INVASÃO A SISTEMAS USANDO ENGENHARIA SOCIAL

Wagner Andrade de Lucena

11 de Maio de 2016

Resumo

Este artigo aborda o uso da engenharia social como meio de enganar as pessoas e realizar invasões a sistemas fechados. Os Engenheiros Sociais estão se aperfeiçoando cada vez mais para se utilizar do poder de persuasão, criatividade e ingenuidade das pessoais para extrair informações tão relevantes que a partir delas é possível conseguir senhas de sistemas e prejudicar as vítimas, tanto financeiramente, como emocionalmente. Desta forma, é importante expor seus meios de ação e como tomar cuidado para não cair nesse golpe usado frequentemente.

Palavras-chave: engenharia social, sistema, informação, pessoa, invasão, senha

1 Introdução

Não há como negar que hoje estamos vivendo na Era da Informação ou Era Digital. Com os avanços tecnológicos, principalmente com a popularização da Internet, o uso da informação no mundo digital pode ser utilizado de diversas formas, como por exemplo, para a geração de conhecimento, para comunicação através de blogs ou redes sociais e até para ganhos financeiros de forma lícita. Porém, para os maus intencionados, a informação pode ser utilizada para prejudicar empresas e pessoas, tanto financeiramente, como para o cometimento de crimes contra a honra, como calúnia, difamação e injúria.

No que diz respeito ao uso da informação para ganhos financeiros de forma ilícita, pode ser citado o furto de informações de cartões de crédito de diversas pessoas para uso em compras online, a obtenção de informações bancárias para invadir uma conta online e realizar a transferência de dinheiro e o furto de projetos inovadores de empresas, através de invasão aos seus sistemas e posteriormente a venda para empresas concorrentes. Portanto, informação é dinheiro.

Já para o cometimento de crimes contra honra, podemos citar a invasão a perfis de redes sociais para denegrir a imagem de uma pessoa ou empresa. Para o cometimento dessas condutas maliciosas citadas anteriormente, os criminosos, na maioria das vezes, usam da Engenharia social para furtar informações.

Engenharia social, como salienta Wendt e Nogueira Jorge, "é a utilização de um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais os criminosos tenha interesse ou a executar alguma tarefa e/ou aplicativo." (2013: 21).

De acordo também com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, citado por WENDT, NOGUEIRA JORGE, 2013, p.21), a Engenharia social é "um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações."

Pessoas são mais fáceis de serem enganadas do que computadores. Por conta disso, a demanda em delegacias especializadas em crimes virtuais só cresce no Brasil. Cada vez mais as pessoas estão sendo enganadas de diversas formas com o uso de Engenharia social. Os criminosos usam da criatividade para extrair dados confidenciais. Portanto, nos parágrafos seguintes vamos expor como as vítimas são facilmente enganadas e maneiras de prevenção. Além disso, serão citados exemplos práticos.

2 Engenharia social

Existe uma frase que diz: “Pessoas são extremamente mais fáceis de Hackear do que computadores”. Isso é comprovadamente uma verdade. Os computadores ou sistemas podem estar protegidos com os mais diversos tipos de mecanismos de segurança, como firewalls, softwares anti-vírus, senhas, controles de acesso etc, porém nada disso adianta caso os seres humanos não tenham consciência de que fornecer uma informação relevante para o engenheiro social, pode ser a chave para a quebra de segurança de um sistema.

Para ficar mais claro como isso acontece, vejamos uma conta de e-mail. Existem serviços de e-mail que oferecem como mecanismo de recuperação de senha, uma resposta a uma pergunta de segurança que foi cadastrada previamente pelo usuário. Desta forma, um engenheiro social que queira invadir um e-mail, entra no serviço, coloca o e-mail a ser atacado e clica na opção referente a recuperação de senha. Lá ele vai encontrar a pergunta de segurança que o usuário cadastrou. Digamos que ele colocou como pergunta de segurança: “Qual o nome de minha mãe?” e como resposta está realmente o nome da mãe do usuário. Para o engenheiro social, quando se deparar com essa informação, foi a facilitação necessária para invadir a conta. Basta saber o nome da mãe do usuário para entrar. E isso não seria um problema, pois ele se utiliza de diversos mecanismos e ferramentas para descobrir o nome da mãe do usuário. Uma delas é buscando a resposta na Internet, através, por exemplo, de redes sociais. Como as pessoas expõe suas informações sem se preocupar em protegê-las, o engenheiro social, nesse caso, pode descobrir apenas vasculhando sua rede social.

Perceba a facilidade que um engenheiro social teria para invadir uma conta de e-mail. Isso deve-se muito a não preocupação dos usuários em não proteger melhor suas informações. É assim que os engenheiros sociais trabalham. Procuram brechas de segurança que as pessoas deixam para invadir. No caso do e-mail, o usuário poderia ter utilizado uma pergunta de segurança, cuja resposta fosse confidencial. Além disso, ele poderia ter protegido melhor suas informações pessoais nas redes sociais. Só uma atitude dessa, dificultaria bastante a ação do atacante.

Um ataque de engenharia social requer um conjunto de informações prévias que são a base para a ação do criminoso. Ele antes de praticar uma ação contra uma vítima, faz um planejamento, ou seja, ele estuda a vítima, verifica seus pontos fracos, busca informações dela em fontes abertas, para depois investir contra a mesma.

Acontecem muitos casos em que os criminosos que se utilizam de engenharia social ligam para a residência das pessoas e já com as informações previamente adquiridas da Internet, por exemplo, simulam ser de uma instituição confiável, como órgãos do governo, bancos, sites de grandes lojas, operadoras de telefonia, tudo isso para usar como isca e coletar informações como senhas de banco, números de cartões de créditos ou senhas de WiFi. Eles fazem isso com diversas pessoas, e uma coisa é certa, pelo menos uma será vítima. Eles usam as vulnerabilidades das vítimas, frente a determinadas situações do cotiano, como por exemplo, uma pessoa pode estar passando por uma situação de endividamento financeiro numa instituição bancária e o criminoso sabendo disso, se passa por um gerente que irá tentar ajudá-la a quitar sua dívida, extinguindo os juros, para tanto, precisa da senha do banco para efetuar tal transação. Como a vítima já está passando por uma situação delicada, acaba acreditando e fornecendo a informação.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, citado por WENDT, NOGUEIRA JORGE, 2013, p.21-22), apresenta alguns exemplos de ataques pelos engenheiros sociais, são eles:

- Exemplo 1: você recebe uma mensagem de e-mail, cujo remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de Internet Banking está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso à conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso à conta bancária e enviá-la para o atacante.

- Exemplo 2: você recebe uma mensagem de e-mail dizendo que seu

computador está infectado por um vírus. A mensagem sugere que você instale uma ferramenta disponível em um site da Internet para eliminar o vírus de seu computador. A real função desta ferramenta não é eliminar o vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.

- Exemplo 3: algum desconhecido liga para a sua casa e diz ser do suporte técnico do seu provedor. Nesta ligação ele diz que sua conexão com a Internet está apresentando algum problema e,então, pode sua senha para corrigi-lo. Caso você entregue sua senha, este suporte técnico poderá realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso à Internet e, portanto, relacionando tais atividades ao seu nome.

Nos casos apresentados acima mostra única e exclusivamente que as informações sensíveis, como senhas, foram passadas pelos usuários, ou seja, típicos casos de ataques por engenharia social. Mostra que as pessoas são os elos mais frágeis para se entrar num sistema protegido.

Não existe um padrão característico nas ações dos autores nesses tipos de ataques. O que vale é a criatividade do autor dessas ações e sua capacidade de persuadir as vítimas a oferecer as informações desejadas. Eles exploram os aspectos físicos nos ambientes e psicológicos das pessoas.

No aspecto físico dos ambientes, a Figura 1 ilustra como eles agem.

Note na figura como as pessoas facilitam para a ação do engenheiro social no aspecto físico. Isso acontece muito em empresas. Eles exploram o local de trabalho. Muitos funcionários não se preocupam em proteger as informações sigilosas. Talvez por conta da inexistência de uma política de segurança sólida dentro da corporação, talvez pela falta de treinamento dos funcionários, no que diz respeito a proteger melhor as informações sensíveis da empresa.

Pode-se tirar várias situações dessa imagem. A citar:

- Exemplo 1: Há um funcionário no telefone informando sua senha. O interlocutor poderia ser um engenheiro social se passando por um técnico da TI e conseguiu convencê-lo a passar essa informação confidencial.

Figura 1: http://blog.segr.com.br/engenharia-social-uma-ameaca-silenciosa-nas-empresas/

Inclusive existem diversas pessoas na sala ouvindo essa informação, ou seja, alguém ali dentro, poderia ser um engenheiro social. Para proteger a informação, o funcionário não deveria estar passando informações confidenciais pelo telefone. Essa senha poderia ser de um sistema, tanto pessoal, quanto corporativo e ser aplicada num golpe.

- Exemplo 2: Perceba também que existe um visitante olhando a tela de uma funcionária, a qual está acessando informações privadas. O visitante poderia ser um intruso. Ele poderia ter utilizado de técnicas de engenharia social para estar naquela sala, capturando informações sensíveis, para posteriormente aplicar um golpe. Observa-se que ninguém ali está preocupado em protegê-las. O ideal era que a máquina da funcionária estivesse posicionada de tal forma que ninguém tivesse a visão da tela, só ela mesma. A não permissão de pessoas estranhas num ambiente onde tem informações sensíveis, seria outro ponto a ser protegido, como ter controle de acesso bem rígido.

- Exemplo 3: Engenheiros sociais também vasculham lixeiras, pois po-

dem conter informações necessárias para aplicar o golpe. Observe na imagem uma lixeira com diversos documentos oficiais. Isso é o "prato cheio" para eles. Ali pode conter diversas informações confidenciais sobre a empresa, principalmente de sistemas. O ideal, nesse caso é utilizar fragmentadoras de papéis.

- Exemplo 4: Observe uma mesa na imagem. Nela contém uma anotação com usuário e senha. Isso é comum em empresas, nas quais os funcionários como forma de lembrar o login e senha do sistema, deixam essas informações em papéis em cima da mesa. Isso é um perigo, pois um engenheiro social, pode por exemplo, estar disfarçado de funcionário de serviços gerais e facilmente obter essa informação, somente simulando uma limpeza.

No aspecto psicológico, os engenheiros sociais exploram o lado sentimental das pessoas. Por exemplo, eles enviam e-mails para milhares de pessoas dizendo ser da Receita Federal, na qual informa que o indivíduo tem um problema pendente a ser resolvido no órgão e para adiantar, precisa que ele clique no link ou arquivo em anexo. Dentre milhares de pessoas, uma deles pode ter realmente esse problema e acreditando na mensagem de e-mail acaba abrindo o arquivo, o que na verdade seria um arquivo malicioso que infectou a máquina com o objetivo de colher informações confidenciais, como senhas de redes sociais, de bancos, de sistema de empresas, números de cartões de créditos, ou seja, todo aquele sistema fechado que o indivíduo usa, fica vulnerável por conta somente da abertura de um arquivo enviado por e-mail.

Segundo Wendt e Nogueira Jorge, "as principais técnicas utilizadas pelos engenheiros sociais são baseadas na manipulação da emoção de seus "alvos". Assim, trabalham principalemte com o medo, a ganância, a simpatia e, por último, a curiosidade. O usuário de internet, motivado por essas circunstâncias, acaba prestando informações que não devia ou clica em links que direcionam a sites de conteúdo malicioso e/ou para execução de algum código maléfico em sua máquina." (2013: 23-24).

Ainda segundo Wendt e Nogueira Jorge, "outro aspecto a destacar sobre

a engenharia social é a utilização do chamado efeito saliência: quando o criminoso usa, para chamar a atenção de suas potenciais vítimas, algum assunto que está em destaque na mídia mundial, nacional e/ou regional, como a morte de um ator famoso, um acidente de grandes proporções etc." (2013:24).

A engenharia social também pode ser utilizada a favor do bem. É a *engenharia social contra o crime*. As forças policiais também a usa nas investigações criminais, principalmente nos casos de crimes cibernéticos. Por exemplo, o policial pode se infiltrar num fórum fechado, cujo o teor do site são imagens ou vídeos de crianças ou adolescentes em cenas pornográficas. Ao se infiltrar, ele poderia coletar indícios sobre a prática desse crime. Vale ressaltar que para infiltração de policial em organizações criminosas requer autorização judicial, como prevê o Art. 3º, VII, da Lei 12.850/12.

No âmbito de organizações empresariais ou públicas, segundo Kevin Mitnick (2005, citado por WENDT, NOGUEIRA JORGE, 2013, p.23), a utilização de algumas técnicas são essenciais para a prevenção de ataques por engenharia social. Ele apresenta as seguinte:

- Desenvolver protocolos claros e concisos que sejam cumpridos consistentemente em toda a organização;
- Organizar um treinamento em consciência da segurança;
- Criar regras simples que definam quais são as informações confidenciais;
- Elaborar uma regra simples segundo a qual sempre que alguém solicitar uma ação restrita (ou seja, uma ação que envolva a interação com um equipamento relacionado a um computador, cujas consequências não sejam conhecidas), a identidade do solicitante seja verificada de acordo com a política da empresa;
- Desenvolver uma política de classificação de dados;
- Treinar funcionários para resistir a ataques de engenharia social;
- Testar a suscetibilidade de seu funcionário a ataques de engenharia social, conduzindo uma avaliação de segurança.

Ainda no âmbito de organizações empresariais ou públicas, Mitnick e Simon (2005: 203), apresentam algumas orintações para o treinamento dos seus funcionários:

- Fique ciente de que certamente os engenheiros sociais vão atacar sua empresa em algum momento, talvez repetidamente. Pode haver uma falta de consciência generalizada de que os engenheiros sociais constituem uma ameaça substancial. Muitas pessoas nem sequer têm consciência de que essa ameaça existe. Geralmente elas não esperam ser manipuladas e enganadas, e são pegas desprevenidas por um ataque de engenharia social. Muitos usuários da Internet têm recebido um e-mail supostamente enviado da Nigéria solicitando ajuda para fazer a transferência de uma soma substancial de dinheiro para os Estados Unidos. No e-mail é oferecida uma porcentagem da soma bruta em troca de assistência. Mais tarde, solicita-se que a vítima adiante uma quantia referente a algumas taxas para iniciar o processo de transferência, e ela fica de bolso vazio. Uma senhora em Nova York caiu no conto-do-vigário recentemente e pediu emprestado a seu empregador centenas de milhares de dólares para pagar essas taxas. Em vez de passar seu tempo de lazer em seu iate novo, que pretendia comprar, ela está tendo de considerar a perspectiva de dividir uma vaga na penitenciária federal. As pessoas realmente caem nesses ataques de engenharia social; caso contrário, os vigaristas nigerianos parariam de enviar e-mails.

- Use o desempenho de papel para demonstrar a vulnerabilidade pessoal a técnicas de engenharia social e para treinar funcionários em métodos de resistência. A maioria das pessoas opera sob a ilusão de invulnerabilidade, considerando-se espertas demais para serem manipuladas, persuadidas, enganadas ou influenciadas. Elas acreditam que essas coisas só acontecem a pessoas 'tolas'. Existem dois métodos para ajudar os funcionários a entender sua vulnerabilidade e torná-los verdadeiramente cientes dela. Um deles é demonstrar a efetividade da engenharia social 'colocando alguns funcionários no fogo' antes de participarem de um seminário de consciência de segurança e fazendo-os relatar suas ex-

periências durante o evento. Outra abordagem sugere a análise de casos de engenharia social para ilustrar como as pessoas são suscetíveis a esses ataques. Em qualquer um dos casos, o treinamento deve examinar o mecanismo dos ataques, analisando por que funcionou e discutindo como podem ser reconhecidos e como é possível resistir a eles.

- Procure esclarecer aos trainees que eles se sentirão tolos se forem manipulados em um ataque de engenharia social depois do treinamento. O treinamento deve enfatizar a responsabilidade de cada funcionário por ajudar a proteger ativos corporativos sensíveis. Além disso, é vital que os responsáveis pelo treinamento re-conheçam que a motivação para seguir protocolos de segurança em certas situações só aumenta quando se entende por que esses protocolos são necessários. Durante o treinamento em consciência da segurança, os instrutores devem dar exemplos da proteção assegurada pelo protocolo e dos danos que podem recair sobre a empresa se as pessoas o ignorarem ou forem negligentes com relação a seu cumprimento. Também é útil ressaltar que um ataque de engenharia social bem-sucedido pode pôr em risco as informações do funcionário e de seus amigos e colegas na empresa. O banco de dados dos recursos humanos da empresa pode conter informações pessoais extremamente valiosas para ladrões de identidade. Mas o fator mais motivador pode ser o fato de que ninguém gosta de ser manipulado, enganado, trapaceado. Desse modo, as pessoas são altamente motivadas a não serem vítimas de vigaristas, porque isso as fará se sentir tolas ou estúpidas.

3 Ferramentas utilizadas na Engenharia social

Existem diversas ferramentas que são utilizadas para a utilização da engenharia social. Elas automatizam as buscas por informações referentes aos alvos de interesse dos criminosos. São utilizadas também por forças policiais para a realização de investigações criminais.

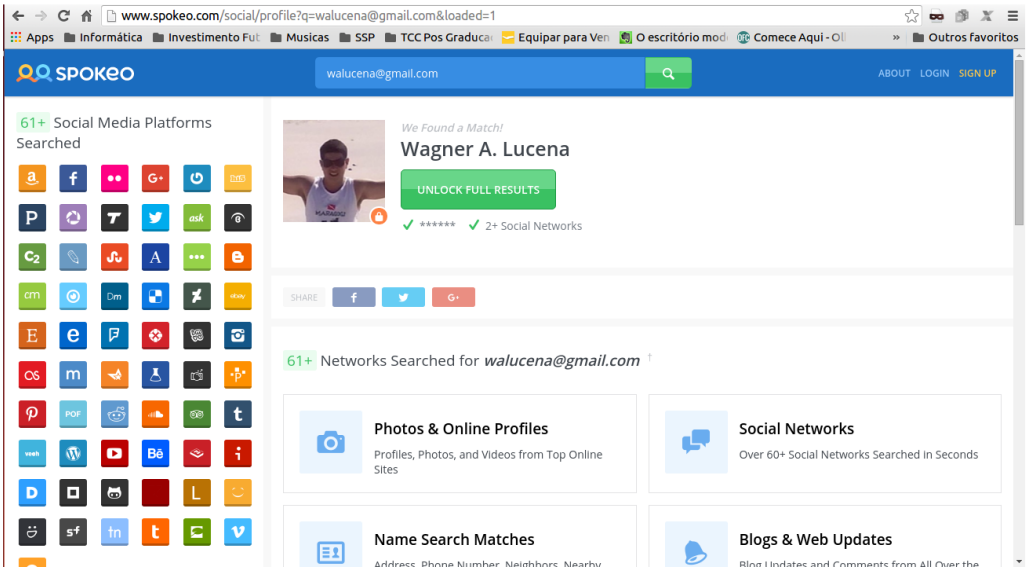

Figura 2: http://www.spokeo.com/social/profile?q=walucena@gmail.com&loaded=1

Uma delas é o Spokeo. "Foi desenvolvido para que você possa buscar informações sobre amigos, parentes e até pessoas indesejadas. Porém, o Spokeo vai além do que outros serviços faze, importando todos os seus contatos de e-mail. A partir disso, e com o pagamento de alguns dólares mensais, ele monitora continuamente seus contatos e irá informar caso alguma dessas pessoas faça alguma atualização ou ação em qualquer parte do mundo online – a página inicial do site promete ajudá-lo e descobrir fotos pessoais, vídeos e segredos de seus amigos e colegas". (J.R, 2009, citado por WENDT, NOGUEIRA JORGE, 2013, p.23)

A Figura 2 mostra um exemplo na busca por informações do proprietário do e-mail walucena@gmail.com. Como resultado, o aplicativo apresentou uma conta na rede social Twitter com nome, sobrenome e uma foto. Foi constatado que realmente trata-se da pessoa que utiliza o e-mail citado. Para um engenheiro social, essa informação pode ser o pontapé inicial para realizar um ataque. Vale ressaltar que o exemplo utilizado foi a versão gratuita do aplicativo. A versão paga apresentaria um leque maior de informações.

Outra ferramenta é o Maltego. Esse aplicativo se concentra em fornecer

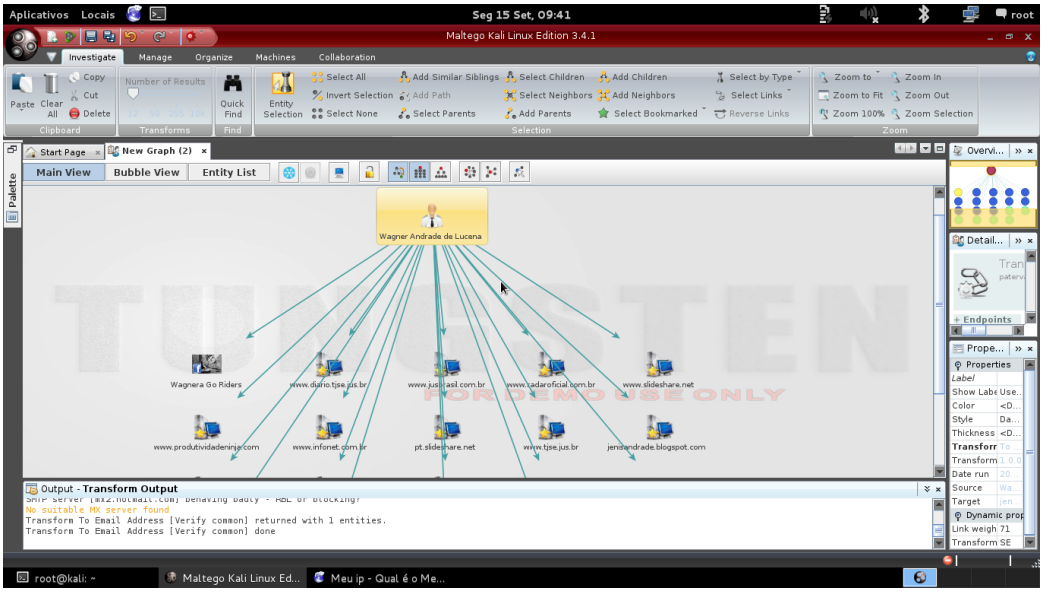

Figura 3: Software Maltego que pode ser adquirido no site www.paterva.com

como resultado, informações provenientes de fontes abertas da Internet. É um processo automatizado. Basta fornecer, através de uma gama de opções, um critério de entrada, como por exemplo, nome completo do alvo, número de telefone, nome do perfil do alvo no Facebook, endereço eletrônico, etc.

A imagem a seguir mostra um exemplo de pesquisa com o nome Wagner Andrade de Lucena. Note que as informações são apresentadas em modo gráfico. Fica mais intuitivo e melhor de ser visualizado.

Ao clicar em um desses resultados, irá abrir uma janela, e na aba propriedades tem o link com o endereço onde a informação referente ao nome pesquisado foi encontrada. Ao entrar no endereço, a página é aberta e apresenta as informações.

No caso citado, observe na imagem a seguir que abriu um blog, no qual contém além do nome pesquisado, outras informações que podem ser úteis para o engenheiro social, tais como, e-mail do alvo, a provável universidade onde o alvo estuda ou estudou, nome de pessoas ligadas ao alvo e pelo teor do assunto do blog, pode-se deduzir que o alvo trabalha com tecnologia.

Além dessas, outras informações podem ser coletadas sobre o alvo, como

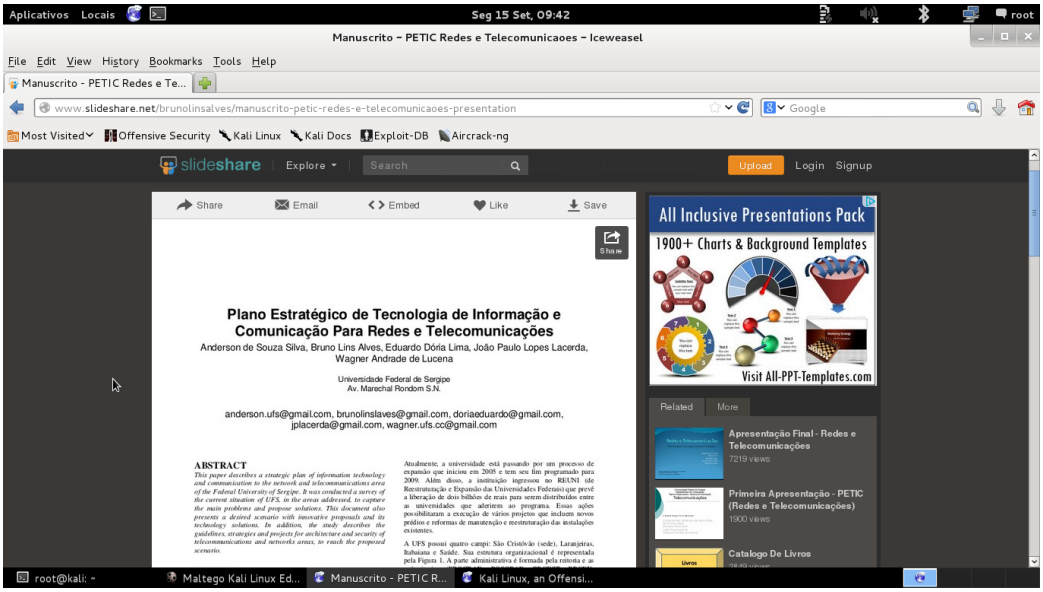

Figura 4: http://pt.slideshare.net/brunolinsalves/manuscrito-petic-redes-e-telecomunicaoes-presentation

RG, CPF, redes sociais, etc.

Portanto, é uma ferramenta poderosa que facilita o trabalho do engenheiro social, pois a coleta de informações não é manual e sim automatizada.

4 Estudo de Caso

Para resguardar as vítimas, os nomes apresentados serão fictícios.

Duas amigas jovens, Joana e Carla se comunicavam bastante através da rede social Facebook. Cada uma tinha seu perfil na rede social. As duas foram vítimas de engenharia social.

Em casa, Joana olhando sua conta de e-mail abriu sua caixa de correio eletrônico através de seu notebook. A primeira mensagem de e-mail tinha como título: "Veja as suas fotos da última festa". Como Joana era uma garota super curiosa, acabou abrindo o arquivo em anexo no e-mail, porém para ela nada aconteceu. Apareceu uma página com a seguinte informação: "Página não encontrada". Até aí tudo bem. Joana apagou a mensagem e foi

ler seus outros e-mails.

O que Joana não sabia era que o arquivo que ela abriu era malicioso e foi vítima de engenharia social. O programa instalado em sua máquina, sem ela perceber, monitorava todos os suas atividades no computador, incluindo todas as senhas que ela digitava para entrar em sites restritos, como o Facebook.

O indivíduo que enviou esse e-mail para Joana já a conhecia previamente. Ele sabia que Joana era uma garota curiosa, que gostava de festas e escolheu uma forma de persuadir Joana a abrir tal arquivo para poder monitorá-la através do computador.

Aconteceu que como Joana entrava muito no Facebook, o indivíduo conseguiu capturar a senha dela. Sendo assim, nos períodos da noite, ele entrava no Facebook de Joana, se passando por ela e conversava com todos seus amigos, incluíndo sua melhor amiga Carla.

Nesse processo, tarde da noite, o criminoso começa a conversar com Carla, através do Facebook de Joana. Ele a convence de conversarem no Skype, pois seria melhor através da Web Cam. Carla acreditando que seria Joana, aceita o convite e vai conversar através da Web Cam com o indivíduo. Porém, o criminoso a convence de que só ela deveria ligar a Web Cam, pois a dele estava quebrada e não poderia aparecer. Carla acredita na conversa e liga.

O que aconteceu foi que Carla estava somente com a parte de baixo das vestimentas, ou seja, semi-nua. O indivíduo a viu dessa forma e gravou toda a cena.

Carla e Joana só foram descobrir que foram vítimas, após se encontrarem na escola no outro dia. Foi aí que notaram que a conta do Facebook de uma delas foi hackeada, ou seja, alguém entrou indevidamente.

Após o episodio, as duas foram registrar Boletim de Ocorrência na delegacia especializada em combate a crimes cibernéticos para que as providências fossem tomadas.

O que vale ressaltar aqui é o descuido que as duas garotas tiveram para se tornarem vítimas.

Com relação a Joana, o descuido foi abrir um arquivo de um e-mail de desconhecido. O engenheiro social usou a curiosidade dela.

Já Carla, se descuidou ao não perceber as conversas genéricas que estava tendo com o indivíduo. Como elas eram muito amigas, poderia ao menos antes de iniciar uma comunicação por vídeo, perguntar a Joana um segredo entre as duas. A depender da resposta, ela teria certeza que se tratava da amiga, porém isso não aconteceu.

5 Considerações finais

As pessoas devem ficar mais atentas e resguardar com maior segurança seus dados pessoais. Desta maneira, minimiza a situação de ser vítima de um golpe utilizado tão frequentemente que é a engenharia social.

Portanto, iniciativas educacionais no sentido de expor a sociedade os cuidados que devem tomar com suas informações pessoais. O trabalho de prevenção é muito importante. Isso ajuda a diminuir o número alto de ocorrências em delegacias especializadas em combater crimes cibernéticos.

No caso de funcionários que trabalham em organizações privadas ou públicas, é importante que as instituições tenham uma política forte de segurança, no que tange as informações sensíveis. É importante um trabalho de treinamento constante com os funcionários para que evitem cair na cilada do engenheiro social.

6 Referências bibliográficas

_____. **Definição de Engenharia social, Cartilha de segurança, cert.br**. Disponível em: http://cartilha.cert.br/glossario/#e Acesso em 22 de setembro de 2015.

MITNICK, Kevin; SIMON, William. **A arte de enganar: Controlando o Fator Humano na Segurança da Informação.** São Paulo: Pearson Prentice Hall, 2003.

MITNICK, Kevin; SIMON, William. **A arte de invadir: as verdadei-**

ras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos. São Paulo: Pearson Prentice Hall, 2005.

WENDT, Emerson; NOGUEIRA JORGE, Higor Vinicius. **Crimes Cibernéticos: Ameaças e Procedimentos de Investigação.** 2º edição, Rio de Janeiro, Brasport, 2013.

J.R. Raphael. **Engenharia social: eles sabem seus segredos e contam para todo mundo. PC WORLD.** Disponível em: http://pcworld.com.br/dicas/2009/03/23/en social-eles-sabem-seus-segredos-e-contam-para-todo-mundo/. Acesso em: 02 março 2016.

FONSECA, Paula Fernanda. **Gestão de Segurança da Informação: O Fator Humano**. Disponível em: http://www.ppgia.pucpr.br/ jamhour/RSS/TCCRSS08A/Paul %20Artigo.pdf. Acesso em: 04 de março de 2016.

_____. **Maltego.** Disponível em https://www.paterva.com/web6/products/download.php. Acesso em: 04 de março de 2016.

_____. **Spokeo: Search people.** Disponível em http://www.spokeo.com/social/profile?q=waluce Acesso em: 04 de março de 2016.