estrutura de Helpdesk para realizar o ataque.

Exemplo: O mais simples e mais efetivo ataque é ligar no suporte técnico e dar apenas um nome ou sobrenome, dizer ser um usuário e pedir para trocar ou redefinir a senha. A falta de treinamento e alinhamento nos processos e o desejo de

[26] Caller ID: Número de telefone do remetente.

agradar o usuário, muitas vezes aliado com a falta de experiência para trabalhar sob a pressão faz com que muitos atendentes de suporte realizem a troca da senha sem verificar e confirmar os dados do usuário. É possível tentar várias e várias vezes um ataque deste tipo em uma mesma empresa devido ao grande número de analistas e usuários que podem ser usados caso não se tenha sucesso nas primeiras tentativas.

Os funcionários também estão vulneráveis a receber ataques por telefone. Em segurança de informação, este tipo de abordagem por telefone é conhecida como "*Quid Pro Quo*", que em latim significa "Isto por isto".

Este ataque é realizado ligando para números de pessoas aleatórias dentro de uma empresa, alegando ser do suporte técnico que está retornando uma ligação, até encontrar algum usuário que realmente tinha um problema e esperava um retorno. O engenheiro social pode ajudar a resolver o problema por telefone e durante o processo, executar programas maliciosos, instalando malwares ou abrindo vulnerabilidades nos computadores dos usuários ou na rede. Uma vez que o hacker tem o malware instalado, o engenheiro social pode utilizá-lo para coletar a informação desejada e para necessidades futuras.

Empregados novos ou que não foram treinados corretamente são normalmente alvos mais vulneráveis a ataques deste tipo.

Itens necessários para um ataque por telefone:

- Telefone – Um aparelho e uma linha telefônica são necessários para fazer a ligação.
- Caller ID Privado ou Restrito – É recomendado utilizar um número de telefone configurado para manter o Caller ID restrito ou privado para que o alvo não possa identificar o número de telefone utilizado, impedindo rastreamento.
- Voice Changer – Equipamento de áudio utilizado para alterar a voz, fazendo parecer um homem ou uma mulher e impedindo reconhecimento por voz.

4.1.1 Prevenção

Uma das melhores maneiras de proteger contra tentativas de ataque por telefone é saber com quem você está falando. Se alguém ligar no telefone da empresa, deve-se pedir mais informações como nome, telefone para contato, verificar o número de contato no telefone, etc., para ter certeza de que eles são quem eles dizem ser. Se a pessoa não puder lhe dar qualquer informação, muito provavelmente é alguém tentando lhe enganar. Avise imediatamente ao setor de segurança de informação ou SOC (Security Operations Center, em tradução literal) da empresa.

Todos os funcionários devem receber treinamento sobre confidencialidade e vazamento de informações, que focam todos os tipos e formas possíveis de ataque e de vazamento de informações.

4.2 Entregador

Se disfarçar de entregador é um ataque muito comum e fácil, devido ao baixo nível de atuação necessário. Motoboys, Office boys, funcionários dos correios, serviços de entregas de correspondências e objetos como FEDEX, entregas de flores, delivery (entrega) de comida, etc., são tipos de entregadores que podem ser utilizados para a criação do disfarce, mas devem ser adaptados conforme o ambiente do alvo para aumentar as chances de sucesso.

Este tipo de ataque é eficaz porque passa confiança ao alvo, pessoas quando vê o engenheiro social usar um uniforme e algumas vezes até um veículo clonado da empresa de entregas, se sentem mais seguras e menos suscetíveis a golpes. Entregas são comuns em todos os tipos de condomínios, prédios corporativos ou residenciais e empresas, não levantando qualquer suspeita.

Após a entrada no local alvo, o engenheiro social pode continuar seu plano para alcançar seu objetivo.

4.2.1 Exemplos

Bilionário é assaltado com o uso de personificação

Em 2007, uma pessoa se disfarçou de entregador e roubou Ernest Rady, um bilionário que vive em San Diego. O ladrão bateu na porta de Rady dizendo ser um entregador com uma encomenda e a esposa de Ernest abriu a porta.

Fonte[27]: http://www.lasorsa.com/

Carteiro falso roubava correspondências

Um homem fingia entregar cartas nas caixas de correio, mas a real intenção erra roubar as correspondências que já foram entregues, procurando por cartões de crédito, cartões de caixa eletrônico ou de conta bancária. Ele se entregou após 46 acusações de obtenção de bens por engano, duas acusações de receptação de bens roubados e 1 acusação de roubo.

Fonte[28]: http://www.theage.com.au/

PenDrive Perdido

Em um ataque em 2006, uma empresa de auditoria de segurança que trabalhava para uma cooperativa de crédito usou PenDrive USB com um malware para obter senhas e informações de login para as máquinas. Eles levaram os PenDrive para a empresa e os deixaram em locais diferentes e aleatórios, os funcionários encontraram e começaram a usá-los, espalhando o trojan pela empresa.

Fonte[29]: http://www.darkreading.com/

[27] Disponível em: http://www.lasorsa.com/security/delivery-man-robs-billionaire-making-off-with-several-hundred-dollars/

28 Disponível em: http://www.theage.com.au/articles/2003/03/18/1047749768526.html

[29] Disponível em: http://www.darkreading.com/perimeter/social-engineering-the-usb-way/208803634

4.2.2 Prevenção

Ataques deste tipo são difíceis de identificar e evitar, mas não é impossível. Com um pouco de educação e conhecendo sobre a pessoa que costuma fazer entregas. Geralmente entregadores são responsáveis por certa área, e caso não seja o mesmo funcionário de sempre, pode-se e deve-se solicitar o crachá e outros dados para identificação. Muitos engenheiros sociais inexperientes e sem o devido planejamento não terão as credenciais necessárias, porém, um bom engenheiro social com um bom Pretexting terá consigo um crachá falso idêntico ao da empresa que tem sua foto e até mesmo o veiculo clonado da empresa de entrega, além de saber nomes de funcionários e conhecimento da região e da área de entregas.

A maneira mais segura de evitar este ataque é não permitir que um entregador entre no prédio, as entregas podem ser feitas diretamente para a portaria, recepcionistas, seguranças ou na área de docas do condomínio. Apesar de tudo, algumas vezes é necessário que o entregador precise fazer a entrega do documento ou objeto em mãos, neste caso, deve-se sempre ter algum funcionário o acompanhando e jamais deixa-lo sozinho. Este cuidado pode não evitar um assalto ou crimes do tipo, mas irá diminuir a chance de qualquer tipo de ataque com engenharia social.

Em qualquer suspeita ou atitude estranha, como nervosismo ou falta de conhecimento da área, empresa ou colegas de trabalho, deve-se imediatamente entrar em contato com a empresa e verificar a identidade do entregador.

4.3 Suporte Técnico Local

Um dos ataques mais populares e efetivos no mundo da engenharia social é se passar por um funcionário do suporte técnico local da empresa, sendo possível conseguir informações valiosas e em grandes quantidades e causar prejuízos enormes. Com acesso físico a rede local de computadores o ataque fica muito mais fácil por não ter que passar pelas camadas de proteção externas da empresa, potencializando os danos. Este tipo de ataque exige que o atacante entre fisicamente na empresa alvo, o que o torna mais difícil e perigoso. A infiltração pode

ser feita utilizando-se algumas técnicas de engenharia social, como Pretexting e a personificação.

4.3.1 Prevenção

Para se proteger de uma tentativa de ataque onde alguém personifica um analista de suporte é saber se ele é realmente do suporte técnico, pressionando-o e fazendo perguntas que alguém do suporte técnico da empresa saberia responder. A menos que algum novo funcionário tenha sido contratado no suporte técnico, provavelmente o mesmo técnico irá lhe atender. Se você não sabe quem a pessoa é, questione-o e certifique-se que é um funcionário da empresa. O crachá também deve ser verificado em caso de dúvida.

Muitas vezes dispositivos USB (PenDrive com softwares maliciosos por exemplo) são usados em ataques deste tipo para infectar uma máquina rapidamente ou roubar arquivos. Para evitar uma infecção automática, recomenda-se desabilitar a funcionalidade de *autorun* (recurso de execução automática de dispositivos de armazenamento móvel) do computador, impedindo que qualquer arquivo seja executado automaticamente ao se conectar um PenDrive ou um CD. Caso a invasão à empresa ocorra em horários não-comerciais onde não há pessoas ou há poucas, é possível roubar informações de máquinas desligadas utilizando um PenDrive com qualquer distribuição de Linux inicializável por um pendrive USB para acessar o HD e pegar os arquivos com a máquina desligada.

5 Fatores Psicológicos

Como falado anteriormente por definição engenharia social é um artifício utilizado por pessoas maliciosas, que são denominadas como "engenheiros sociais" que se aproveitam da fragilidade ou da inocência dos usuários, com o intuito de obter informações necessárias para posteriormente realizarem um ataque.

Um engenheiro social utiliza as técnicas psicológicas que todos nós também usamos em nosso dia-a-dia, como a busca por credibilidade, cobrar obrigações recíprocas, o uso de técnicas de persuasão, influencia e autoridade. Normalmente o engenheiro social aplica estas técnicas de maneira manipuladora, enganosa, de maneira com que as pessoas sem perceber forneçam as suas informações.

Um teste realizado durante a conferência Defcon em julho 2010, foi utilizado para avaliar o risco de divulgação de informações por funcionários das empresas. Todos foram submetidos aos processos de engenharia social: 135 trabalhadores de 17 grandes empresas, incluindo a Coca-Cola, Ford, Pepsi, Cisco, Wal-Mart, foram testados.

Os resultados são interessantes, já que 96% deles, que foram contatados por telefone ou e-mail, divulgaram informações consideradas como "sensíveis", do tipo: versão do sistema operacional, softwares antivírus e navegadores utilizados na empresa, etc.

Outro fator curioso da pesquisa foi que algumas das técnicas psicológicas foram aplicadas, onde os pesquisadores se passaram por auditores ou consultores através de técnicas combinadas como elicitação, persuasão e personificação.

5.1 Persuasão

Segundo Aristóteles (384-322 a.C.) a persuasão "é uma espécie de demonstração, pois certamente ficamos completamente persuadidos quando consideramos que algo nos foi demonstrado".

A persuasão é uma estratégia usada na comunicação, trata-se da capacidade de convencer alguém. O ato de persuadir visa induzir outro individuo a aceitar uma idéia, atitude, ou realizar uma ação, através de métodos lógico-racionais, simbólicos ou até mesmo emotivos.

Alguns métodos de persuasão lógico-racional podem ser através de provas, argumentações lógicas, e métodos científicos. Este tipo de persuasão é muito utilizado por advogados, vendedores e também por engenheiros sociais.

Outro método da persuasão é através do apelo emotivo dos seres humanos. Este método utiliza-se da crença, da fé, da tradição, dos valores pessoais, do controle mental das propagandas e publicidade.

A seguir temos uma situação de ataque que é usado por engenheiros sociais, usando técnicas de persuasão.

“Somos da equipe de suporte da Microsoft – queremos ajudar”

Ele começa com uma ligação telefônica afirmando ser do serviço de suporte da Microsoft e diz que está ligando por causa de um número anormal de erros que teriam origem no seu computador.

Após a descrição acima, o engenheiro social irá "demonstrar" isso para a vítima, ou seja, que realmente trabalha na Microsoft, por isso, ele a convence seguir passo a passo até o event log[30] de seu computador.

Todo usuário do Windows terá dezenas de erros neste log, simplesmente porque acontecem pequenas coisas; um serviço trava algo não inicializa em fim. Sempre existem erros, porém quando um usuário sem experiência abre event log e se depara com todos esses erros, fica assustado e preocupado.

Pronto, a vítima está vulnerável e pronta para fazer qualquer coisa que o suposto funcionário do suporte pedir.

Através deste exemplo podemos perceber o uso da metodologia lógico-racional da persuasão, é aplicado de maneira que a vítima se convença que seu computador está com problemas, mesmo ele estando sem defeito algum.

5.2 Táticas de Influência

Comumente, confundimos influencia com persuasão, porém, apesar de semelhantes, são duas metodologias distintas.

Persuasão é a capacidade de convencer alguém a algo, ou seja, quando se tem a real intenção de mudar opiniões, atitudes e pensamentos de outras pessoas.

[30] Event Log: Registro de eventos do sistema operacional.

A influência também tem a capacidade de mudar opiniões e pensamentos, porém ela é feita de maneira mais ampla é e muitas vezes, é feita até de maneira involuntária.

Existem diversas formas e meios de comunicação e pessoas que exercem o poder da influência, tais como TV, rádio, internet, presidente de empresas, diretores, acionistas, supervisores, governantes, pai, mãe, professores dentre outros.

A influência é muito usada em atividades com engenharia social, de maneira que na maioria dos ataques, os engenheiros sócios procuram influenciar suas vítimas a fim de conseguir sua confiança.

5.3 Credibilidade

Kevin Mitnick em “A arte de Enganar”, de 2003, fala que a credibilidade é a primeira fase a ser alcançada na maioria dos ataques efetuados através da engenharia social, sendo um ponto fundamental para as demais fases subsequentes. O engenheiro social nesta etapa tenta ganhar a confiança e gratidão de sua vítima, reproduzindo ações dignas de uma pessoa confiável.

Engenheiros sociais primeiramente confiam para construir confiabilidade e assim atingir a credibilidade, eles são mestre na arte de enganar, fazem suas vitima ficarem "seguras" de maneira que não desconfiem de suas ações.

Abaixo temos pequenos exemplos simples, mas bastante aplicados, por engenheiros sociais:

Exemplo 1 - "Agora insira a sua senha, mas lembre-se de não dizê-la em voz alta".

Essa parece ser uma declaração de alguém que não é "digno" de confiança?

Exemplo 2 - "Senhor sua conexão pode cair por alguns instantes, mas se isso acontecer, por favor, me avise e tentarei restabelecê-la novamente, ok?".

Após estas palavras, certamente ele mesmo irá cuidar para que a conexão caia, para que ele possa supostamente “restabelecê-la”, obtendo credibilidade, confiança e gratidão de sua vítima.

Outro fator que gera grande credibilidade junto a outras pessoas, e possíveis vítimas, é o simplesmente fato de convivência com pessoas de cargos importantes.

Por exemplo, almoçar com o CEO, da empresa, te dará credibilidade diante as outras pessoas, subordinadas a ele.

5.4 Amizade

"As pessoas gostam daqueles que gostam delas" autor desconhecido. A frase acima é muito simples, porém retrata muito bem este método utilizado por engenheiros sociais na obtenção de informações.

O ser humano costuma se agradar e sentir-se bem quando elogiado, por isso o método de amizade usado por engenheiros sociais, tem como o fruto, conquistar a vítima, através de elogios, favores, fazendo com que a vítima se torne vulnerável a suas vontades.

5.5 Reciprocidade

Essa vulnerabilidade é explorada por engenheiros sociais de maneira muito peculiar e bem arquitetada.

Reciprocidade se dá quando atendemos um pedido retribuindo algo por alguém. Originada da palavra recíproco, esta metodologia é usada por engenheiros sociais de maneira que algumas vezes os mesmos causam problemas para as vítimas, para que depois os próprios possam solucionar, deixando a pessoa com a consciência de obrigação de retribuição para com eles.

Quando falamos em reciprocidade, estamos tratando de obrigações e concessões que o indivíduo sente que precisa realizar como se fosse algum tipo de "divida" moral para com outra pessoa. Podemos dizer que se trata de um contrato ou promessas entre duas pessoas. O termo em engenharia social é popularizado como o "vaivém", porém não se limita apenas a ele.

Atitudes simples como, segurar a porta do elevador para alguém, ser gentil para com uma pessoa, de maneira que o mesmo passe a acreditar nestas gentilezas, já é o início de uma relação que futuramente poderá acabar em vazamento de alguns vestígios de informações privadas, simplesmente pelo fato de que a pessoa se sentirá na obrigação de retribuir os favores e gentilezas feitas a ela.

Como uma forma de entendimento prática do conceito de reciprocidade, temos um pequeno exercício:

Da próxima vez em que estiver em uma conversa, e algo lhe for perguntado, simplesmente não diga nada. Fique em silencio, ou ignore a pergunta, e siga em frente com a conversa.

Observe como algo simples como uma pergunta, cria um senso de obrigação de resposta em nosso psicológico. Você pode ignorar e não responder, porém ficará com o pensamento preso a pergunta.

A ideia de reciprocidade está profundamente enraizada em todos nos seres humanos. A maioria das pessoas sente que se alguém faz um favor, uma gentileza a eles, então eles mentalmente se sentem na obrigação de retornar essas gentilezas.

5.6 Personificação

Personificação em engenharia social é a capacidade de criar um indivíduo, ou representar um papel. Quanto mais simples esse papel, melhor. Como uma simples ligação para alguém e dizer: “Oi, eu sou Fulano do setor de informática e preciso redefinir sua senha". Outra tática comum que pode ser utilizada em um ataque de personificação é o engenheiro social se passar por assistente da gerência ou mesmo presidência e pedir a um funcionário, em nome do seu superior, alguma informação.

É comum encontrarmos a personificação sendo combinada com outras técnicas de engenharia social, como por exemplo, a elicitação ou autoridade.

5.7 Autoridade

O uso da autoridade é uma das formas mais clássicas e simples em ataques de engenheiros sociais. Esta técnica normalmente é combinada com a metodologia da personificação, onde o engenheiro social assume o papel de um indivíduo que ele não é, ou seja, um impostor.

Usualmente utilizada por telefonemas, e-mails, ou até mesmo pessoalmente, neste tipo de golpe o atacante se faz passar por gerente, presidente, ou outro cargo dentro de uma organização.

Podemos dividir autoridades em 3 (três) grupos:

1. Autoridade Legal
2. Autoridade Organizacional
3. Autoridade Social

Autoridade legal é baseada no governo e na lei. Estão relacionadas com policiais, juízes e delegados.

Autoridade organizacional é toda autoridade definida por meio de uma organização, normalmente, refere-se a uma hierarquia. Uma pessoa que ocupa um cargo alto na hierarquia dentro de uma organização vai ter acesso às informações mais importantes de maneira mais rápida e fácil. Presidentes, gerentes, supervisores, coordenadores, diretores, são exemplos de pessoas que exercem o poder de autoridade dentro das organizações.

Autoridade social refere-se a “lideres naturais”, ou seja, pessoas com perfil de autoridade natural. São colegas de trabalho, amigos da faculdade, todos de qualquer grupo social.

A escolha de qual categoria de autoridade á se usar pode depender da vulnerabilidade do alvo. A autoridade é explorada principalmente pelo simples fato de que psicologicamente, algumas pessoas se sentem na obrigação de serem prestativas para com seus superiores, ou seja, não questionam, nem se preocupam se as informações concedidas são de valor ou não, desde que o solicitante seja uma pessoa de hierarquia maior que o seu.

5.8 Framing

Podemos dizer que framing (Enquadramento, em tradução literal), é o uso das experiências e conhecimentos adquiridos pessoais ao longo da vida, de maneira que ele influencie no jeito com que as pessoas reajam em determinadas situações.

Framing é usado na política, em ações de marketing e também na engenharia social, entre outros setores da sociedade.

5.8.1 Framing na política

O uso de framing na política tem se tornado muito comum. A forma com que as mensagens são formuladas faz muita diferença na maneira como o eleitor irá perceber.

Se a campanha, por exemplo, faz referência direta ou indiretamente, a algo que aconteceu com o candidato, ou que o mesmo esteve presente quando aconteceu, a mensagem irá apresenta-lo como o candidato mais preparado, usando sua experiência para convencer os eleitores de sua capacidade.

Tudo que pode alterar as nossas percepções ou maneira como tomamos nossas decisões, pode ser classificado como framing. O fato de um amigo dizer que na semana passada ele fez uma viagem para uma cidade, que tomou determinado caminho e pegou transito, por conta de uma obra ou construção, certamente muitos de nós, se tivermos que realizar a mesma viaje, iríamos traçar outra rota, mesmo que mais longa para evitar o atraso em potencial.

5.8.2 Framing em ações de marketing

“Nossa mente insiste em procurar padrão nas coisas” autor desconhecido.

Partindo deste pensamento, é que campanhas de marketing são desenvolvidas, como por exemplo:

Figura 3: Carro de entregas da Fedex

Fonte: http://www.imam.com.br/imam/images/stories/federal-express-truck.jpg

A imagem acima é de um caminhão da Fedex.

Observe bem a imagem e veja se encontre a uma seta.

Agora que você irá vê-la, você irá percebê-la sempre que olhar para imagem do caminhão.

Figura 4: Logo Fedex

Fonte: http://articlesandtexticles.co.uk/imgs/0609/fedex02x.gif

Esta forma de framing utilizada no logotipo faz uma referência sobre os serviços prestados pela empresa.

Essa flecha existe para comunicar o movimento, a velocidade.

5.8.3 Framing em ações de marketing

O uso do framing também é feito por engenheiros sociais, manipulando as informações de que a vítima irá receber a fim de fazer com que a decisão final dela, seja o que o engenheiro social precisa.

Para um melhor entendimento do conceito, vejamos o exemplo:

O questionário abaixo oferece duas soluções alternativas para 600 pessoas afetadas por uma doença mortal.

- O tratamento A salva a vida de 200 pessoas;
- O tratamento B tem 33% de chance de salvar todas as 600 pessoas e uma possibilidade de 66% de salvar ninguém.

72% dos participantes que responderam às perguntas escolheram a opção A, e apenas 28% dos participantes escolheram a opção B.

Obs. As identidades das pessoas que responderam o questionário não foram divulgadas por uma questão de segurança.

Analisando o exemplo acima observamos que quando as perguntas são realizadas com uma interpretação positiva as pessoas geralmente escolhem a vida ao invés de questões feitas com uma possível interpretação negativa.

Engenheiros sociais usam o framing, principalmente na elaboração de perguntas e declarações de maneira que as pessoas respondam e sem saber apontem para o objetivo do atacante. O framing está diretamente ligado ao conceito de conversa, conforme visto nas técnicas de elicitação.

5.9 PNL

Outro campo de estudo da psicologia que podemos encontrar envolvida em engenharia social é a programação neurolinguística, também conhecida como PNL.

A sigla PNL, em suma se significa: como as palavras (linguística), podem atingir a mente (neuro), e produzir uma ação (programação). A ideia é baseada na ideia de que a mente, o corpo e a linguagem interagem para criar uma percepção, e que tal percepção pode ser alterada através da aplicação desta técnica. Cada parte da PNL possui uma função especifica, de maneira que as três juntas possam atingir a percepção desejada.

A parte que se refere à neuro, parte do princípio de que todos os comportamentos nascem dos sentidos (visão, audição, olfato, paladar, tato). Percebemos o mundo através dos nossos sentidos, e é através destes, que "compreendemos" a informação e depois agimos. Nossa neurologia inclui não apenas os processos mentais invisíveis, mas também as reações fisiológicas as ideias e os acontecimentos. Uns refletem os outros no nível físico. Corpo e mente forma uma unidade inseparável, um ser humano.

Já quando falamos em linguagem, refere-se usarmos a linguagem para ordenar nossos pensamentos e comportamentos e nos comunicarmos uns com os outros.

Por fim, a programação estuda a maneira como organizamos nossas ideias e ações a fim de produzir resultados.

PNL é usada em várias formas em nossas vidas. Os professores utilizam para manter seus alunos na linha. Polícia geralmente utiliza para interrogar as pessoas. Anúncios contam com a PNL para obter os seus produtos vendidos, e até mesmo nos utilizamos da PNL sem que percebermos.

Alguns engenheiros sociais, mais experientes e mais confiantes em seus golpes, aplicam algumas técnicas da PNL para ludibriar e enganar suas vítimas.

O estudo de caso abaixo mostra como e onde as técnicas da PNL são aplicadas em um suposto ataque de engenharia social.

5.9.1 Estudo de Caso cartão de crédito clonado

Antes da análise do estudo de caso, é importante se ressaltar alguns pontos:

1. O objetivo do golpe é conseguir o número e o código de segurança do cartão de crédito de uma vítima;
2. Vulnerabilidade: Poucas pessoas sabem, mas o código de segurança dos cartões de credito é único. Nem mesmo os bancos ou bandeiras responsáveis pela emissão do cartão tem acesso a ele. O número de segurança é quem valida que o cartão está de fato em sua posse;

Á vitima recebe uma ligação e a pessoa do outro lado da linha (engenheiro social) inicia a conversa:

- (SE) - Boa tarde, estamos ligando do departamento de segurança do cartão Mastercard, meu nome é fulano, meu número de identificação funcional é 5789;

Obs.: Como primeiro contato o engenheiro social, utiliza o nome de uma empresa de bandeira de cartão, que é conhecida e possui vários clientes, e possivelmente a vítima também é um cliente desta instituição. Outro ponto a se ressaltar é o uso de um "número de identificação funcional", pois com isso ele apresenta uma falsa garantia para que a vítima possa posteriormente identifica-l, transmitindo assim uma confiança indireta.

- (SE) - O senhor comprou cinco quilos de ração para pinguim, no valor de R$ 3.070,23, de uma empresa chamada SOS Pinguim, estabelecida em Porto Alegre?

Obs.: Nesta etapa do golpe, o engenheiro social, usa um produto que provavelmente a vítima não comprou e que obviamente a vítima irá responder que não fez a compra.

- (SE) - Senhor então provavelmente, seu cartão de crédito foi clonado e estamos telefonando para verificar. Se isto for confirmado, estaremos emitindo um crédito do valor a seu favor.

Obs.: Aqui o atacante dá o encerramento de sua fala de maneira positiva do caso de houver uma colaboração da vítima para descobrir se o cartão foi clonado ou não.

Um ponto importante é que normalmente a fala “senhor então provavelmente, seu cartão de crédito foi clonado" é feita em um tom de preocupação, para que a vítima fique preocupada. Esta técnica é utilizada na PNL, para que o lado neuro da vítima fique focado apenas nas próximas perguntas que iram confirmar *se o cartão foi clonado, e não perceba que está sobre ataque.*

- (SE) - Antes de processar o crédito, gostaríamos de confirmar alguns dados, o senhor concorda?

Obs.: Neste momento, o engenheiro social demonstra a vítima que ela será ressarcida com o crédito da suposta compra mais para isso ele deverá "confirmar" alguns dados. Está técnica, se chama rapport (Harmonia, em tradução literal), é estudada e aprofundada na PNL. Resumidamente, esta técnica é quando as pessoas sentem que estão sendo escutadas com real interesse em uma comunicação.

- (SE) - O seu endereço é Rua Barra Funda, 9000, CEP 05007-030, seu nome completo é Gregório Jesus Santos...

Obs.: Aqui o objetivo é conseguir no mínimo três respostas "sim". Esta técnica se chama engrama, que na PNL, é um estado onde o estado neuro entra em um estado permanente de respostas neste caso o "sim". As informações que o engenheiro social irá fornecer e pedir a confirmação normalmente são informações simples, que podem ser encontras em redes sociais por exemplo.

- (SE) - Qualquer dúvida ou pergunta que o senhor tenha, o senhor deve entrar em contato com o número 0800 que se encontra na parte de traz de seu cartão e falar com nosso departamento de segurança. Por favor, anote o seguinte protocolo 080920131234.

Obs.: O objetivo desta etapa é fornecer a sua vítima, informações verdadeiras, como o número de 0800, que é um número verdadeiro, mas combinado comum protocolo de atendimento falso, fornecendo a vítima um "voto de confiança".

- (SE) - O senhor poderia, por favor, lê-los para me confirmar?

Obs.: Com esta pergunta o engenheiro social está confirmando se a vítima continua no rapport, ou seja, se a pessoa do outro lado da linha continua dentro da armadilha e está pronto para levar o "bote", ou se ele deverá repetir os passos anteriores até que a vítima esteja condicionada.

- (SE) - Desculpe senhor, mas temos que nos certificar de que o senhor está de posse de seu cartão. O senhor está com ele em mãos ou pode pegá-lo? Por favor, preciso que o senhor pegue seu cartão e leia para mim o seu número.

Obs.: A partir daqui inicia-se à parte mais importante. Deste ponto em diante o engenheiro social pretende chegar ao seu objetivo, que é o número do cartão e os números de segurança.

- (SE) - Por favor, vire seu cartão e localize, por favor, os três últimos números.

Obs.: Neste momento, podemos observar que a vítima, fornece todas as informações que lhe são solicitadas sem saber que está sobre ataque. Os solicitados são usados para fazer comprar via internet, ou nas lojas, para provar que você está de posse do cartão. Após a vítima “confirmar” os números solicitados o engenheiro social prossegue.

- (SE) - Correto! Senhor somente esclarecendo, era necessário verificar que seu cartão não está perdido nem foi roubado, e que o senhor está de posse dele. Isso confirma que o seu cartão foi infelizmente, clonado, mas vamos estornar o valor, pode ficar tranquilo.

Obs.: Após esta etapa, o engenheiro social já atingiu seu objetivo. Está de posse do número do cartão e os números de segurança do mesmo. É importante frisar, algumas declarações fornecidas pelo atacante, tais como “senhor, somente esclarecendo, era necessário verificar que seu cartão não está perdido e nem foi roubado", com esta frase, ele consegue se justificar pela solicitação dos números do cartão de maneira que a vítima não desconfie de nada. Outra frase importante, é “mas vamos estornar o valor, pode ficar tranquilo”, ou seja, é hora de finalizar a ligação sem que a vítima desconfie de nada.

- (SE) - O Senhor teria alguma pergunta?

Obs.: Está pergunta é feita em um tom tranquilo, sem pressa, para que a vítima não acorde de seu estado de rapport. Depois que a vítima responde dizendo "não" ou faz alguma pergunta, que o engenheiro social, naturalmente irá pedir para que ela entre em contato com o “0800”, depois de pelo menos 2 horas, "para dar tempo de o sistema processar as informações" ou por "ser outra equipe" que irá atender a ligação, o atacante agradece e desliga.

5.9.2 Prevenção

O estudo acima ilustra um ataque usando técnicas de engenharia social combinadas com métodos da PNL.

Algumas medidas de prevenção a este golpe podem ser tomadas para que este tipo de ataque seja evitado, tais como, ao receber uma ligação parecida com está, desligue e ligue você mesmo imediatamente para o número 0800 do seu cartão. Para confirmar a se a informação de clonagem procede.

Um ponto muito importante que deve ser observado é de que quando tratamos de PNL, os estudos estão se referindo a traços psicológicos, caráter, formar de agir, e interagir. Diferente da psicologia, que é um estudo que trata das emoções.

6 Ferramentas de Engenharia Social

6.1 Ferramentas de engenharia social – Física

Segurança Física pode ser entendida como medidas físicas que são utilizadas para proteger pessoas, não permitindo acesso não autorizado a instalações, documentos e equipamentos, e também para proteger de espionagem, furto e sabotagem e de ataques.

As medidas para segurança física podem incluir barreiras, iluminação, sistemas de controle de acesso, sistemas de segurança, fechaduras, cartões de acesso, cofres, alarmes e sistema de CFTV.

Tais sistemas de segurança física são uteis para alertar tentativas de acesso não autorizado, frustrar ou atrasar estes acessos.

6.1.1 Lock picking

Lock picking[31] é uma técnica usada para descobrir falhas na estrutura de fechaduras, maçanetas ou cadeados e explorar esta falha para conseguir entrar em locais sem ter autorização.

Esses métodos de abertura de fechaduras podem ser utilizados por chaveiros e também podem ser utilizadas em casos de esquecimento de chaves ou por autoridades civis, porém, o uso para fins ilícitos é crime.

É um método de entrada indetectável a olho nu, mas poderia ser facilmente revelado por um profissional de análise forense.

Esta técnica possui ferramentas úteis para um engenheiro social acessar locais sem precisar fazer arrombamentos e pode ser aprendida vendo vídeos na internet.

[31] Lock Picking: Termo da língua inglesa usada para abrir uma fechadura.

Figura 5: Ferramentas de Lock Picking

Fonte Foto: http://commons.wikimedia.org/wiki/File:Lockpicking_Tools.jpg

6.1.2 Ferramentas

6.1.2.1 Shove Knife

Shove knife é uma ferramenta utilizada para arrombar portas de empresas e residências e que pode ser feita com uma haste de ferro ou comercialmente.

Para utilizá-la basta colocar acima da fechadura entre a porta e o batente, forçando para baixo e para fora até que a porta se abra.

Figura 6: Shove Knife

Fonte Foto: http://en.wikipedia.org/wiki/File:Quik-Pik_EMI_Shove_Knife,_June_2012.jpg

6.1.2.2 Chave Micha

É uma técnica de lock picking para abertura de fechaduras utilizando uma chave micha.

A chave micha deve ser de tamanho igual e espaçamento entre os cortes semelhantes à fechadura que deseja, para que funcione corretamente.

Consiste em colocar a chave na fechadura e ficar vibrando até que os pinos se encaixem de forma correta para abrir a fechadura.

Figura 7: Chave Micha

Fonte da Foto: http://en.wikipedia.org/wiki/File:Bumping_key.jpg

http://en.wikipedia.org/wiki/Lock_bumping

6.1.2.3 Raking

Raking é um conjunto de ferramentas que podem ser usadas para abrir rapidamente uma fechadura, pois ela simula uma variedade de posições de pino.

É preciso colocá-la na fechadura e fazer movimentos de cima para baixo, utilizando tensões diferentes aumentando assim a possibilidade de quebrar o bloqueio da fechadura.

Figura 8: Ferramentas de Raking

Fonte Foto: http://www.lockpicks.com/brockhage-lock-pick-set-b230.aspx

http://www.lockwiki.com/index.php/Raking

6.2 Ferramentas de engenharia social: Câmeras

As câmeras são excelentes ferramentas para os engenheiros sociais para capturar informações mais rapidamente, pois possibilitam tirar fotos das informações que precisa.

Engenheiros sociais também podem utilizar as câmeras para fazer gravações de vídeos, contudo, é preciso que a câmera seja discreta e também que não faça nenhum barulho quando a foto é tirada.

6.2.1 Tipos de Câmeras

6.2.1.1 Pequena / Compacta

Um bom exemplo de uma câmera compacta pode ser uma câmera colocada em um botão de camisa ou paletó. Ela irá gravar e salvar os vídeos em um pequeno dispositivo de armazenamento que pode caber em um bolso.

Outras opções de soluções mais “hands-on” (Nas mãos, em tradução literal) podem ser câmeras colocadas em uma caneta, isqueiro, relógio e até mesmo no

chaveiro das chaves de um carro. Todos estes exemplos podem gravar vídeos e áudio de maneira discreta.

Figura 9: Micro Câmeras

Fonte Foto: http://www.spyshops.ca/images/img0099.jpg

6.2.1.2 Aparelho Celular

Os telefones celulares auxiliam bastante o engenheiro social na realização gravações ou fotos de informações confidenciais, pois este tipo de aparelho não chama a atenção quando está sendo utilizado.

Porém é preciso que o engenheiro social tenha cuidado quando for tirar uma foto ou quando estiver fazendo uma gravação, pois alguns aparelhos podem fazer som ou emitir uma luz e isso faria com que ele fosse percebido.

6.3 Ferramentas de engenharia social: Telefone

O telefone pode se tornar uma ferramenta para um engenheiro social aplicar o “hacking”.

Um exemplo deste tipo de golpe foi aplicado pelo famoso John Draper, também conhecido como Captain Crunch . Ele utilizou de seus conhecimentos de sistemas e projetou sistemas para conseguir realizar chamadas gratuitas.

Outro exemplo do Crunchm foi perceber que um apito de uma caixa de cereal era capaz de emitir o mesmo tom de frequências que era utilizado pela AT&T.

Iremos mostrar algumas ferramentas que auxiliam o engenheiro social a fazer seus trabalhos de maneira mais fácil.

6.3.1 Caller ID Spoofing

Hoje em dia muitas residências e aparelhos celulares possuem identificador de chamadas.

Com o identificador de chamadas, podemos visualizar o número de quem está nos ligando, desta forma poderemos decidir se atendemos ou não a chamada.

O primeiro identificador de chamadas foi inventado na Grécia por George Theodore.

Assim como e-mails falsos pode omitir ou alterar o remente do e-mail, Caller ID spoofing pode fazer uma chamada parecer ser de qualquer outro número de telefone.

Com este programa o engenheiro social poderá fazer uma chamada alterando o ID de seu telefone.

Figura 10: Exemplo de Caller ID

Fonte: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTArPFeCgXhmn7Omrv2IOgb-oMdGCHFGr0YJgRLJm_fRX1hjUAC

Um engenheiro social pode utilizar este recurso para indicar que a chamada está sendo feita de uma:

- Empresa de entrega

- Fornecedora de serviço de telefonia, água, internet, etc.
- Empresa parceira
- Filial da empresa
- Gerente ou Diretor da empresa

6.3.2 Caixa Postal

Um dos principais ataques que podem ser feitos por telefone celular é ouvir as mensagens da caixa postal do alvo.

Muitas pessoas utilizam este recurso que lhes permite entrar em seu correio de voz, porém, alguns se esquecem de alterar sua senha, deixando a senha padrão, que em muitas vezes é “1234 ou 1010”.

Se um atacante conseguir obter o número de telefone celular das vítimas e com isso ter acesso a sua caixa postal, ele poderá ouvir suas mensagens confidenciais e utilizar estas informações para lançar um ataque de engenharia social.

6.4 Ferramentas de engenharia social Baseada em computador

Hoje em dia muitas informações circulam na rede mundial de computadores, desta forma, um bom rastreamento das informações é um aspecto importante para um engenheiro social.

Para conseguir informações do alvo o engenheiro social precisara combinar sistemas de extração de informações, bem como ferramentas físicas.

Iremos apresentar algumas ferramentas que os engenheiros sociais usam. Essas ferramentas são voltadas para a coleta de informações, dados e até mesmo pode ser usado o Metasploit Framework para testar a infraestrutura da empresa.

6.4.1 Toolkit (SET)

Toolkit (SET) foi desenvolvido por David Kennedy e é uma ferramenta padrão para aplicar testes de penetração e ataques de segurança utilizando engenharia social.

É uma ferramenta muito utilizada por profissionais da área de segurança, pois pode ser utilizado para análise e prevenção de tentativas de ataques em um ambiente típico de engenharia social.

Figura 11: Kit de Ferramentas de Engenharia Social
Fonte da Foto: https://www.trustedsec.com/files/Set-Box_2.png

6.4.2 Maltego

Maltego é um software utilizado pela área de inteligência e perícia, possibilitando a varredura e coleta de informações de maneira eficiente. Possui uma interface gráfica de visualização, permitindo identificar, localizar, agregar e visualizar as relações entre as informações.

Ele encontra ligações entre os bits de informação ele faz o trabalho duro de busca de informação, tais como endereços de e-mail, sites, endereços IP e informações de domínio.

Maltego automatiza a forma como você pesquisa as informações, fazendo várias interligações de dados, desta forma faz com que o engenheiro social economize horas de pesquisa procurando informações e determinando onde que está à informação se relaciona.

Embora a mineração seja útil, o engenheiro social precisa fazer uma pesquisa minuciosa para pegar as informações realmente importantes.

6.4.3 Cree.py

É uma ferramenta gratuita que procura tags de localização geográficas das informações ou fotos que os usuários postam nas redes sociais, como o Twitter, Facebook, Foursquare, Instagram, Flickr, entre outros.

Cree.py reúne as informações que podem ser usadas para reconhecimento de um alvo, onde ele mora, quando ele esta em casa ou quando está viajando e para onde. Também pode ser usado para criar padrão de comportamento do alvo, identificando os lugares que ele freqüenta (lanchonetes, clubes, restaurantes favoritos e até mesmo locais que mais viaja). Esses padrões do comportamento do alvo podem ser muito úteis na engenharia social quando se trata de pretexting. Ele pode ser usado para criar relações de confiança com o alvo, com base em interesses supostamente comuns ou experiências, ele diz.

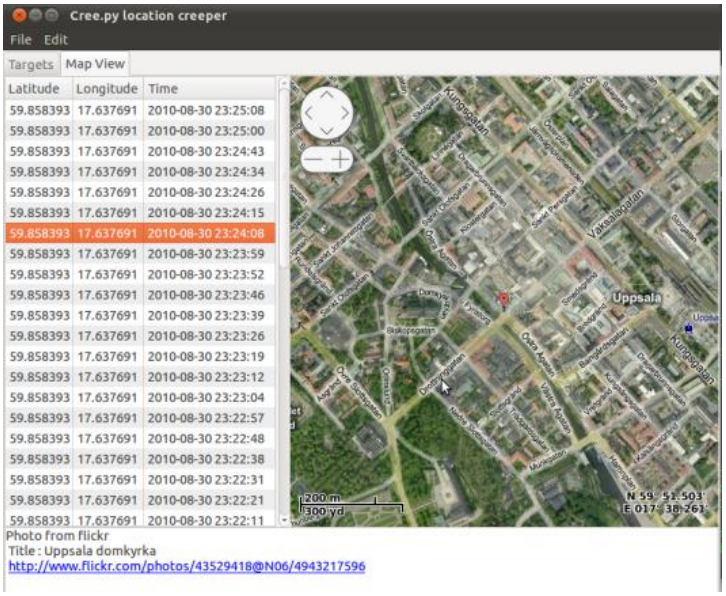

Figura 12: Foto de satélite do site Cree.py[32]

Fonte da Foto: http://ilektrojohn.github.io/creepy/creepy_mapview.png

[32] Matéria disponível em: http://www.darkreading.com/vulnerability/creepy-social-engineering-tool-pinpoints/229400561

7 Leis

As práticas de engenharia social são classificadas com um tipo de cibercriminalidade. Assim como a criminalidade tradicional, a cibercriminalidade pode assumir diversas formas e pode ocorrer a qualquer hora ou lugar. Um crime cibernético, nada mais é do que um “crime” com o uso da tecnologia e da forma física (ser humano) ou através dos dois juntos, por exemplo, à engenharia social.

O termo cibercrime, é utilizado para definir todas às más praticas e crimes cometidos com o uso da tecnologia, que podem variar de atividades contra dados, infrações de conteúdo e de copyright (direitos autorais, em tradução literal), fraudes, acessos não autorizados, pornografia infantil e cyberstalking (assedio na internet) entre outros.

Infelizmente a legislação brasileira não é tão rígida quanto aos crimes cibernéticos, de maneira que algumas condutas são comparadas e enquadradas em artigos já encontrados no código penal brasileiro.

A ausência de punições aos infratores tem gerado muitas discussões no poder legislativo brasileiro, pois se tratando de crimes cibernéticos, as leis brasileiras ainda se encontram muito defasadas, apresentado grandes “brechas” para que os criminosos não respondam por seus crimes.

A fim de preencher esta lacuna no código penal, em 09/07/2012 foi apresentado na Comissão Especial de Reforma do Código Penal, o Projeto de Lei do Senado também conhecida como (PLS) 236 conforme apresenta a agenda divulgada pelo Senado Federal:

Tipo: Comissão Especial Interna do Senado Federal

Finalidade: Examinar o Projeto de Lei do Senado nº 236, de 2012, que reforma o Código Penal Brasileiro.

Requerimento de criação: PLS 236 de 09/07/2012

17/07/2012: Designação

08/08/2012: Instalação

18/10/2013: Apresentação de Emendas - prazo final
18/11/2013: Relatórios Parciais - prazo final
02/12/2013: Relatório do Relato - Geral - prazo final
16/12/2013: Parecer Final da Comissão - prazo final

Quantidade de membros: Senadores: 11 titulares e 11 suplentes

PRESIDENTE: Senador Eunício Oliveira - PMDB - CE

VICE-PRESIDENTE: Senador Jorge Viana - PT - AC

RELATOR: Senador Pedro Taques - PDT - MT

O PLS 236/2012, traz um conjunto variado de crimes cibernéticos, que em sua maioria foram colocadas em uma parte especial, criado especificamente para este fim. O capitulo foi nomeado de “Titulo VI – Crimes Cibernéticos (pag. 84 da PLS 236/2012)”.

Além de ser enquadrado em alguns artigos da nova PLS 236/2012, juridicamente as práticas de engenharia social podem também ser enquadradas em outros artigos do código penal brasileiro, tais como:

- Estelionato - “Art. 171” – Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro fraudulento.
- A pena prevista para este artigo é de reclusão, de 1 (um) a 5 (cinco) anos, e multa.

- Falsidade Ideológica – “Art. 299” - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante.
- A pena prevista para este artigo é de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, se o documento é particular.

- Parágrafo único - Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena de sexta parte.
- Falso reconhecimento de firma ou letra.

- Furto – “Art. 155” - Subtrair, para si ou para outrem, coisa alheia móvel.
- Pena - reclusão, de um a quatro anos, e multa.
- § 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
- § 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
- § 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.
- Furto qualificado
- § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:
- I - com destruição ou rompimento de obstáculo à subtração da coisa;
- II - com abuso de confiança, ou mediante fraude, escalada ou destreza;
- III - com emprego de chave falsa;
- IV - mediante concurso de duas ou mais pessoas.
- § 5º - A pena é de reclusão de 3 (três) a 8 (oito) anos, se a subtração for de veículo automotor que venha a ser transportado para outro Estado ou para o exterior. (Incluído pela Lei nº 9.426, de 1996).
- Furto de coisa comum

- Formação de Quadrilha – “Art. 288” - Associar-se mais de três pessoas, em quadrilha ou bando, para o fim de cometer crimes.
- Pena - reclusão, de um a três anos. (Vide Lei 8.072, de 25.7.1990)
- Parágrafo único - A pena aplica-se em dobro, se a quadrilha ou bando é armado.
- Constituição de milícia privada (Incluído dada pela Lei nº 12.720, de 2012).

- Art. 288-A. Constituir, organizar, integrar, manter ou custear organização paramilitar, milícia particular, grupo ou esquadrão com a finalidade de praticar qualquer dos crimes previstos neste Código: (Incluído dada pela Lei nº 12.720, de 2012)
- Pena - reclusão, de 4 (quatro) a 8 (oito) anos. (Incluído dada pela Lei nº 12.720, de 2012)

- Violação de Correspondência – “Art. 151”. - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:
- Pena - detenção, de um a seis meses, ou multa.
- Sonegação ou destruição de correspondência
- § 1º - Na mesma pena incorre:
- I - quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói;
- Violação de comunicação telegráfica, radioelétrica ou telefônica.
- II - quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida à terceiro, ou conversação telefônica entre outras pessoas;
- III - quem impede a comunicação ou a conversação referida no número anterior;
- IV - quem instala ou utiliza estação ou aparelho radioelétrico, sem observância de disposição legal.
- § 2º - As penas aumentam-se de metade, se há dano para outrem.
- § 3º - Se o agente comete o crime, com abuso de função em serviço postal, telegráfico, radioelétrico ou telefônico:
- Pena - detenção, de um a três anos.
- § 4º - Somente se procede mediante representação, salvo nos casos do § 1º, IV, e do § 3º.
- Correspondência comercial
- Invasão de Propriedade – “Art. 150”- Entrar ou permanecer, clandestina ou astuciosamente, ou contra a vontade expressa ou tácita de quem de direito, em casa alheia ou em suas dependências:
- Pena - detenção, de um a três meses, ou multa.

- § 1º - Se o crime é cometido durante a noite, ou em lugar ermo, ou com o emprego de violência ou de arma, ou por duas ou mais pessoas:
- Pena - detenção, de seis meses a dois anos, além da pena correspondente à violência.
- § 2º - Aumenta-se a pena de um terço, se o fato é cometido por funcionário público, fora dos casos legais, ou com inobservância das formalidades estabelecidas em lei, ou com abuso do poder.
- § 3º - Não constitui crime a entrada ou permanência em casa alheia ou em suas dependências:
- I - durante o dia, com observância das formalidades legais, para efetuar prisão ou outra diligência;
- II - a qualquer hora do dia ou da noite, quando algum crime está sendo ali praticado ou na iminência de o ser.
- § 4º - A expressão "casa" compreende:
- I - qualquer compartimento habitado;
- II - aposento ocupado de habitação coletiva;
- III - compartimento não aberto ao público, onde alguém exerce profissão ou atividade.
- § 5º - Não se compreendem na expressão "casa":
- I - hospedaria, estalagem ou qualquer outra habitação coletiva, enquanto aberta, salvo a restrição do n.º II do parágrafo anterior;
- II - taverna, casa de jogo e outras do mesmo gênero.

Apesar de todos os esforços do governo para combater crimes cibernéticos, infelizmente é muito difícil de enquadrar e punir pessoas que utilizam das técnicas de engenharia social, isso porque algumas das técnicas usadas nas praticas destes crimes nem podem ser consideradas como crimes. Técnicas como vasculhar o lixo quando o mesmo se encontra em locais públicos obter dados que estejam disponíveis na internet, e até mesmo conseguir algumas informações ao ouvir uma conversar em lugares públicos não pode ser tratado como cibercrime ou como crimes tradicionais. Outro fator que também deve ser lembrado, é de que algumas provas que poderiam ser usadas para capturar estes criminosos, simplesmente não tem validade em nosso território jurídico.

8 Prevenção

Empresas estão contratando profissionais em engenheira social para que possam atuar como consultores de segurança como é o caso de Kevin Mitnick, por exemplo, que antes erra um hacker especialista em golpes usando a engenharia social e hoje, tem uma empresa de segurança da informação especializada em engenharia social.

Segundo o site da empresa Cimento Tambe (http://www.cimentoitambe.com.br/) [33] Funcionários são treinados por engenheiros sociais que visam conscientizá-los da importância de sempre que forem fornecer qualquer informação, devem antes verificar se o solicitante é realmente é quem diz ser, se o setor no qual ele trabalha necessita destas informações, e a terem mais cuidado com os papéis que serão jogados no lixo e sempre lembram a todos de que eles também são parte da segurança da empresa, e que para um engenheiro social, eles são o elo mais fraco dela.

Alguns pontos citados anteriormente no decorrer deste trabalho, mostravam formar de prevenções contra possíveis ataques com engenharia social.

Não existe uma forma 100% eficaz, para evitar este tipo de ameaça, porem, as perdas e os riscos de podem, ser reduzidos significadamente se alguns pontos importantes forem melhor elaborados e cumpridos:

8.1 Pontos Importantes para empresas

Elaboração de um plano de segurança onde o mesmo abranja não só a segurança física ou tecnológica (hardwares, softwares, câmeras, etc.), mas também os funcionários que trabalham dentro da organização;

Treinamentos contínuos dos funcionários para que os mesmo sempre estejam cientes da responsabilidade que cada informação que eles detenham da empresa são importantes;

[33] Disponível em: http://www.cimentoitambe.com.br/engenharia-social-o-novo-nome-da-espionagem-industrial/

O departamento de TI deve sempre estar atento às ameaças que a empresa pode sofrer, e caso a mesma esteja sobre ataque, os mesmo deve agir de forma rápida para solucionar o problema e realizar um plano de melhoria a fim de minimizar os danos e evitar futuros ataques;

Deve se tomar um cuidado muito grande com a inclusão de novos funcionários na empresa. Quando isso acontecer, os mesmos devem ser apresentados a todos os responsáveis do departamento a fim de evitar infiltrações de espiões ou outros tipos de invasores;

8.2 Pontos Importantes para pessoas comuns

Muito cuidado ao utilizar smatphones ou tablets em locais públicos, pois os mesmos podem apresentar um risco a suas informações, de maneira que ao usar este recurso, é sempre importante se certificar que não exista ninguém olhando por cima dos nossos ombros;

Nunca fornecer informações pessoais por telefone, como CPF, RG, números de conta bancaria, senhas, ou outro tipo de informações, possam ser usas para possíveis ataques, sem que se tenha certeza de quem esta do outro lado;

Cuidado com as correspondências nas caixas de correios, para que as mesmas não sejam roubadas;

Sempre avaliar quais e como realizar o descarte correto de informações, como contas pagas, cartões de credito vencidos entre outras;

CONSIDERAÇÕES FINAIS

Este trabalho abordou o tema engenharia social a fim de esclarecer seu significado e suas formas de atuação, assim como mostrar que a informação é o bem mais valioso para organizações e pessoas e demonstrar a importância na proteção das mesmas.

Pôde-se concluir que grande parte dos problemas envolvendo segurança da informação estão diretamente ou indiretamente ligados a engenharia social, pois estes estão relacionados à falhas humanas. Pessoas podem ser influenciadas, manipuladas, enganadas para divulgar informações ou simplesmente não as protegem de maneira eficiente, muitas vezes devido à falta de conhecimento e treinamentos sobre o assunto.

O objetivo estabelecido inicialmente foi atingido, tornando este trabalho um instrumento de conscientização sobre a engenharia social, de maneira que ao final de sua leitura, seja possível identificar um ataque, reconhecer um possível engenheiro social, entender as técnicas e formas de coleta de informações.

REFERÊNCIAS

MITNICK, KEVIN; WOZNIAK, STEVE; L. SIMON, WILLIAM. Ghost in the Wires: **My Adventures as the World's Most Wanted Hacker**. Back Bay Books, 24 de Abril de 2012, 448 páginas.

MITNICK, KEVIN; WOZNIAK, STEVE; L. SIMON, WILLIAM. **The Art of Deception: Controlling the Human Element of Security**. Wiley, primeira edição, 17 de outubro de 2003, 368 páginas.

MITNICK, KEVIN; WOZNIAK, STEVE; L. SIMON, WILLIAM. **The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers**. Wiley, 27 de dezembro de 2005, 288 páginas.

HADNAGY, CHRISTOPHER; WILSON, PAUL; **Social Engineering: The Art of Human Hacking**. Wiley, primeira edição, 21 de dezembro de 2010, 416 páginas.

BOOTHMAN , NICHOLAS. **How to Make People Like You in 90 Seconds or Less**. Workman Publishing Company, 15 de setembro ed 2000, 160 páginas.

PIPKIN, DONALD. **Halting the Hacker: A Practical Guide to Computer Security**. Prentice Hall, segunda edição. 5 de setembro de 2002, 384 páginas.

WILDING, EDWARD**. Information Risk And Security: Preventing And Investigating Workplace Computer Crime**. Gower Pub Co, 31 de maio de 2006, 350 páginas.

MASLOW, ABRAHAM. **Hierarquia das Necessidades de Maslow**. Recuperado em 10 abril de 2008. Disponível em http://www.businessballs.com/maslow.htm.

Long, Johnny. **No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing**. Syngress, primeira edição, 21 de fevereiro de 2008, 384 páginas.

ADLER, RONALD; RODMAN, GEORGE. **Understanding Human Communication**. Oxford University Press, décima edição, 1 de fevereiro de 2008, 496 páginas.

CIALDINI, ROBERT. **Influence: The Psychology of Persuasion**. Collins, edição revisada, 15 de julho de 1993, 336 páginas.

Offensive Security Team, disponível em http://www.offensive-security.com/about.php. Acessado pela última vez em 11/10/2013.

LockWiki, disponível em http://www.lockwiki.com/index.php. Acessado pela última vez em 01/11/2013.

The Social Engineer Official Website. Disponível em http://social-engineer.org. Acessado pela última vez em 20/10/2013.

David Kenny, TrustedSec, disponível em https://www.trustedsec.com/. Acessado pela última vez em 19/09/2013.

TechRepublic, disponível em http://www.techrepublic.com.com/ . Acessado pela última vez em 25/09/2013.