

ENGENHARIA SOCIAL E A ALEATORIEDADE NA ESCOLHA DO ALVO

José Tenório Abs Junior¹

Velcir Barcaroli²

RESUMO

No universo da Tecnologia da Informação, muito se foca em criptografia de dados, firewalls e programas farejadores de vírus, como ferramentas de combate que objetivam minimizar ao máximo as chances de acesso indevido às informações nos ambientes institucionais e domésticos. No entanto, as brechas de segurança não estão restritas apenas às vulnerabilidades técnicas. É nesse cenário que surge a figura do Engenheiro Social, um criminoso que por meio de técnicas de convencimento busca explorar a ingenuidade do ser humano com o intuito de acessar, de forma não autorizada, os mais variados sistemas de informação. De forma aleatória, o atacante identifica seu alvo baseado em suas fraquezas, e investe sob ele com técnicas de persuasão, intimidação e pressão psicológica. Por meio de pesquisa bibliográfica e coleta de dados na internet, este artigo relata o risco provocado pela exposição descuidada de informações pessoais e de empresas, no ambiente organizacional ou em redes sociais, onde constata que um breve deslize poderá tornar qualquer indivíduo ou organização vulnerável a ponto de se tornar uma vítima em potencial.

Palavras-chave: Engenharia-social. Vulnerabilidades. Sistemas de informação.

1 INTRODUÇÃO

O desenvolvimento das tecnologias da informação e comunicação – TIC's, revolucionaram a maneira com que as pessoas interagem, seja no ambiente doméstico ou institucional. A democratização da informação, exposta a todos que desejem acessá-la, assumiu um papel fundamental no desenvolvimento das sociedades.

A internet tornou-se um poderoso motor de consumo e alavancagem de poder econômico. No Brasil, de acordo com Scudere (2007), o volume de transações on-line, no ano de 2005, representou 19,6% do volume total de transações entre empresas, atingindo um volume financeiro de US\$ 50 bilhões, um crescimento de 98% em relação ao ano anterior.

Nos milhões de servidores espalhados pelo mundo, um número inimaginável de dados, é armazenado e acessado a todo o momento. Contas bancárias, números de cartão de crédito,

¹ Graduado em Sistemas de Informação no ano de 2012 Especialista em Segurança da Informação UCEFF, 2016.

² Bacharel em Ciência da Computação UNOESC, 1998. Especialista em tecnologias e desenvolvimento de Software UFSC, 2005. Mestrando em Computação Aplicada, UPF. E-mail: velcir@uceff.edu.br.

senhas de acesso, projetos industriais milionários, relatórios confidenciais, entre outros, passaram a ser considerados ativos dentro das organizações.

De maneira similar, as informações pessoais de indivíduos que fazem uso de sistemas online, agora alimentam uma base de dados de tamanho incalculável. Estas informações, assim como no caso das instituições, passaram a ter um alto valor financeiro agregado.

De olho nestas informações, está todo o tipo de bandidagem que se possa imaginar. Mas, no universo das tecnologias da informação e comunicação, são os hackers, indivíduos com amplos conhecimentos sobre softwares e hardwares, além de habilidosos programadores, que tiram o sono dos profissionais de Tecnologia da Informação (TI), e dos especialistas em segurança da informação.

Basicamente, eles desenvolvem, incessantemente, técnicas de invasão por meios de computadores, com o propósito de roubar estes dados e usá-los em benefício próprio. Junto a eles, aparece a figura do engenheiro social, um sujeito especialista na exploração das vulnerabilidades humanas.

Motivados por objetivos financeiros ou, simplesmente, pelo desafio de burlar sistemas de segurança, o engenheiro social não faz uso de técnicas avançadas, como no caso dos hackers. Para ele, a estratégia central é o uso do dom da persuasão, somada ao seu amplo e profundo conhecimento das fraquezas e anseios humanos, com o objetivo de manipular suas vítimas e, de certa maneira, fazê-las trabalhar em seu favor.

Assim, sendo o fator humano o elo mais fraco da segurança, conforme afirma Mitnick (2003), e havendo grandes probabilidades de ser incluído nas estatísticas das vítimas de roubos de informações sigilosas, sem que necessariamente alguém tenha determinada pessoa ou empresa em particular como propósito, como defende Scudere (2007), o tema da aleatoriedade na escolha do alvo, por parte do engenheiro social, passa a ser importante variável a ser levada em consideração no momento da formatação de estratégias e políticas de segurança institucionais e domésticas.

Diante da constatação de que potenciais vulnerabilidades surgem por meio do descuido humano, levante-se a questão problema sobre quais os riscos que empresas e pessoas estão expostas por conta da exibição de informações de maneira despreocupada e sem critérios mínimos de segurança.

Neste sentido, este artigo tem por objetivo apresentar, por meio de exemplos extraídos da internet e de análises de casos encontrados na rede social *Facebook*, os riscos que o descuido com a exposição de informações pode trazer ao indivíduo ou empresas e o papel da engenharia

social na exploração das vulnerabilidades geradas pela falta de critérios na exposição destas informações.

2 REFERENCIAL TEÓRICO

Neste tópico será abordado sobre a base teórica da segurança da informação, bem como, os três sistemas de segurança.

2.1 SEGURANÇA DA INFORMAÇÃO

Com a chegada da automação de processos dentro das instituições, e devido à alta conectividade de diferentes dispositivos dentro do ambiente empresarial, naturalmente surgiu a necessidade de se armazenar e proteger uma vasta quantidade de dados e informações. Estes dados e informações, agora considerados ativos, passaram a ter uma alta importância financeira, estratégica e operacional.

A qualidade e a fidedignidade destes ativos passaram a ter relação direta com os lucros das empresas. O cruzamento e interpretação destes dados, assumiram papel crucial na estrutura das estratégias que baseiam as tomadas de decisões pelos gestores. Assim, diante da necessidade de um cuidado especial com a proteção destes dados e informações, fez surgir a Segurança da Informação.

Já, Sêmola (2003) entende a Segurança da Informação como uma área do conhecimento que tem por objetivo proteger os dados e informações contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Esta proteção, sugerida por Sêmola (2003), é justamente as três propriedades básicas da Segurança da Informação: confidencialidade, integridade e disponibilidade. Estas três propriedades podem ser assim entendidas, conforme o Quadro 1.

Quadro 1 – Três propriedades básica da segurança da informação

Confidencialidade	Tem por objetivo a preservação do teor sigiloso da informação. Isto significa que somente pessoas autorizadas terão direito de acessá-las. O direito de acesso deverá ser definido de acordo com o grau de sigilo da informação e com o cargo ocupado pelo usuário do sistema. Classificações como “confidencial”, “reservada” e “pública”, definirá o grau de sigilo da informação.
--------------------------	--

Integridade	Trata-se da proteção da informação contra alterações indevidas. Ela busca preservar a plenitude e exatidão do conteúdo.
Disponibilidade	Busca garantir que a informação esteja disponível sempre que usuários que estejam autorizadas a acessá-las as busquem nos sistemas.

Fonte: Adaptado de Sêmola (2003, p. 83).

Esta informação que consome tantos esforços por parte das instituições, para a sua proteção, não fica somente armazenada em meios físicos, como discos ou servidores. Boas partes estão arquivadas nas mentes das pessoas. E, sua totalidade, será acessada por outros seres humanos. É aqui que surge o “fator humano” que Mitnick (2003) entende como o elo mais fraco da segurança. E, é de olho nessa fragilidade que surge a figura do Engenheiro Social.

2.2 ENGENHARIA SOCIAL

A Engenharia social pode ser entendida como a exploração da falta de preparo dos recursos humanos no trato e proteção de informações sigilosas e importantes, com o objetivo único de conseguir informações privilegiadas sobre determinada pessoa ou instituição.

Mitnick (2003) defende que a o engenheiro social usa a influência e a persuasão com o objetivo de enganar as pessoas e convencê-las de que ele é alguém que na verdade não é. Peixoto (2006) define o engenheiro social, entre outras características, como uma pessoa gentil, dinâmica e criativa que tem como meta a captura de informações por meio de conversas envolventes e persuasivas.

Nakamura (2007) complementa os conceitos acima com o entendimento de que se trata de uma técnica que busca explorar as fraquezas humanas e sociais, comprometendo a segurança de indivíduos ou de uma organização.

Para Marcelo e Pereira (2005), a ignorância e inocência das pessoas são as principais ferramentas de trabalho deste golpista. O uso da persuasão, em pessoas tecnicamente despreparadas, faz com o que engenheiro social atinja com facilidade seu objetivo de acessar áreas restritas e informações confidenciais de organizações e pessoas. Esta técnica, geralmente utilizada quando não existem falhas de segurança evidentes nos sistemas, e que possam ser exploradas, possui uma excelente relação de “custo de ataque” versus “benefícios das informações roubadas”, favorável à prática da engenharia social.

Em entrevista à revista Fonte, Mitnick (2007, p. 24) ressalta:

A influência humana pode ser usada para o que é conhecido como “engenharia social”, que significa que você pode enganar, manipular ou influenciar uma pessoa, uma vítima, para conseguir que ela atenda uma solicitação, geralmente pessoas confiáveis em uma organização. Então, claro, se as empresas não treinarem seus funcionários sobre o que é a engenharia social, sobre as diferentes abordagens utilizadas pelos engenheiros sociais e treinar funcionários nas políticas de segurança e motivá-los a não quebrá-las sob qualquer circunstância, as empresas estarão correndo risco de ser atacadas pela engenharia social.

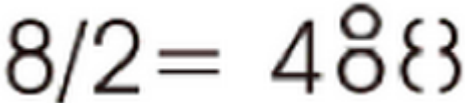
Assim, a pessoa enganada, que tem suas vulnerabilidades exploradas pelo golpista, e que é desconhecadora do valor da informação, acaba por ceder, de maneira intencional ou não, em razão da falta de treinamento, uma vez que a grande maioria dos recursos destinados à segurança são investidos apenas em tecnologia, resultando em baixo investimento no treinamento de pessoas.

O grande diferencial do modo de agir do engenheiro social, em relação aos hackers, é que eles não necessitam fazer o uso de técnicas de força bruta ou de encontrar erros em máquinas. Desenvolvem suas habilidades com ou sem o uso das tecnologias, com um único foco, que sempre será o ponto mais vulnerável em todos os processos: o ser humano.

De modo geral, o golpista explora assuntos capazes de mexer com o emocional de suas vítimas, enganando e manipulando as pessoas para que elas forneçam o conjunto de informações do seu interesse. Dissimulado, o engenheiro social assume outras personalidades, se utilizando de amizades como isca. Grande capacidade de persuasão, autoconfiança e facilidade de comunicação são características bem evidentes.

A figura 1, ilustra como Marcelo e Pereira (2005, p. 5) veem os engenheiros sociais, e explicam que “Ao perguntamos a uma pessoa qual é a metade de 8, normalmente ela responderia 4 mas o engenheiro social vê assim a resposta:

Figura 1 – Resposta do Engenheiro Social à pergunta “qual a metade de 8”?



$$8/2 = 4888$$

Fonte: Adaptado de Marcelo e Pereira (2005, p. 5).

Os autores, Marcelo e Pereira (2005, p. 5), complementam com a explicação de que a visão lógica e matemática seria a forma com que normalmente as pessoas veem a solução para

o problema e acrescentam que “Para o Engenheiro Social o mais ilógico às vezes pode ser a resposta mais óbvia para o problema”.

2.3 A ALEATORIEDADE NA ESCOLHA DOS ALVOS

Existe uma tendência em se imaginar que coisas ruins só acontecem com os outros. Isso ocorre tanto no campo pessoal quanto no campo profissional. Para a maioria das pessoas, que levam uma vida relativamente simples, a probabilidade de ser vítima de alguém mal-intencionado, é infinitamente inferior que a probabilidade de que ocorra com seu vizinho “bem de vida”.

O mesmo acontece dentro das instituições. Empresas pequenas, por exemplo, que movimentam poucos valores financeiros e que possuem poucos ativos, tendem a imaginar que, entre eles e o banco da esquina, bandidos estariam obviamente de olho no banco.

Mas, este tipo pensamento não é privilégio apenas dos “pequenos”. Instituições consideradas de maior porte, com maior visibilidade, também sofrem com o paradigma da falsa percepção de segurança. Trata-se de uma sensação disseminada e dominante.

O grande equívoco deste tipo de pensamento é que nem sempre o alvo destes golpistas é pré-determinado. Outro ponto importante, é que nem sempre as motivações que levam a prática de ataques são financeiras. Muitas vezes, busca-se apenas o desafio de se burlar determinado sistema ou de se conseguir determinada informação, para que assim o golpista consiga sua “notoriedade”.

As pessoas, justamente por acreditar que não estão na mira, terminam por perder a precaução no que diz respeito à segurança de suas informações pessoais no mundo digital.

Hoje, as redes sociais estão recheadas de informações confidenciais que, ainda que pareçam insignificantes vistas de maneira isolada, terminam por formar um vasto banco de dados, recheados de referências sigilosas. Para isso, basta um mínimo de esforço por parte do golpista, que precisará apenas pesquisar e capturar os dados já disponíveis e compilá-los de forma inteligente.

Em termos de segurança da informação no ambiente institucional, notas coladas nos monitores com senhas escritas, números de telefones particulares expostos ou organogramas deixados sobre as mesas são um grande chamariz. Se houver alguém buscando a oportunidade para a “invasão”, lhes é entregue as ferramentas necessárias para a execução.

É aqui que entra em ação o engenheiro social. Diz Mitnick (2003, p. 7):

A maioria das pessoas supõe que não será enganada, com base na crença de que a probabilidade de ser enganada é muito baixa; o atacante, entendendo isso como uma crença comum, faz a sua solicitação soar tão razoável que não levanta suspeita enquanto explora a confiança da vítima.

O engenheiro social sabe que, mesmo no maior sistema de segurança que se possa imaginar, existe um componente frágil, que pode ser “quebrado” com muita facilidade: o ser humano. Para Mitnick (2003) a ingenuidade e a fragilidade das pessoas são as principais armas utilizadas pelo engenheiro social.

Para a maioria das empresas, é somente quando vulnerabilidades aleatórias se encontram com as ameaças, dando origem aos incidentes, que a segurança da informação passa a ser vista como ferramenta de proteção indispensável, conforme ratifica Scudere (2007, p. 78):

A experiência me permite dizer que mais de 90% das empresas envolvidas em eventos associados a fraudes apenas procuram por uma análise técnica especializada após a ocorrência de ao menos um incidente relevante de impacto ou quando ao menos um dos vários sintomas possíveis atinge o limite interno das explicações aceitáveis.

Ainda, sobre a displicência de gestores que acreditam estar fora do campo de alcance de prejuízos provocados pela ausência de políticas de segurança da informação Scudere (2007, p. 80) continua:

Muitas vezes, infelizmente, a área tecnológica tenta explicar a você – gestor de negócios – que um ou diversos incidentes graves podem acontecer a qualquer momento e você ouve, sim, atentamente, mas no final da reunião... `Bem, como está o valor de nossas ações hoje?

O que acontece é que, neste exato momento, sistemas desenvolvidos por hackers estão vasculhando a internet, de maneira ininterrupta, em busca de vulnerabilidades conhecidas ou não, em máquinas conectadas à Internet.

Se a empresa “A” apresentar características favoráveis à invasão, e por consequência tenha sua rede invadida, isto terá acontecido de maneira aleatória. O ataque em momento algum foi disparado contra a empresa “A”, o que quer dizer que aquele nunca foi um alvo escolhido de maneira intencional.

É comum que ataques sejam deflagrados pela simples razão de que se é possível realizá-los. Schopenhauer tem uma frase famosa, que se encaixa perfeitamente com o perfil do praticante deste tipo de ataque: "Ter talento é acertar num alvo que ninguém acertou. Ser gênio é acertar num alvo que ninguém viu".

Sobre esta imprevisibilidade, Scudere (2007, p. 81) diz:

Para que possa entender melhor, entre final de 2001 e início de 2003, iniciou-se um fenômeno que vem apenas acentuando-se com relação à origem dos incidentes de segurança e fraudes tecnológicas. Até aquela data, as estatísticas apontavam para algo em torno de 70% das incidências de origem externa. O que isso quer dizer? Você podia aparecer nessa estatística, mas não quer dizer necessariamente que alguém tinha a sua empresa em particular como alvo.

Assim, o engenheiro social, quando não tem um alvo específico, faz uma varredura de maneira indireta, encontrando aleatoriamente vulnerabilidades que possam ser exploradas, sejam em máquinas ou em pessoas.

Indiscutivelmente muitas das falhas são encontradas em máquinas por razões técnicas, como equipamentos de proteção mal configurados ou mal instalados. Mas, a falta de conscientização e compromisso por parte das pessoas, em ambiente de trabalho ou doméstico, deixa as portas escancaradas às ameaças.

Scudere (2007, p. 44) cita alguns dados preocupantes. O autor apresenta os seguintes números, de acordo com a Associação Americana de Administração, conforme o Quadro 2.

Quadro 2 – Dados da associação americana de administração

75% dos empregadores dos Estados Unidos sentem a necessidade de monitorar o uso da internet por parte dos seus funcionários;
--

26% das empresas pesquisadas já fizeram ao menos uma demissão por justa causa por consequência de navegação indevida ou inadequada;

Entre 50% e 75% dos empregados declararam usar a internet para fins pessoais durante o horário de trabalho.

Fonte: Adaptado de Scudere (2007, p. 44).

Este uso pessoal durante o horário de trabalho, significa basicamente, visitas a perfis de redes sociais, visitas à sites de origem e conteúdos duvidosos e o uso do e-mail particular. Em todos estes destinos, criminosos estão à espreita, somente esperando que a isca lançada seja mordida. Isto significa aumentar a probabilidade de encontro com a aleatoriedade. Estas pessoas, em seus ambientes de trabalho, não deveriam estar navegando livremente na internet.

Este é um comportamento que representa a antítese daquilo que se quer, que é maximizar as condições de segurança e, conseqüentemente, minimizar os riscos do comprometimento ou divulgação indevida dos ativos de informação das empresas. Diz Scudere (2007, p. 8):

Porém, você, como um gestor atuante no mundo digital, não pode se esquecer da implacável efetividade do inesperado, que o atinge de frente e o surpreende, materializando uma incerteza desprezada num incidente em geral de altíssimo impacto, no qual sua exposição a riscos poderá estar igualmente próxima a níveis máximos. Assim, é fato concreto entre os especialistas em riscos que as técnicas de ataques e violação de sistemas tornam-se cada vez mais sofisticadas e inteligentes, buscando explorar exatamente aquelas áreas que você desprezou em seus estudos de proteção ou por apenas considera-las de alguma forma improváveis do ponto de vista técnico ou até mesmo demasiadamente simples ou mesmo óbvias e que jamais teriam sucesso, caso fossem tentadas.

Portanto, o mundo digital requer cuidados redobrados, evitando assim a perda de informações da empresa ou mesmo de dados pessoais.

3 METODOLOGIA

Este estudo faz uso da pesquisa exploratória, pois visa dar maior proximidade com o problema em questão, segurança na internet. Bem como, seu planejamento é flexível, interligando experiências práticas com o problema da pesquisa, Gil (2010).

O instrumento de coleta de dados deste artigo foi a internet, com utilização da rede social *Facebook* e, de acordo com Figueiredo *et al.* (2012), esta forma de coleta de dados classifica-se como outros.

O delineamento da pesquisa, de acordo com a técnica utilizada, classifica-se como de levantamento ou *survey*, segundo Figueiredo *et al.* (2012). Busca informações sobre perfil e comportamento dos indivíduos, gerando generalidades sobre o universo pesquisado.

4 APRESENTAÇÃO E ANÁLISE DOS DADOS

4.1 VÍTIMAS ALEATÓRIAS

Com o objetivo de ilustrar como a vítima de um ataque de engenharia social pode ser escolhida ao acaso, seguem quatro exemplos de situações que ocorrem no cotidiano de pessoas e empresas.

O primeiro deles, “O Ataque Russo”, conta a história de um grupo de hackers russos, autores do maior roubo de dados da história. Os exemplos dois e três foram colhidos dentro da plataforma do *Facebook*, e demonstram de forma clara a ingenuidade e facilidade com que pessoas, escolhidas aleatoriamente, escancaram publicamente suas informações privadas.

O quarto e último exemplo, foi extraído de um vídeo publicado na internet pela Febelfin, acrônimo do francês *Fédération belge du secteur financier*, ou, em português, Federação Belga do Setor Financeiro, que fez parte de uma campanha institucional que tinha por objetivo alertar as pessoas para a exposição de seus dados na Internet.

4.2 O ATAQUE RUSSO

Reconhecido como o maior roubo de dados da história, uma gangue russa de hackers, conhecida como CyberVor, atacaram aleatoriamente 420 mil websites e conseguiram coletar 1,2 bilhões de logins e senhas. Nesse mesmo ataque, conseguiram ainda 540 milhões de endereços de e-mail.

As vítimas, que em momento algum expuseram de maneira irresponsável seus dados pessoais, e que agora estavam servindo aos golpistas um vasto banco de dados, com informações pessoais e/ou empresariais, também foi escolhido de maneira totalmente aleatória.

A técnica utilizada pelos russos é chamada de SQL Injection, e tem como propósito forçar comandos dentro do ambiente dos sites com o objetivo de que retornem o conteúdo do banco de dados.

Neste ataque, os hackers buscavam, de maneira genérica, websites que fizessem login. Qualquer um dos 420 mil atacados, o foram por uma fatalidade. Já os usuários destes sites, vítimas reais, uma má sorte sem tamanho.

4.3 COMO LANÇAR UMA ISCA

No dia 12 de março de 2015, uma usuária do Facebook, que por razões de privacidade será chamada de J.N. (iniciais do nome), publicou em um grupo chamado “Bom Negócio Chapecó”, a seguinte mensagem: “Estou add pessoas para participar de um grupo de bate papo no whats para pessoas de Chapecó e região interagir, fazer amizades jogar conversa fora, interesse deixe o seu whats no comentário que add”.

O termo “Add”, no universo das redes sociais, significa “Adicionar”, ou seja, incluir na lista de amigos. Já a palavra “whats”, faz referência a um aplicativo de troca instantânea de mensagens, desenvolvido para dispositivos móveis, chamado “WhatsApp”.

Na figura 2, editada de modo a não aparecer nomes e telefones, é possível verificar que, em um intervalo de nove horas, 49 pessoas responderam a postagem de J.N., informando seus números pessoais de telefones celulares.

Figura 2 – No Facebook – 49 números de telefones em menos de dez horas



Fonte: Dados da pesquisa.

O primeiro a responder o anúncio foi W.C. (iniciais do nome). Além do seu telefone exibido na resposta do anúncio, em rápida visita à sua página pessoal, com apenas um click no mouse é possível traçar o seguinte perfil de W.C., conforme a Quadro 3.

Quadro 3 – Perfil do usuário W.C.

Morador da cidade de Chapecó, município do estado de Santa Catarina.
Trabalha em um grande frigorífico da região (omitido neste trabalho por razões de privacidade).
Estudou na IFSC – Instituto Federal de Santa Catarina.
É pai de uma Menina com menos de 1 ano de idade.
Casado com M.D.C. (iniciais do nome).
Gosta de motos.

Gosta de corridas automobilísticas.
Torcedor do Grêmio.
Torcedor da Chapecoense.
Curtiu a página “Bíblia Online de Estudo”, o que leva a concluir ser uma pessoa religiosa.
Gosta de realizar negócios (participa de 10 grupos locais de classificados).
Tem apenas 1 filha.

Fonte: Dados da pesquisa.

Além do perfil W.C., pode-se acessar facilmente o perfil da sua esposa, conforme demonstrado no Quadro 4 o perfil da esposa de W.C., construído a partir de sua resposta ao chamado no facebook.

Quadro 4 – Perfil da esposa de W. C.

Auxiliar de Inspeção no mesmo frigorífico que o marido
Formada em Nutrição pela UNOCHAPECÓ – Turma de 2012.
Natural da cidade de Sul Brasil, município do estado de Santa Catarina.
Estudou na “Escola de Educação Básica Hélio Wasum”.
Possui 2 irmãs: M.D.C. e M.A.C. (iniciais do nome).
Torcedora do Grêmio.
Torcedora da Chapecoense
Gosta de música gauchesca.
Um alto número de fotos da sua filha postadas em seu mural.
Tem apenas 1 filha.

Fonte: Dados da pesquisa.

A quarta pessoa a responder ao anúncio foi de P.P. (iniciais do nome). Além do seu telefone exibido na resposta do anúncio, assim como, no exemplo anterior, um click no mouse foi possível traçar o seguinte perfil, conforme mostra o Quadro 5.

Quadro 5 – Perfil do usuário P.P.

Natural do Rio de Janeiro.
Atualmente reside em Balneário Camboriú, município do estado de Santa Catarina.
Tem fluência em espanhol.

Casou em 2013, mas o casamento durou menos de um ano.
Solteira.
Torcedora do Flamengo.
Gosta de música sertaneja.
Prefere assistir à comédia.
Gosta de seriados de televisão com conteúdo adolescente.
Gosta de ler.
Participa de vários grupos de namoro no facebook.
Demonstra carência em mensagens postadas em seu perfil, como: "se sentindo sozinha", "se sentindo triste" e "quem quiser entra no meu grupo de namoro do whats só deixar o número" (em resposta a essa última postagem sobre o grupo de namoro, 23 pessoas responderam, com seus respectivos números de telefone)."

Fonte: Dados da pesquisa.

4.4 ATESTADO DE INGENUIDADE

Em outra publicação, capturada no mesmo dia do exemplo anterior, desta vez publicada em um grupo do *Facebook* chamado “Negócio Fechado – Chapecó”, a usuária M.R.S.R. (iniciais do nome), não só expõe suas informações pessoais em seu perfil, como também comunica publicamente que possui R\$ 5.000,00 guardados para compra de um veículo.

Figura 3 – Usuária de *Facebook*, M.R.S.R



Fonte: Dados da pesquisa.

Assim como no exemplo anterior, traçar um perfil da usuária M.R.S.R. foi simples e rápido, conforme o Quadro 6.

Quadro 6 – Perfil da usuária M.R.S.R.

Endereço de e-mail disponível publicamente.
Idade disponível publicamente.
A usuária prestou concurso público em 2011.
Recentemente fez doação em dinheiro para campanha circulada na internet.
Natural da cidade de Luzerna, município do estado de Santa Catarina.
Casada.
Tem uma filha.
Gosta de música sertaneja.
Torcedora da Chapecoense.
Religiosa.

Fonte: Dados da pesquisa.

Já, em relação ao perfil do marido de M.R.S.R. a partir de sua resposta ao chamado no facebook, descrito no Quadro 7.

Quadro 7 – Perfil do marido de M.R.S.R

Chama-se C.R. (iniciais do nome).
Local de trabalho disponível (omitido neste trabalho por razões de privacidade)
Estudou na escola “Druziana Sartori”.
Natural de Carazinho, município do estado do Rio Grande do Sul.
Torcedor do Grêmio.
Torcedor da Chapecoense.
Interesses em tatuagem.
Religioso.
Gosta de animais, em especial de cachorros.
Gosta de carros.

Fonte: Dados da pesquisa.

Nos exemplos 4.1 a 4.4, as informações foram colhidas em alguns segundos, visitando seus perfis no *Facebook*, a partir da própria publicação original. Para uma pessoa má intencionada, em posse destas informações pessoais, descobrir o local de residência, numeração dos documentos, referência bancária, entre tantas outras possibilidades, poderá ser feita sem muitas dificuldades, principalmente se o pesquisador for uma pessoa treinada, que sabe onde buscar tais informações.

4.5 O CASO DO VIDENTE BRUXELENSE

No dia 12 de setembro de 2012, na cidade de Bruxelas, Bélgica, a Federação Belga do Setor Financeiro (FEBELFIN), gravou um vídeo que mostrava de maneira surpreendente, a facilidade com que se é possível ter acesso a informações pessoais de qualquer pessoa se utilizando apenas da Internet, conforme demonstra a Figura 4.

Figura 4 – “Vidente” finge esforço para acessar a mente de convidado.



Fonte: Dados da pesquisa.

Protagonizado por Dave, um “talentoso vidente”, pessoas que passavam na rua eram convidadas aleatoriamente para participar de um programa de televisão, filmado dentro de uma tenda, onde Dave “leria” seus pensamentos.

Após sentarem-se um em frente ao outro, Dave começa a “ler” detalhes da vida de cada um dos convidados. Ele comenta sobre seus históricos médicos, cita nome de melhores amigos, fala da vida amorosa (o que gera evidente preocupação em uma das participantes), descreve uma tatuagem, saldos bancários e chega até a ditar, dígito por dígito, a sequência do número do cartão de crédito de uma das pessoas, conforme mostra a Figura 5.

Figura 5 – “Poucas pessoas sabem disso”, revela participante, sobre vida amorosa



Fonte: Dados da pesquisa.

Quando os convidados já não duvidavam das incríveis habilidades de Dave, uma cortina cai e revela um grupo de hackers, todos encapuzados, conectados a fontes públicas de informações, como *Facebook* e *Twitter*. Para o grupo de hackers foi informado apenas o nome completo e o endereço das vítimas, para que pudessem dar início as buscas.

Por fim, os participantes viram um verdadeiro dossiê de suas vidas exposto em uma grande tela, com suas fotos em evidência. Todas as informações eram passadas a Dave por um fone de ouvido.

5 CONSIDERAÇÕES FINAIS

Fica evidente que nenhuma empresa ou pessoa está livre de cair em ataques provocados por *hackers* ou pelo Engenheiro Social. A aleatoriedade estende a todos os riscos de serem vítimas destes golpistas, amargando com isso graves prejuízos financeiros e, em casos mais extremos, sofrendo até lesões físicas.

Especialista na manipulação das vulnerabilidades humanas, o Engenheiro Social exerce domínio sobre suas vítimas trabalhando fatores como a curiosidade, culpa, confiança, simpatia e medo.

É preciso conscientização de que a Engenharia Social está no dia-a-dia de todos. Basta um deslize, ou um rápido momento de desatenção, para que a vítima fique vulnerável. Outro ponto importante é a necessidade da implantação, e controle da execução, de Políticas de Segurança Interna. Afinal, é o próprio quadro de recursos humanos das empresas, que se presumem serem de inteira confiança, o elo mais fraco de todo o sistema de segurança. É ele quem cede, de maneira involuntária ou não, informações críticas ao Engenheiro Social.

O desenvolvimento de um sistema de segurança 100% confiável e impenetrável ainda não é uma realidade. Mas, se medidas de prevenção forem incorporadas nas mentes das pessoas e nos procedimentos, o risco de sofrer prejuízos por conta do roubo de informações sigilosas, cairá de maneira significativa.

Assim, é preciso estar preparado, pois, neste exato momento, alguém pode estar de olho em nossos movimentos, planejando um ataque que poderá nos trazer sérios prejuízos. A única vacina realmente eficaz contra essas investidas é a prevenção por meio de treinamentos periódicos e intensivos.

REFERÊNCIAS

DANTAS, M. L. **Segurança da informação: uma abordagem focada em gestão de riscos**. Olinda: Livro Rápido, 2011.

FIGUEIREDO, A.N.B. et al. **Pesquisa científica e trabalhos acadêmicos**. Chapecó: Arcus, 2012.

FONTES, E. **Políticas e normas para a segurança da informação**. Rio de Janeiro: Brasport, 2012.

GIL, A. C. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 1999.

GIL, A.C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2010.

MANOEL, S. S. **Governança de segurança da informação: como criar oportunidades para o seu negócio**. Rio de Janeiro: Brasport, 2014.

MARCELO, A. **Engenharia social: A arte de hackear pessoas**. Rio de Janeiro: Brasport, 2005.

MITNICK, K. Minas Gerais: **Revista Fonte**. Entrevista concedida a Naira Faria e Paulo César Lopes, 2007.

MITNICK, K.; SIMON, L. **A Arte de Enganar**. São Paulo: Pearson Education do Brasil Ltda, 2003.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

PEIXOTO, M. C. P. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, 2006.

SCUDERE, L. **Risco Digital**. Rio de Janeiro: Elsevier, 2007.

SÊMOLA, M. **Gestão da Segurança da Informação: Uma visão executiva**. Rio de Janeiro: Elsevier Editora Ltda, 2003.