FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Renan Domingues dos Santos

Prazer, Engenheiro Social.
Posso te ajudar?

Americana, SP
2018

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Superior de Tecnologia em Segurança da Informação

Renan Domingues dos Santos

Prazer, Engenheiro Social.
Posso te ajudar?

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. Benedito Luciano Antunes de França

Área de concentração: Fator Humano em Segurança da Informação.

Americana, SP.
2018

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

S238p SANTOS, Renan Domingues dos

Prazer, engenheiro social. Posso te ajudar?. / Renan Domingues dos Santos. – Americana, 2018.

50f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Benedito Luciano Antunes de França

1 Segurança em sistemas de informação 2. Engenharia social I. FRANÇA, Benedito Luciano Antunes de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU:681.518.5

Renan Domingues dos Santos

Prazer, Engenheiro Social. Posso te ajudar?

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação, pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Fator Humano em Segurança da Informação

Americana, 29 de junho de 2018.

Banca Examinadora:

Benedito Luciano Antunes de França (Presidente)
Mestre
Fatec Americana

Henri Alves de Godoy (Membro)
Mestre
Fatec Americana

Daniele Junqueira Frosoni (Membro)
Mestre
Fatec Americana

Se não puder voar, corra.

Se não puder correr, ande.

Se não puder andar, rasteje,

Mas continue em frente de qualquer jeito.

Martin Luther King.

AGRADECIMENTOS

Quero agradecer a Deus por me capacitar, por me fortalecer e manter-me no caminho do certo, buscando sempre meu crescimento profissional e a evolução como ser humano, sendo leal e acima de tudo com muito amor e respeito ao próximo.

Um agradecimento especial para minha Mãe e meu Pai, que me deram uma base de criação sensacional e significativa para que eu chegasse onde eu estou hoje, por cuidarem de mim com muito carinho e amor e por me ensinarem o que é respeito. Minha irmã por ser minha grande inspiração nessa jornada toda e meu presente de Deus.

Todo o quadro de funcionários da FATEC Americana, por oferecer o conhecimento da melhor maneira possível, obrigado pelo trabalho senhores e senhoras profissionais da limpeza, segurança e alimentação (todos os funcionários terceirizados), todo o setor administrativo da faculdade e principalmente os professores e mestres.

A todo o corpo de funcionário da Faculdade de Engenharia Elétrica e de Computação da UNICAMP, em especial ao grupo da Diretoria Técnica de Informação.

Um abraço especial pros meus irmãos que cresceram comigo e os novos que ganhei em Campinas na inesquecível jornada que foi o meu estágio.

Deus abençoe todos nós!

Muito Obrigado.

DEDICATÓRIA

Quero dedicar esse Trabalho ao Sport Club Corinthians Paulista:

O campeão dos campeões
Eternamente dentro dos nossos corações
Salve o Corinthians de tradições e glórias mil
Tu és orgulho
Dos desportistas do Brasil
Teu passado é uma bandeira
Teu presente é uma lição
Figuras entre os primeiros
Do nosso esporte bretão
Corinthians grande
Sempre altaneiro
És do Brasil
O clube mais brasileiro
Salve o Corinthians

Benedito Lauro D'Ávila

RESUMO

Este trabalho de conclusão de curso busca traçar o perfil comportamental dos criminosos virtuais, trazendo características e técnicas sobre o tema Engenharia Social, entre outras artimanhas que estes piratas, como são conhecidos, utilizam para ludibriar suas vítimas e praticar atos ilícitos contra elas. O ideal seria educarmos todos os usuários da Internet, pois quanto mais as pessoas perceberem os riscos que elas ou até os seus familiares estão correndo, tomariam mais cuidados com a divulgação de informações pessoais na Web. A solução proposta é desenvolver, com o apoio do governo federal e das universidades brasileiras, formas efetivas para educarmos tecnologicamente o máximo de público possível, não se limitando apenas aos operadores da área da tecnologia da informação.

ABSTRACT

This undergraduate thesis seeks to trace the behavioral profile of virtual criminals, bringing features and techniques on the theme of Social Engineering, among other tricks that these pirates, as they are known, use to deceive their victims and to commit illegal acts against them. The ideal would be to educate all Internet users, as the more people realize the risks they or their family are running, the more they would take care of the disclosure of personal information on the Web. The proposed solution is to develop, with the support of federal government and Brazilian universities, effective ways to educate the public as much as possible, not just the information technology operators.

SUMÁRIO

LISTA DE GRÁFICOS

INTRODUÇÃO

Todo o conhecimento humano começou com intuições, passou daí aos conceitos e terminou com ideias
(Immanuel Kant)

O objetivo desse Trabalho de Graduação visa realizar uma pesquisa, de caráter teórico-conceitual, relacionando os temas Engenharia Social e Crimes Virtuais; ao longo do estudo, primeiro, vamos fazer uma abordagem sistemática do assunto Engenharia Social, citando alguns exemplos de técnicas e métodos que têm o objetivo de manipular, ludibriar, enganar vítimas virtuais, por meio do qual o atacante/criminoso busca conquistar a confiança da vítima e cometer alguns crimes.

Mostraremos o prejuízo que pode ser imputado a pessoas como também para grandes empresas, por meio de um simples telefonema no intuito de captar informações destas vítimas; utilizaremos o especialista em informática Kevin Mitnick como exemplo de engenheiro social; em seguida, vamos abordar que, não somente os criminosos utilizam desse recurso, mas também corporações que tratam sobre o tema, e que as intervenções ou interceptações não são usadas necessariamente para fins ilícitos. Apresentaremos, por exemplo, uma entrevista realizada por este autor com uma vítima de um tipo de golpe telefônico, muito conhecido no Brasil, buscando exemplificar as técnicas de engenharia social.

Em seguida, direcionamos a reflexão sobre o conhecimento do novo profissional de Segurança da Informação, o denominado profissional forense computacional. Ilustramos os detalhes desta nova função, as ferramentas usadas para suporte e treinamento e, por fim, analisaremos a necessidade imposta pela tecnologia atual, uma vez que, tudo está ancorado no ambiente *online*, como consequência a segurança torna-se um fator diretamente relacionado com o profissional de Segurança da Informação.

A pesquisa de campo efetuada, com a aplicação de uma enquete, intenciona descobrir o nível de preocupação das pessoas que estão conectadas; esta foi realizada por meio da ferramenta Google.Form. Através desta, mapeamos a respeito das informações pessoais, as quais são digitadas em lugares que oferecem gratuitamente a Internet, a fim de verificar se os usuários têm consciência dos riscos destes acessos, tanto em *lan-house* bem como nas empresas ou nos ambientes privados. Conforme veremos, em um ambiente corporativo essa falta de cuidado na socialização de algumas informações de cunho pessoal e de cunho privativo acaba sendo um dos fatores para a ocorrência de crimes virtuais.

A justificativa teórico-conceitual deste Trabalho de Graduação se assenta na necessidade das instituições de ensino superior de preparar e desenvolver, por competências e habilidades, um profissional de Segurança da Informação focado em Engenharia Social, a fim de auxiliar os usuários em um meio corporativo, assim como nos espaços dedicados ao lazer, como entretenimento virtual, a prevenir possíveis ações virtuais.

CAPÍTULO 1 – CONHECENDO A ENGENHARIA SOCIAL

A falta do saber e a falta de informações são os princípios da manipulação (Diôgo Pantoja)

Segundo Mário César Pintaudi, professor especialista em Segurança da Informação, autor do livro "Engenharia Social e Segurança da Informação na Gestão Corporativa", o primeiro relato registrado em que o homem foi feito de vítima por meio da utilização de um comportamento relacionado à Engenharia Social é narrado na Bíblia, de modo particular no livro de Gênesis (Cap. 3, vers. 1-6):

> 1ª – Ora, a serpente era mais astuta que todas as alimárias do campo que o Senhor Deus tinha feito. E esta disse à mulher: É assim que Deus disse: Não comereis de toda a árvore do jardim?
> 2ª – E disse a mulher à serpente: Do fruto das árvores do jardim comeremos,
> 3ª – Mas do fruto da árvore que está no meio do jardim, disse Deus: Não comereis dele, nem nele tocareis para que não morrais.
> 4ª – Então a serpente disse à mulher: Certamente não morrereis.
> 5ª – Porque Deus sabe que no dia em que dele comerdes se abrirão os vossos olhos, e sereis como Deus, sabendo o bem e o mal.
> 6ª – E viu a mulher que aquela árvore era boa para se comer, agradável aos olhos, e árvore desejável para dar entendimento; tomou do seu fruto, e comeu, e deu também a seu marido, e ele comeu com ela (BÍBLIA SAGRADA, Gên. 3:1-6).

Analisando o comportamento da serpente, sua principal característica era ser conhecida como a personagem mais "astuta" e que, pela definição da palavra, indica ser um indivíduo que age com esperteza e não se deixa enganar, tem como objetivo ludibriar outros indivíduos para obter vantagens ou benefícios (FERREIRA, 2010, p. 96). Na narrativa bíblica, Eva foi a vítima, pois foi iludida a comer do fruto da árvore, o qual foi proibido por Deus, mas, desrespeitando a vontade divina, assim o fez, coroando a serpente, de acordo com Pintaudi (2006), como a primeira atacante especializada em Engenharia Social.

Por outro lado, o psicólogo americano Dr. William Moulton Matston desenvolve no livro "As emoções das pessoas normais", uma relação entre as emoções do ser humano com o seu comportamento, possibilitando fazer uma leitura das ações corporais, assim, suas teorias serviram de base para que os pesquisadores elaborassem ferramentas de análise de perfil comportamental. O interessante é que ele diz nesta obra que para enganar uma pessoa "você deve primeiramente obter sua confiança" (MATSTON, 2014, p. 230); nesta obra, ele também detalha três métodos de como conquistar a confiança de um indivíduo. Resumidamente o primeiro método é o consciente e consiste em criar uma situação por meio da qual o atacante cria um problema para a vítima e ele se mantém como o responsável pela solução. O método

de oportunidade é o segundo, no qual o atacante enxerga uma vulnerabilidade e faz seu ataque. São ações que têm pouco tempo de planejamento e conta, muitas vezes, com um pouco de sorte. O último método é o mais complexo, chama-se "método de capacidade", que leva tempo de estudo e de planejamento, além disso, exige uma boa preparação antes de começar a agir, pois como Matston disse "se você perder o controle da situação utilizando-se desse método é bem provável que falhará em conquistar a confiança da vítima caso ela venha a desconfiar de algo errado" (MATSTON, 2014, p. 233).

Em 2003, no evento denominado "InformationWeek Brasil", realizado em São Paulo, a empresa Konsultex Informática concebeu o termo Engenharia Social da seguinte forma:

> Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de Hipnose ou Controle da Mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informações) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos (KONSULTEX, 1993).

2018 anos depois de Cristo a tecnologia atingiu um nível tão grande de especialização que o ser humano está cada vez mais utilizando as novas inovações para facilitar seus problemas do cotidiano ou por entretenimento e lazer. Nessa direção, Reynaldo Ng, consultor de análise forense e autor do livro "Forense Computacional Corporativa", cita três fatos importantes para se compreender este nível atingido pelas novas tecnologias. Primeiro fato é que o mundo atual é extremamente tecnológico, segundo, que o dinheiro é cada vez mais eletrônico (Cartões, SmartCard) e, por último, o mundo se torna cada vez mais *online*, mais integrado (NG, 2007, p. 2-3).

Outro fator importante, especificado por Ng, é que os criminosos evoluíram juntamente com as tecnologias e ganharam aliados extremamente difíceis de serem controlados. Primeiro que a Internet é um mundo por meio do qual qualquer indivíduo pode se esconder facilmente; ademais, ela gera novas facilidades tecnológicas a cada dia, como também, propicia aos usuários, sem certo grau de conhecimento tecnológico, dificuldades na utilização das mesmas. Além disso, há uma grande falta de cuidado por parte dos usuários com essas novas tecnologias, que, quando entram nesse mundo *online*, acabam se tornando vítimas vulneráveis, e, por último, como considera Ng, há uma "falta de mecanismos

adequados de segurança na grande maioria dos sistemas que são desenvolvidos" (NG, 2007, p. 2-3).

Ainda segundo Ng, o surgimento de um novo campo de atuação, a qual ele chamou de "Forense Computacional", deve possuir uma série de

> [...] conhecimentos técnicos e processuais, que envolvem redes de computadores e seus protocolos, configurações de dispositivos, hardware, software, linguagens de programação, ferramentas forenses e metodologia de análise (NG, 2007, p. 3).

Este Trabalho de Graduação pretende mostrar dois pontos principais: primeiro dissertar sobre a facilidade de se conseguir manipular alguém para praticar um crime virtual e, segundo, relatar a necessidade do investimento educacional para os profissionais de Segurança da Informação, a fim de protocolar uma medida de segurança que seja capaz de capacitar todos os usuários no ambiente corporativo e no manejo da Rede Mundial de Computadores para uso social.

Antes de especificarmos o perfil do profissional de Segurança da Informação, conheceremos as novas serpentes do século XX, que conseguiram invadir sistemas sofisticados e furtar documentos ultrassecretos, utilizando de técnicas de Engenharia Social para ludibriar não só o sistema, mas também os usuários.

1.1 – Serpentes do século XX: O caso Kevin Mitnick

O melhor sistema para invadir é a mente humana (Reynaldo Ng)

Estados Unidos da América, dezembro de 1988, de acordo com as informações retiradas do livro "O Jogo do Fugitivo" escrito pelo jornalista americano Jonathan Littman, Kevin Mitnick fez seu primeiro ataque aos 17 anos e trouxe um prejuízo de 200 mil dólares a empresa de serviços de telefonia da Califórnia a "Pacific Bell (Atualmente AT & T Inc.)

> Mitnick tinha 17 anos quando pela primeira vez entrou no sistema de computadores da Pacific Bell, segundo um artigo de dezembro de 1988 do Los Angeles Times, alterando contas de telefone, penetrando em outros computadores e furtando dados no valor de 200 mil dólares de uma companhia de San Francisco (LITTMAN, 1996, p. 24-25).

Nessa seção vamos conhecer o perfil de Kevin Mitnick e trazer algumas de suas técnicas que o fez ser mundialmente conhecido pela prática de crimes relacionados à invasão de sistemas e na obtenção de informações sigilosas por meio de ações ilegais, falsificações e fraudes.

A primeira prisão de Mitnick foi decretada em dezembro de 1988 e revogada seis meses depois como podemos observar:

> […] Dezembro de 1988, Mitnick foi preso sob a acusação de ter causado um prejuízo de quatro milhões de dólares à DEC – Digital Equipment Corp, e por furtar um sistema de computadores altamente secretos. Ganhou liberdade condicional após seis meses de prisão num estabelecimento destinado a jovens (LITTMAN, 1996, p. 25).

Jonathan Littman escreveu o seu livro fundamentado em entrevistas com o próprio Mitnick e com base nisso trouxe algumas técnicas de engenharia social que o mesmo detalhou. Mitnick, por exemplo, fazia ligações via telefone para os escritórios da *Pacific Bell*, fingindo ser empregado da companhia, como se fosse um técnico buscando informação funcional. Os piratas chamam isto de Engenharia Social, pois a chave é conhecer o jargão, ou seja, entender a infraestrutura da companhia e a natureza humana, visto que, de acordo com Mitnick, nos dizeres de Littman, raramente alguém verifica o número de fax, por exemplo.

Em seus planejamentos, Mitnick fazia seu trabalho de detetive e passava a imitar o comportamento do alvo. Outra informação valiosa é que, em dias como a véspera de natal, acabava sendo um dia perfeito para um ataque de Engenharia Social. As pessoas estão menos desconfiadas nos feriados, é mais provável que deixem escapar alguma coisa. Além do mais, a impressão do jornalista era que Mitnick parecia trabalhar como um policial.

Aos 17 anos, Mitnick não tinha a necessidade de ter dinheiro suficiente para comprar equipamentos sofisticados para completar seus ataques, pois, com apenas um telefone e uma boa conversa, era capaz de cometer variados tipos de crimes por diversão: "[…] É possível para uma pessoa com a capacidade de Mitnick cometer praticamente qualquer crime por computador. Pode se inclusive matar uma pessoa usando-se um computador" (LITTMAN, 1996, p. 25).

A opinião pública, a imprensa e os próprios órgãos do governo queriam soluções para aquelas novas práticas de crimes e essa necessidade deu a origem de um novo setor de investigação baseado em crimes envolvendo computadores, o setor denominado de Forense

Computacional. Como Littman cita em seu livro (1996, p. 26-27), as violações de Mitnick deram origem a novas leis para deter os crimes de computador.

Conforme observamos, o caso Kevin Mitnick é um exemplo significativo de como as técnicas de manipulação, de intervenção, interceptação, via fraudes telefônicas, acabaram auxiliando na criação da Engenharia Social, cujo objetivo central é fazer com que a vítima ofereça todas as informações necessárias para a intromissão em um sistema virtual.

O próximo capítulo trata sobre um caso real de um golpe telefônico que tem por si algumas características relacionadas às técnicas envolvendo a Engenharia Social, visto que revela a facilidade de como se pode enganar alguém.

1.2 – Serpentes do século XXI: o falso sequestro

Deve-se aprender sempre, até mesmo com um inimigo (Isaac Newton)

Essa seção aborda sobre um golpe estelionatário muito conhecido no Brasil, chamado de "Golpe do falso sequestro".

Neste Trabalho de Graduação entrevistamos uma vítima desse tipo de golpe. Esse ardil ocorreu no ano de 2013 e foi usado como ferramenta para os criminosos manipularem uma família. A vítima, um membro da família deste autor, será chamada de "Júlia", na época com 38 anos, casada, mãe de um casal de filhos, moradora no Rio de Janeiro; de acordo com o depoimento colhido por este autor, certa quarta-feira, por volta das 16h50min, a vítima recebeu um telefonema, o qual nos foi descrito da seguinte maneira:

> **Vítima**: Alô, boa tarde!
> **Criminosos**: Boa tarde é a senhora "Júlia"?
> **Vítima**: Quem é que está falando?
> **Criminosos**: Ai senhora "Júlia", aqui quem faz as perguntas sou eu, entendeu, e a senhora responde, certo? Aqui é um sequestro, entendeu; estamos aqui com seu filho, tá certo? Agora sem entrar em pânico vamos negociar o resgate, firmeza?

"Júlia" contou que, nessa hora, entrou em estado de choque porque a notícia é impactante e, mesmo que não seja verdadeira, até descobrir que se tratava de um falso sequestro, a informação recebida foi geradora de certo desconforto e se a vítima não se mantivesse calma, produziria certo caos, faria com que a vítima perdesse o raciocínio e o controle dos atos, agindo em conformidade aos desejos do atacante.

Esse criminoso, conforme vimos, utilizou-se do método consciente, pois, criou o problema e a solução para o mesmo, que, no caso, seria o depósito de certa quantia de dinheiro:

> **Criminosos**: Pegamos ele na saída do trabalho, minha senhora; agora fica tranquila que ele tá bem, já comeu alguma coisa aqui, *tá* deitado ali na cama assistindo TV normal, não vamos machucar ele se a senhora cooperar com a gente, entende, a senhora quer falar com ele? Fala com ele aqui.

A vítima conta que não conseguiu se concentrar ao ponto de identificar alguma diferença entre a voz ouvida e a voz do suposto filho dela, visto que os criminosos têm a audácia de imitar a voz do sequestrado a fim de ludibriar e mostrar que, de fato, está com o controle total da situação. A senhora "Júlia" não se recorda se os criminosos tinham sotaque carioca ou paulista, detalhe que seria de máxima importância para desmascarar toda a farsa, haja vista que há diferenças nas falas pronunciadas por paulista ou paulistano em relação ao sotaque carioca. Foi um período curto em que a vítima conversou com seu suposto filho, mas por um deslize cometido pelos criminosos, a senhora "Júlia" descobriu todo o golpe:

> **Criminosos**: Mãe, mãe quem tá falando sou eu, Renan; mãe, me ajuda! Deposita esse dinheiro para eles, mãe; se não eles vão me matar aqui. Mãe, eu não quero morrer!

Quando o atacante telefônico se passou pelo filho, no intuito de enganar a vítima, disse chamar "Renan"; a senhora "Júlia" observou que havia algo errado, pois seus filhos não tinham este nome; esse equívoco fez com que toda farsa e o choque inicial emocional se arrefecessem e ela passou a pensar na situação toda. A partir deste momento, segundo relatou para o autor destas linhas, ela passou a criar artifícios a fim de ganhar mais tempo com os criminosos, enquanto, de outro telefone móvel, ela estabelecia contato com a cunhada dela, no intuito de saber sobre o grau de segurança desta, visto que o nome chamado no suposto sequestro era o mesmo nome de um de seus sobrinhos; o mesmo tipo de contato ela fez, posteriormente, com seu filho, e constatou que também estava bem e seguro.

Sob o domínio da situação, a senhora "Júlia" ganhou as forças necessárias, reequilibrou-se emocionalmente, e desligou o telefone sem dar mais respostas aos criminosos. Conforme relatado, com a situação amenizada, ela refletiu depois que, por bem pouco, não se tornaria mais uma vítima do falso sequestro.

Com efeito, como os criminosos possuíam um nome fictício (Renan) e, a partir de agora, um nome real, o dela (“Júlia”), e que, de fato, a vítima tinha filho, todos os demais detalhes poderiam ser estudados pelos criminosos, o que obrigou, de certa maneira, a família a empreender vigília nas Redes Sociais, bem como adotar certas precauções no compartilhamento de informações pessoais no mundo *online*. Não obstante, conforme veremos em nosso estudo de caso, a partir de questionários previamente elaborados, esses elementos geram uma grande fonte de dados que, quando os atacantes engenheiros sociais exploram, podem obter sucesso nesta espécie de pesca eletrônica, haja vista que nem todas as vítimas tiveram a mesma sorte que a da senhora “Júlia”, conforme vemos todos os dias estampados em diversos telejornais, como o caso relatado na reportagem do “Jornal Nacional”, da Rede Globo de Televisão, exibido em 16 de Julho de 2015: “Golpe do falso sequestro aplicado por telefone ganha nova versão: Prejuízo de vítimas no centro-oeste de SP chegou a R$ 100 mil este ano” (PORTAL G1, 2015).

Sobre a preferência do conceito “pesca eletrônica” em vez do tradicional ataque “phishing”, justifica-se, pois, o segundo é um *malware*, gerado e propagado com a intenção de realizar uma espécie de ataque em escala, como se fosse um armadilha por meio da qual a vítima, ao usar um dispositivo eletrônico se tornaria uma presa fácil nas mãos do atacante virtual. Pesca eletrônica, em nossa visão, seria diferente, pois o atacante que já tem, consciente e deliberadamente, um alvo a ser atacado, e sua coleta de informações, separadas e analisadas, com grande pesquisa e espírito investigativo, estabelece critérios lógicos e técnicos definidos, a fim de provocar a invasão e o delito criminal. Sendo assim, o phishing usaria uma técnica aleatória, uma roleta russa, ao passo que a pesca eletrônica é clara, direta em relação a quais tipos de vítimas que o atacante escolhe captar e invadir (KARASINSKI, 2011).

Sendo assim, as Redes Sociais são lugares onde deveríamos tomar muito mais cuidado nas conexões realizadas; no Facebook, por exemplo, com base em informações pesquisadas, já conta com mais de 2 bilhões de usuários, e como sabemos, muitas pessoas geram muitas informações pessoais (PORTAL G1, 2017). Por exemplo, são informações sobre endereço pessoal, nomes de pessoas que residem no mesmo local, quem são os membros da família, localização do posto de trabalho, espaços lúdicos e de entretenimentos frequentados, entre outras dicas, dados que podem beneficiar um criminoso a desenvolver um enredo que, após a

pesca eletrônica, buscará conquistar a confiança da vítima, a ponto de ludibriá-la e fazê-la cair nas armadilhas do atacante.

O maior problema é quando as informações que o usuário produz ou reproduz são sigilosas, do âmbito de sua responsabilidade, e que afetam diretamente uma empresa, como nos sugere Ng: "[…] Todos os processos integrados às tecnologias que são tratados por pessoas, possuem suas falhas!" (NG, 2007, p. 6).

O alvo dos criminosos passou a ser justamente empresas que têm um capital maior como, por exemplo, a HBO que recentemente foi alvo de um crime virtual e teve cerca de

> 1,5 terabytes de dados roubados (...), com roteiros, episódios não lançados, relatórios financeiros, entre outros arquivos" gerando um grande prejuízo à emissora de televisão, forçando-a a tomar atitudes de um modo até desesperadas para tentar recuperar todo o trabalho perdido (PORTAL G1, 2017).

Pelo o que se sabe a HBO chegou a oferecer US$ 250 mil após furto de dados. Não obstante, a imprensa americana não confirmou a veracidade da mensagem, pois a fonte é um *e-mail* vazado pelos hackers que categorizam que o pagamento seria uma recompensa pela descoberta de vulnerabilidades no sistema (PORTAL G1, 2017).

Essas ações invasivas nos fazem refletir sobre o quanto não estamos preparados em relação à prevenção, bem como o quanto devemos adotar atitudes após a ocorrência de um crime dessa natureza; sem dúvida alguma, esse será o maior desafio para a ação profissional de Segurança da Informação, como abordaremos no capítulo a seguir.

CAPÍTULO 2 – O PROFISSIONAL DE SEGURANÇA DA INFORMAÇÃO

A verdade é que não existe uma tecnologia no mundo que evite o ataque de um Engenheiro Social
(Kevin Mitnick)

A Segurança da Informação conta com três principais conceitos básicos, a confidencialidade, a integridade e a disponibilidade. O livro de Pintaudi define confidencialidade como ato de "transmitir informações com a segurança de que elas cheguem sem que se dissipam para outros meios ou lugares onde não deveriam passar" (PINTAUDI, 2006, p. 38).

A integridade, segundo este mesmo autor, é a garantia de que as informações foram "recebidas pela pessoa correta, […] que as informações não tenham sofrido nenhum tipo de modificação ou alteração comprometendo sua real veracidade" (PINTAUDI, 2006, p. 38-39).

Por fim a disponibilidade, para a mesma fonte autoral, é um grande desafio, pois "de nada adiantaria termos a confidencialidade e a integridade se tais informações não estiverem disponíveis para serem acessadas" (PINTAUDI, 2006, p. 39). Manter esse sistema funcionando é uma das responsabilidades do profissional de Segurança da Informação.

Em 2007, Reynaldo Ng escreveu em seu livro "Forense Computacional Corporativa", a necessidade de investir em um novo setor na organização, visto que, para ele, ela deve "[…] possuir uma equipe que tenha os conhecimentos necessários para realizar processos de investigação forense, com o objetivo de identificar e minimizar estas falhas, diminuindo assim possíveis perdas para a organização" (NG, 2007, p. 6).

Uma pequena parcela de empresas que decidiram implementar esse setor com ajuda dos funcionários já ativos na organização tiveram uma boa iniciativa, porém muitos desses funcionários eram de outras áreas da informática, tais como Suporte, Administração de Banco de Dados, Processamento de Dados, e estas áreas não conseguem realizar a atividade forense da melhor forma, pois além de não terem o conhecimento especializado, costumam realizar atividades em paralelo às atividades do dia a dia: "[...] Essa prática forense necessita de profissionais de Segurança da Informação, Administração de Firewall e *Intrusion Detection System* (IDS) / *Intrusion Prevent System* (IPS)" (NG, 2007, p. 1).

Na organização empresarial, o setor de Segurança da Informação precisa estar alinhado com os outros setores para obter uma gestão empresarial satisfatória, pois é imprescindível que se leve em conta todos os ativos da empresa:

> […] Tudo que manipula direta ou indiretamente a informação, inclusive ela própria, ou seja; em termos de segurança das informações, um ativo pode ser um computador, uma impressora, um fichário na mesa da secretária, ou até mesmo o próprio usuário, não devendo ser confundido com o ativo patrimonial (PINTAUDI, 2006, p. 37).

Ao alinhar com os setores de nível executivo, nível tático e de nível operacional, o setor de segurança passa a receber as informações de toda a corporação e começa a trabalhar em conjunto com os responsáveis destes níveis, para que toda a organização atinja um padrão adequado. Embora existam muitos planos para o desenvolvimento de um programa de conscientização, criados exclusivamente pelo departamento de Tecnologia da Informação, não se pode esquecer que um padrão ideal envolve principalmente o ser humano, que é o fator de maior risco para a empresa; é extremamente necessário o auxílio do setor de Recursos Humanos para a criação de um programa de conscientização que, para Pintaudi (2006, p. 58), deverá ser criativo, dinâmico e convincente.

Pintaudi cita três fatores de risco por meio dos quais o engenheiro pode e deve explorar o seu ataque, sendo eles 1) o fator físico, 2) o fator tecnológico e 3) o fator humano; acerca deste último fator, ele define como algo "[…] que se deve dar uma atenção especial. Pois se cobrindo de cuidados perante ela, pode-se evitar que as outras duas venham a acontecer ou diminuir a probabilidade de ocorrência" (PINTAUDI, 2006, p. 52).

O profissional de Segurança da Informação precisa ficar atento aos fatores de risco de segurança e pensar somente no investimento desta na área tecnológica, com equipamentos de ponta, infraestrutura de primeiro mundo, *firewalls* e sistemas de segurança muito bem estruturados: Para Pintaudi não adiantaria, por exemplo, considerar a segurança em termos físicos e não considerá-la, também, em termos humanos (2006, p. 40). Para fins de ilustração, o autor deste Trabalho de Graduação considera o termo "físico" como todos os elementos relacionados ao meio ambiente, como computadores, ar-condicionado, isolamento acústico, vazão de incêndio, saídas de emergência, etc.

Uma boa prática forense requer um investimento inicial em profissionais especializados e infraestrutura, assim a tarefa mais complicada é justamente convencer o dono da empresa, sendo ela de pequeno, grande ou médio portes, a realizar esse tipo de investimento que, necessita de dinheiro e pode não trazer nenhum tipo de lucro para seu

produto; nos dizeres de Pintaudi "[…] é um investimento a ser aplicado e não simplesmente mais uma despesa a ser adicionada ao orçamento" (2006, p. 65).

Recentemente o Jornal "Estadão" publicou uma reportagem sobre o aumento de crimes virtuais no Brasil e como podem partir de qualquer lugar do planeta; de acordo com a matéria jornalística sob o título "Crimes virtuais afetam 42 milhões de brasileiros", publicada em 27 de janeiro de 2017, a questão a se discutir agora não é mais se vamos sofrer um ataque, a questão é se estamos prontos e seguros caso este venha a acontecer:

> O Brasil ocupa lugar de destaque no cenário global de cibercrimes. Em 2016, 42,4 milhões de brasileiros foram vítimas de crimes virtuais. Em comparação com 2015, houve um aumento de 10% no número de ataques digitais. Segundo dados da Norton, provedora global de soluções de segurança cibernética, o prejuízo total da prática para o país foi de US$ 10,3 bilhões (ESTADÃO, 2017).

2.1 – Gestão em segurança no ambiente corporativo

O preço da liberdade é a eterna vigilância (Thomas Jefferson)

Deve-se levar em consideração que, para uma boa Gestão em Segurança, é de extrema necessidade que todos os setores da empresa estejam alinhados em um padrão tático e que todos os funcionários colaborem com as políticas de segurança. "[…] O principal objetivo de uma política de segurança é informar aos usuários as suas obrigações para a proteção da tecnologia e do acesso à informação" (NG, 2007, p. 101).

Políticas de Segurança são regras que devem definir quais os padrões de gerenciamento de segurança serão implementados, bem como os processos de gerenciamento dos recursos de informação, e essas regras devem ser aplicadas também em caso de serviços prestados por empresas terceirizadas, criando procedimentos de segurança para receber esses prestadores: "[…] Um computador "Estranho" (no qual a organização não possui nenhum domínio sobre o que está instalado) pode realizar uma série de atividades suspeitas no ambiente corporativo" (NG, 2007, p. 105).

Um exemplo de procedimentos de segurança nesse caso seria implementar um sistema de controle a partir de cadastro de Endereços *MAC Address* dos equipamentos. Apenas os equipamentos que tenham sido cadastrados podem ter acesso ao ambiente de rede; um controle neste nível fará com que todo novo equipamento, antes de ter acesso à rede de dados da organização, seja identificado, avaliado e documentado, o que aumenta "[...] o nível de

controle, além de auxiliar um processo de investigação sobre equipamentos de terceiros no ambiente corporativo" (NG, 2007, p. 105).

O *Intrusion Detection System* (IDS) e o *Intrusion Prevent System* (IPS) são ferramentas que trabalham no segmento de rede com foco no monitoramento do tráfego de dados para "[…] detectar e informar sobre atividades suspeitas como ataques e tentativas de acesso indevido" (NG, 2007, p. 107-108). O IDS, neste caso, não consegue tomar uma ação, apenas serve como sistema para detecção de ameaças, enquanto o IPS trabalha com uma grande base de informações sobre vulnerabilidades de sistemas, e suas assinaturas que, uma vez identificado o ataque, "pode ou não tomar ações preventivas" (NG, 2007, p. 107-108).

Tendo consciência de que qualquer informação, sendo ela confidencial ou não, é de extrema importância para a corporação, esta orientação de como cuidar das informações, para que todos os procedimentos de segurança sejam seguidos, não têm que ser apenas implantado para o profissional do setor de Tecnologia da Informação, deve se educar todos os funcionários e prestadores de serviço, visto que "[...] nunca é demais prevenir, educar e estar cada vez mais atento, pois aquelas informações que você acha que são inofensivas podem ser as chaves para os segredos mais valiosos que a empresa guarda" (PINTAUDI, 2006, p. 8).

A empresa de segurança Sysmatec, por exemplo, apresenta três ações que são relevantes para a orientação de seus funcionários:

> 1º – Estabeleça uma política de utilização da internet. Permita que os funcionários conheçam as regras da empresa a respeito do uso pessoal do e-mail e da internet;
> 2º – Determine a necessidade de cada funcionário de acessar informações delicadas e restrinja o acesso somente para o que for necessário a cada função na empresa;
> 3º – Educar os usuários nas táticas de engenharia social. Reforce que eles nunca devem informar suas senhas (PINTAUDI, 2006, p. 16-17).

A grande diferença entre o hacker e o Engenheiro Social é que o hacker age de forma a explorar as vulnerabilidades técnicas, enquanto o engenheiro social explora as vulnerabilidades humanas: "[...] nem todo engenheiro social é um hacker, mas em alguns casos o hacker chega a ser um engenheiro social" (PINTAUDI, 2006, p. 17).

Um fato é que a grande maioria dos funcionários/usuários não têm a devida noção de que em seu computador há documentos e arquivos que são importantes para a empresa, tornar esse conhecimento comum entre os funcionários, procurar incentivar a ponto de criar uma cultura de segurança dentro da organização é, para Ng, "[...] um ponto crucial para que um

processo de análise forense possa ser implementado dentro de uma organização" (NG, 2007, p. 101).

Os funcionários têm o costume de não se policiar em relação a segurança e são desatentos com os dados privados, por isso é tão primordial educar os usuários para que adquiram essa cultura de segurança, sem dúvida, esta ação é um dos fatores mais importantes e mais complicados de se realizar, pois a colaboração dos usuários tem uma grande influência no resultado final. Neste sentido, foram criadas metodologias e boas práticas para o ambiente corporativo; Reynaldo Ng sugere três dessas principais metodologias:

> 1º – ITIL: Forte em processos de TI, mas limitado em segurança e desenvolvimento de sistemas;
> 2º – COBIT: Forte em controles de TI e métricas de TI, mas não diz como (fluxo de processos), sendo fraco em segurança;
> 3º – ISO 27001: Forte em controles de segurança, mas não diz como (fluxo de processos) (NG, 2007, p. 19).

Desta forma, é possível saber quais os pontos críticos dos processos, pontos de falhas, responsabilidades, tecnologias e procedimentos com os quais devem ter um maior cuidado assim como quais itens devem ser priorizados, no caso de um investimento a ser realizado. A Engenharia Social é parte integrante da análise dos riscos, relativa às ameaças advindas à segurança das informações:

"[…] É no ambiente de trabalho principalmente que o cuidado deve ser maior. Pois não se sabe se poderá ser contornada, recuperada ou revertida determinada situação condizente a um ataque de engenharia social" (PINTAUDI, 2006, p. 35).

2.2 – A Segurança da Informação no Brasil e no mundo

A desconfiança é a mãe da Segurança (Madeleine Scudéry)

No início dos anos 2000 o mundo passava por uma grande evolução tecnológica e com ela um grande número de novas vulnerabilidades técnicas e diferentes tipos de incidentes surgiram junto com essas inovações. Em outubro de 2003 a empresa Módulo Security Solutions S.A. realizou uma pesquisa e listou as 10 principais ameaças à Segurança da Informação (o total é superior a 100% devido ao questionário receber múltiplas escolhas):

> 1º – Vírus – 66%;
> 2º – Funcionário Insatisfeito – 53%;
> 3º – Divulgação de Senha – 51%;
> 4º – Acesso Indevidos – 49%;
> 5º – Vazamentos de Informações – 47%;
> 6º – Fraudes, Erros e Acidentes – 41%;
> 7º – Hackers – 39%;
> 8º – Falhas na Segurança Física – 37%;
> 9º – Uso de Notebooks – 31%;
> 10º – Fraudes em E-Mail – 29%.
> (SECURITY SOLUTIONS, 2003, *Apud* PINTAUDI, 2006, p. 87).

Alguns países decidiram se juntar em prol do desenvolvimento de um grupo técnico chamado de *Computer Security Incident Response Team*, que é responsável por "[…] receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores" (FIRST, 1995-2017).

A *Forum of Incident Response and Security Teams* (FIRST) é uma organização mundial que foi fundada no início dos anos 90 com esses mesmos objetivos e é "[...] formada por equipes de uma ampla variedade de organizações, incluindo educacionais, comerciais, fornecedores, governamentais e militares" (FIRST, 1995-2017). Essa organização conta com um total de 385 equipes em 82 países diferentes. Oficialmente o Brasil conta com 5 equipes de respostas a incidentes:

> 1º – Axur Csirt
> [Localizada em Porto Alegre];
> 2º – Brazilian Academic and Research Network – CAIS/RNP
> [Localizada em Campinas];
> 3º – Computer Emergency Response Team Brazil
> [Localizada em São Paulo];
> 4º – Computer Security Incident Response Team of ARCON
> [Localizada no Rio de Janeiro];
> 5º – Defenda CERT
> [Localizada no Rio Grande do Sul] (FIRST, 1995-2017).

No dia 13 de julho de 2000, através do Decreto Nº 3.505, o Governo Federal brasileiro, oficializou a criação de um Comitê Gestor de Segurança da Informação (CGSI), o qual, segundo o professor Josué Menezes, Pós-Graduado em Recursos Humanos, relata em seu livro "Gestão da Segurança da Informação, publicado em 2006, que tem como objetivo assessorar a Secretaria-Executiva do Conselho de Defesa Nacional nos assuntos relativos à Segurança da Informação.

Este Decreto instituiu a Política de Segurança da Informação definindo como pressupostos básicos, de acordo com Menezes, três novos métodos de prevenção:

> 1) Criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
> 2) Conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade;
> 3) A criação da Infraestrutura de Chaves Públicas do Governo Federal (MENEZES, 2006, p. 96-97).

No Brasil, a entidade privada que é responsável pela padronização de regras e normas técnicas, é a ABNT – Associação Brasileira de Normas Técnicas -, a qual foi fundada em 1940 e é reconhecida como Único Fórum Nacional de Normalização, conforme expede o artigo 2 da Resolução nº 7, de 24 de agosto de 1992, do CONMETRO (Conselho Nacional de Metrologia, Normalização e Qualidade Industrial) (CONMETRO, 1992).

A ABNT participou em outubro de 1998 de uma reunião realizada em Tóquio que foi organizado pela ISO – *International Organization For Standardization* - e IEC – *International Electrotechnical Comission* - e contribuiu com o seu voto para que se aprovasse uma norma internacional, "[...] comprometida com a salvaguarda das informações nas organizações, quanto aos seus três componentes básicos: a confidencialidade, a integridade e a disponibilidade" (MENEZES, 2006, p. 50). Em agosto de 2001, o Brasil adotou a Norma ISO como seu padrão, através da ABNT, sob código NBR ISO/IEC 17799. Com essa iniciativa, as empresas no Brasil passaram a contar com uma norma referencial básica para a consecução de suas demandas mercadológicas, com maior segurança.

O primeiro Projeto de Lei que definiu regras para controlar o uso da Internet e procedimentos que caracterizam as práticas de crimes virtuais (cibercrimes) foi elaborado pelo senador Eduardo Azeredo (PSDB–MG); a última versão do projeto foi aprovado em 2012 como Lei Ordinária 12.737/2012 (BRASIL, 2012). Com a necessidade de uma atualização, em 23 de abril de 2014, a então Presidente Dilma Rousseff sancionou a Lei N° 12.965/14, mais conhecida como a Lei do Marco Civil da Internet, que "regula o uso da internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para atuação do estado" (BRASIL, 2014).

2.3 – A Engenharia Social na CIA: o caso do ex-diretor John Brennan

A consciência vale por mil testemunhas (Marcus Quintilianus)

Os detalhes do caso que será apresentado é baseado no documento "Global Internet Report 2016", que foi elaborado pela equipe de *Computer Security Incident Response Team* (CSIRT), da *Internet Society* e é assinado pela Presidente e CEO Kathy Brown e pelo Diretor sócio, Michael Kende. Este documento trata primeiramente sobre o grande crescimento de novos usuários conectados à Internet e reitera a necessidade de se educar os novos usuários a respeito dos assuntos vinculados aos crimes virtuais, ações de prevenção e análise forense. O documento detalha alguns casos de crimes virtuais recentes envolvendo grandes companhias ou pessoas com alto poder de decisão; o caso do John Brennan é um exemplo dessas pessoas que ocupam um cargo importante no seu país. Brennan era Diretor na *Central Intelligence Agency* (CIA) nos Estados Unidos e em outubro de 2015, como explicita o documento, um grupo de hackers conseguiu acesso a conta privada *AOL Account* do diretor (INTERNET SOCIETY, 2016, p. 83). O grupo de CSIRT relata que dentro desse grupo de hackers havia um que tinha o codinome de Verizon, e este, por meio de técnicas de Engenharia Social, conseguiu ter acesso, se passando pelo diretor, ao *CIA AOL PIN* do diretor e aos quatro últimos números do seu cartão de banco.

O documento ainda diz que o diretor não teve nenhum tipo de prejuízo financeiro com esse ataque, porém, para sua imagem, foi algo devastador, uma vez que tentou por muitas vezes trocar sua senha, mas os hackers, toda vez conseguia ter acesso a conta novamente, até que "[…] ele desabilitou a sua conta " (INTERNET SOCIETY, 2016, p. 83). A CIA não sabe ao certo de como o hacker Verizon conseguiu ter acesso a esse serviço da companhia e então resolveu adicionar duas novas etapas de autenticação no seu sistema de *AOL Access* com a intenção de solucionar o problema encontrado. O documento termina com a seguinte nota a qual foi chamada de *Lessons Learned* que, traduzido, nos mostra o "[...] perfil de ataque dos engenheiros sociais e a necessidade dos funcionários de serem treinados sobre como tratar as informações pessoais, por fim, mostra o quanto difícil é para o usuário entender e usar as técnicas de segurança em um ambiente online" (INTERNET SOCIETY, 2016 p. 83).

CAPÍTULO 3 – ESTUDO DO CASO

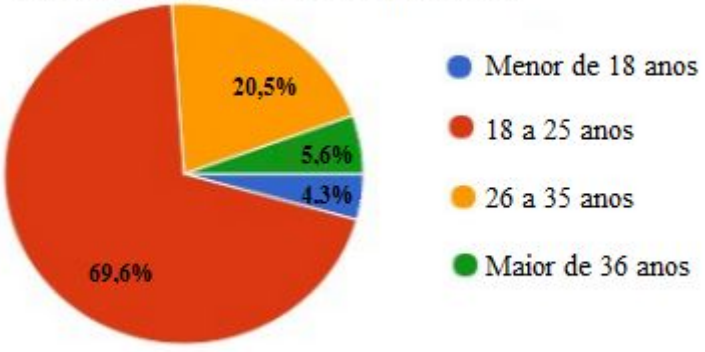
É impossível para um homem aprender aquilo que ele acha que já sabe (Epicteto)

Nesta seção buscaremos exemplificar, mediada por uma enquete, produzida por meio de uma ferramenta *online* e gratuita do Google (Google Forms), o quanto o usuário comum da Internet conhece sobre o tema Engenharia Social, e se ele acredita que esse recurso utilizado por pessoas mal intencionadas possa ser capaz de lhe causar algum ônus. A pesquisa foi realizada entre os dias 23 e 26 de outubro de 2017 e conseguiu captar 161 (cento e sessenta e uma) respostas.

A enquete foi propagada, com a inserção de seu *link*, na Rede Social (Facebook), postada em um grupo de estudantes da Universidade Estadual de Campinas (Unicamp): https://www.facebook.com/groups/GrupoUnicamp/?ref=bookmarks. Os universitários e visitantes desta página tiveram total liberdade de acessar o *link* da pesquisa e responder a enquete. Embora originalmente não fosse a intenção de saber o grau de escolaridade ou quem eram os usuários respondentes desta pesquisa, pudemos verificar que, grande parte dos colaboradores, pertenciam aos cursos de Alimentos, Matemática, Computação, Engenharia Elétrica e Automação, entre outras.

Não julgamos ser relevante a diferenciação entre usuários do sexo masculino ou feminino, uma vez que consideramos a igualdade de gêneros sexuais, mas avaliamos como oportuno a indicação da idade dos entrevistados, a fim de analisar a faixa etária e a disposição para os riscos cibernéticos:

Gráfico 1 - Faixa etária: 161 respondentes

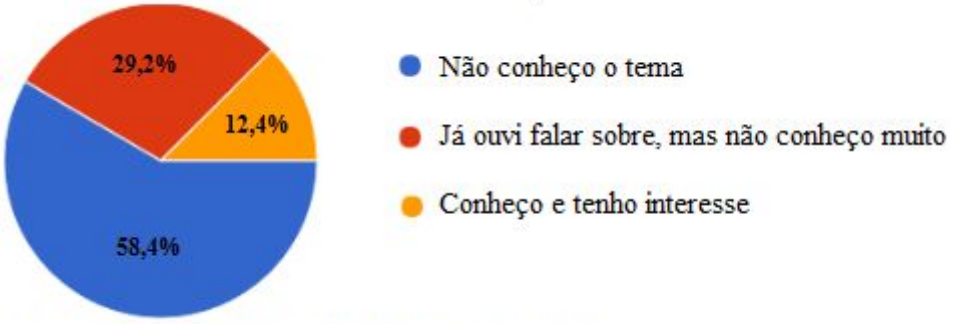


Fonte: Autoria própria (2018): Dados da pesquisa.

Conforme observamos, o Gráfico 1 funda-se nas respostas obtidas de 161 colaboradores. Como se visualiza, 69,6%, cerca de 112 respondentes, se enquadram na faixa etária entre 18 e 25 anos. O segundo maior público registrado foi dos que dizem ter entre 26 e 35 anos, com um total 33 entrevistados (20,5%); sendo que nas faixas etárias entre 36 anos ou mais e menores de 18, tivemos 9 (5,6%) e 7 (4,3%) respondentes, respectivamente.

Em seguida, acerca do tema Engenharia Social, tivemos os seguintes resultados com relação ao nível de conhecimento dos entrevistados; esse nível foi classificado de 1) para aqueles que nunca ouviram falar sobre o tema; 2) para aqueles que já ouviram falar sobre o tema, porém não têm conhecimento específico; 3) para aqueles que conhecem e têm interesse no tema abordado:

Gráfico 2 - Nível de conhecimento sobre Engenharia Social

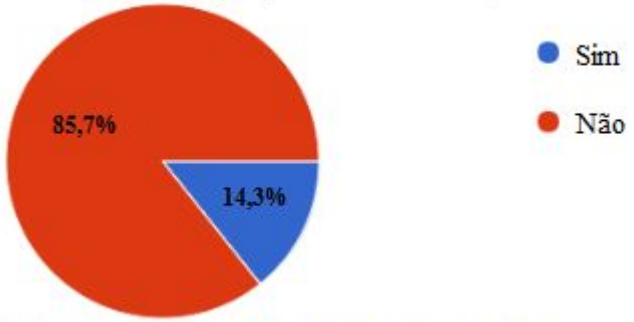


Fonte: Autoria própria (2018): Dados da pesquisa.

No Gráfico 2, de um total de 58,4% dos entrevistados, cerca de 94 respondentes, disseram que não conhecem o tema, enquanto um total de 29,2% responderam que já ouviram falar, mas não sabem muito do tema, e a minoria, com 12,4%, diz conhecer a temática.

Nesta linha de raciocínio a respeito da Engenharia Social, o autor deste Trabalho de Graduação queria saber se a empresa em que os entrevistados trabalham ou a instituição de ensino em que estes estudam e que fornece Internet gratuitamente, se, especificamente nesses locais, os usuários da rede foram ou não orientados sobre este tema:

Gráfico 3 - Orientação proveniente da Empresa ou da Escola sobre Engenharia Social

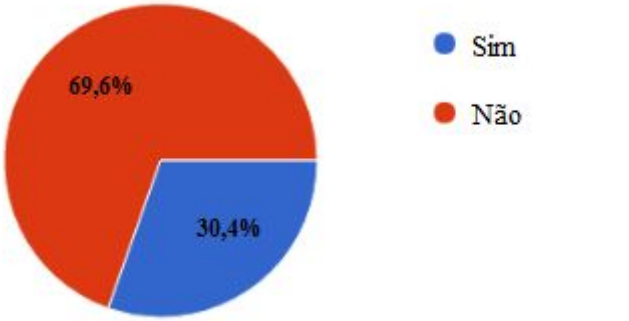


Fonte: Autoria própria (2018): Dados da pesquisa.

Para a questão proposta no Gráfico 3, obtivemos dos 161 respondentes que, 138 afirmaram negativamente, ao passo que 23 pessoas disseram que receberam orientação expedida pela Empresa ou pela Escola a respeito da Engenharia Social.

No tocante ao tema crimes virtuais, a enquete trouxe as seguintes questões: o entrevistado já sofreu algum tipo de crime desta categoria (Gráfico 4), e se o mesmo tinha sofrido com a prática de crimes virtuais ou prévio conhecimento de alguma empresa ou organização que tenha sofrido crimes virtuais (Gráfico 5), dados para os quais foram obtidos os seguintes resultados:

Gráfico 4 - Você já foi vítima desses crimes virtuais

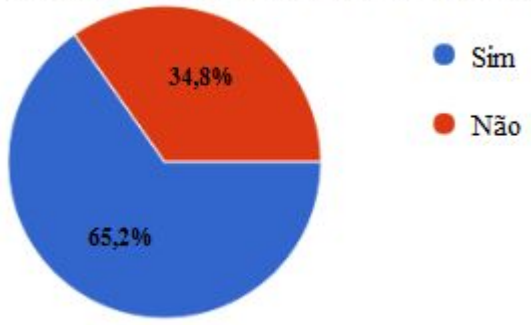


Fonte: Autoria própria (2018): Dados da pesquisa.

Para a questão proposta no Gráfico 4, obtivemos dos 161 respondentes que, 112 afirmaram negativamente, ao passo que 49 pessoas disseram que já foram vítimas de crimes virtuais. É importante salientar, segundos dados obtidos da leitura documental, a fim de erigir as bases teóricas e conceituais deste Trabalho de Graduação que, provavelmente, muitas pessoas disseram não ter sido vítimas (quase 70% dos respondentes), porquanto, podemos inferir, por terem receio de se exporem e, possivelmente, por ainda não conhecerem a

estratégia e astúcia dos invasores, que, até o exato momento, fazem as crer que não foram atacadas.

Gráfico 5 - Você conhece alguma empresa que tenha sido vítima desses crimes virtuais

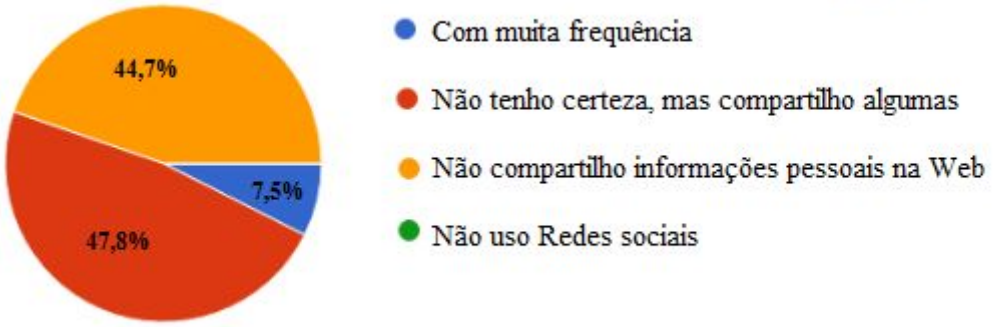


Fonte: Autoria própria (2018): Dados da pesquisa.

Já no Gráfico 5, 105 respondentes afirmaram positivamente (65,2%), ao passo que 56 pessoas disseram não conhecer nenhuma empresa vítima de crimes cibernéticos.

A partir deste momento a enquete buscou fazer uma relação entre Engenharia Social e crimes virtuais, para isso, o autor deste Trabalho de Graduação fez uso das Redes Sociais (Facebook, Instagram, Twitter) como locais *online* por meio dos quais a pesca virtual é completamente fácil de se realizar, sobretudo pelo fato de ser um local onde atualmente as pessoas estão conectadas:

Gráfico 6 - Mensuração da frequência de compartilhamento de informações pessoais na Web



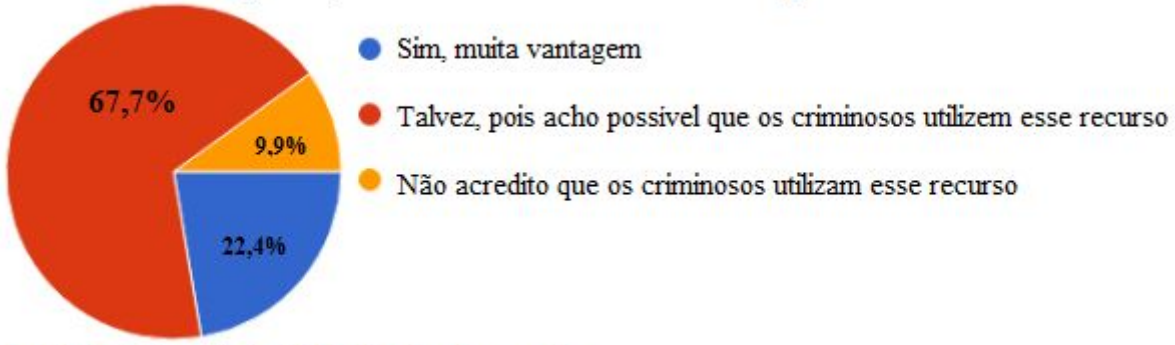
Fonte: Autoria própria (2018): Dados da pesquisa

Conforme explicita o Gráfico 6, dos 161 respondentes, 77 (47,8%) dos entrevistados admitem que compartilham algum tipo de informação pessoal na Web, ao passo que 44,7%, ou seja, 72 dos entrevistados disseram não compartilhar informações deste tipo nas Redes

sociais; apenas 12 dos entrevistados (7,5%) disseram compartilhar informações pessoais com muita frequência.

Acerca da conexão destes dois assuntos, crimes virtuais e compartilhamento de informações pessoais na Web, este autor confirmou na questão posterior, no intuito de diagnosticar se os entrevistados acreditavam que as informações socializadas na rede e o recurso fornecido pela Engenharia Social poderiam ser utilizados por pessoas mal intencionadas na prática de atos ilícitos:

Gráfico 7 - Mensuração do grau de consciência do usuário sobre a pesca virtual

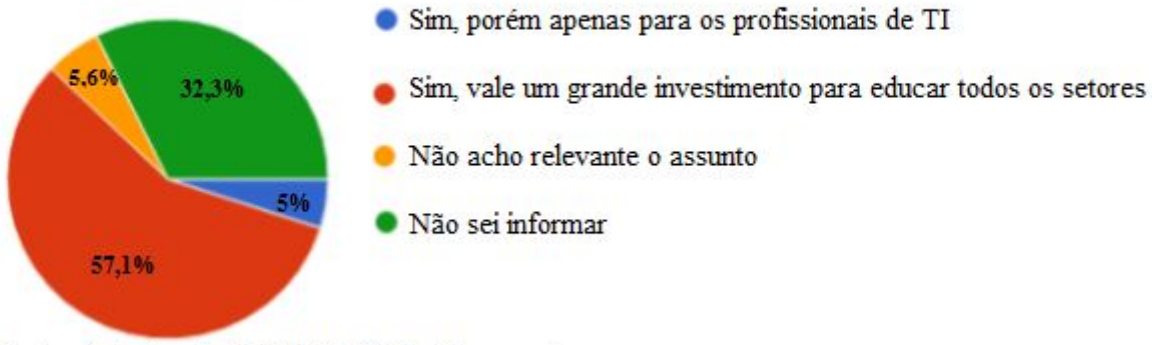


Fonte: Autoria própria (2018): Dados da pesquisa.

Conforme indica o Gráfico 7, 109 de 161 usuários (67,7%) disseram acreditar que, possivelmente, os criminosos cibernéticos fazem uso da pesca virtual para captar vítimas no mundo *online,* ao passo que 36 (22,4%) categorizaram o uso deste recurso para ludibriar as vítimas, enquanto 9,9%, ou seja, 16 entrevistas creem que os criminosos não fazem uso da pesca virtual como recurso para o delito *online*.

A última questão efetuada era saber se o brasileiro aceitaria pagar, via dinheiro público, um investimento em educação virtual para todos os setores empresariais e organizacionais sobre esta temática, ou se este investimento deveria ser realizado apenas para o setor de Tecnologia da Informação (TI):

Gráfico 8 - Educação tecnológica pautada em Engenharia Social para servidores públicos com dinheiro do erário



Fonte: Autoria própria (2018): Dados da pesquisa.

O Gráfico 8 apresenta que, a maioria dos respondentes, 92 (57,1%) de 161, acredita que valeria a pena fazer um investimento com dinheiro público para todos os servidores dos entes republicanos; não obstante, apenas 8 (5%) acreditam que esse investimento seria necessário para as pessoas que atuam exclusivamente no setor de TI. Por outro lado, 52 (32,3%) dos entrevistados não se consideram capazes de responder esta questão e 9 (5,6%) dos entrevistados não consideram o assunto relevante para auferir investimento público.

3.1 - Análise do Estudo de Caso: estamos preocupados?

O que me preocupa não é o grito dos maus [...]é o silêncio dos bons (Martin Luther King)

Os usuários da Internet que, conforme os dados obtidos através da Pesquisa de Campo deste Trabalho de Graduação, mostra-nos que a maioria, ou seja, 90,1% dos 161 entrevistados, que têm entre 18 e 25 anos (69,6%) e entre 26 a 35 anos (20,5%), possuem renda mensal, visto que trabalham, o que os possibilita fazer aquisições de materiais eletrônicos, entre eles computador pessoal, acesso a Internet, entre outros gastos pessoais, que os tornam potencialmente vulneráveis à pesca virtual.

Este grupo vem do final da adolescência e até a fase mais adulta e tem uma vida mais ativa no cenário financeiro, com várias necessidades, como adquirir novos negócios e imóveis ou apenas o prazer, conforme dissemos, de adquirir novos produtos. Esta classe é responsável por fazer parte de um grupo que mais movimenta o capital interno e agora, com com os avanços tecnológicos, pode movimentar também o capital externo, utilizando-se da Internet para efetuar ou receber transações que, dependendo do poder aquisitivo do usuário, pode ser

na casa de milhões de reais ou moedas de outras espécies, como o velho papel do Euro, do Dólar, assim como a mais nova moeda virtual de troca, a famosa *Bitcoins*.

Como disse Martin Luther King na epígrafe desta seção, é possível fazermos uma analogia com a frase dita, visto que "o grito dos maus", são, no mundo atual, artimanhas que um engenheiro social utiliza, via diálogo com a vítima, para obter os seus dados mais importantes e utilizá-los em algum ato ilícito, podendo afetá-la ou seus familiares.

A preocupação começa uma vez que se tem a noção de que a cada dia mais estamos muito mais próximos e conectados a muita gente estranha, as quais, muitas vezes, mal intencionadas, visto que estão à nossa volta e podem praticar atos contra nós, tais como difamação, calúnia, espionagem, perseguição, e, como vimos, tudo isso legalmente, pois apossaram de informações que nós gratuitamente geramos e compartilhamos na Rede, portanto, elas são socializadas com a nossa permissão, uma vez em que todos os entrevistados responderam que utilizam de Redes Sociais no seu cotidiano, sendo que 47,8% dos 161 respondentes afirmaram que compartilham informações cruciais ou sigilosas sobre sua vida, e, por incrível que pareça 67,7% dos entrevistados têm plena ciência que os criminosos possam obter vantagens ao utilizar da pesca virtual, a fim de criar um bom plano de ação, como foi relatado no episódio do falso sequestro. Isto pode ser um paradoxo, pois embora as pessoas tenham ciência do que estão fazendo na Rede, mas acreditam de alguma forma que estão blindadas espiritualmente contra todo tipo de ação cibernética.

Finalmente o preocupante "silêncio dos bons", estende, em primeiro lugar, ao governo brasileiro que, por sua vez, deveria agir de forma a integrar, de maneira inteligente e eficaz, a informática como disciplina na matriz curricular na Educação Básica e fornecer um grande investimento em infraestrutura para que seja possível ter um bom espaço de ensino em todas as escolas públicas do país. Em segundo lugar, as instituições de ensino brasileiras que, com seu poder educativo, com sua função social e cidadã, poderia auxiliar os estudantes, com orientações, cursos, fóruns, palestras, a respeito desta temática, para que, em um futuro próximo, possam estar habilitados como novos profissionais no mercado e terem uma consciência e hábitos mais seguros no acesso à Rede.

CONCLUSÃO

Ninguém vai dar segurança para você... É um problema seu! (LUIZ GASPARETTO)

O fato de que o ser humano virou refém da tecnologia é algo que devemos aceitar, assim como a Internet, que se tornou algo que o ser humano necessita, tanto para o uso pessoal - para o entretenimento e lazer -, como para o uso profissional - nas práticas do empreendedorismo e do comércio virtual -, assim a segurança, neste universo *online*, se tornou algo que merece muita atenção, porque existe, de fato, milhares de vulnerabilidades, sendo elas tecnológicas e humanas. Os próprios desenvolvedores procuram se importar mais com a acessibilidade do seu produto final do que com a segurança do mesmo, tornando o seu produto nocivo para o usuário, haja vista que, muitas vezes, o usuário não tem essa noção, pois são produtos novos no mercado. Da mesma forma que tem pessoas que querem trazer um benefício para a população, há outros motivadas em obter vantagens em cima de outros, fazendo uso destas novas vulnerabilidades. Uma senha de banco, por exemplo, um cartão clonado, fotos íntimas dos usuários, são matérias que estão constantemente em movimento nesse mundo *online*, e caso esses arquivos ou materiais se tornem públicos, as consequências aplicadas à vítima podem ser devastadoras para a vida destes simples usuário que, na verdade, têm a intenção de se divertirem e aproveitarem dessas novas tecnologias. Porém, o objetivo deste Trabalho de Graduação é mostrar a necessidade de orientar e de educar, tanto os usuários comuns da Internet, como os usuários profissionais da Rede, a respeito das boas práticas de utilização deste recurso da Internet, a fim de compreenderem que a Internet não é só um espaço lúdico e onírico, mas um ambiente eminentemente perigoso. Do mesmo jeito que a Internet pode gerar ganhos financeiros significativos, com aqueles *clicks*, esses ganhos também, paradoxalmente, podem ser transferidos para um hacker criminoso em segundos, a despeito das crises de consciências posteriores que os empresários possam ter por não investirem nas boas práticas oriundas da Segurança da Informação. Conforme supracitado, os objetivos deste Trabalho de Graduação de curso são de divulgar a necessidade das escolas de ensino superior em orientar os novos profissionais em Tecnologia da Informação sobre o tema Engenharia Social e crimes virtuais, para que eles sejam capazes de precaver-se, de educar e capacitar todos os demais usuários da Internet, via palestras e cursos sobre o tema, tornando-os mais aptos a fazerem uso desse esplêndido universo *online*, caracterizado por Apolos e Circes, ou seja, pessoas divinas e entidades maliciosas.

O presente Trabalho de Graduação não exaure a profundidade e complexidade que a temática nos reporta. Ademais, há uma vasta literatura ainda sendo produzida sobre o assunto. As nações, assim como o Brasil, têm criado diversos sistemas legais para fiscalizar, responsabilizar e punir os infratores digitais. No entanto, novas abordagens poderão ser investigadas em futuras pesquisas, seja no tocante à análise do fator humano como um agravante na Segurança da Informação, seja ainda nos estudos de como as Empresas e Universidades brasileiras têm atuado na criação de Políticas de Privacidade e de Segurança na Rede.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Referências**: NBR 6023 : ABNT, Rio de Janeiro, 2002. 24p. Disponível em: <http://www.abnt.org.br>. Acesso em: 12 set. 2017.

AT&T. **Pacific Bell (Antiga Pacific Bell).** Disponível em: <https://www.att.com/>. Acesso em: 9 ago. 2017 *Apud* LITTMAN, Jonathan, **O jogo do fugitivo**. Trad. Fernando Carlos Silva. Rio de Janeiro: Rocco, 1996.

BÍBLIA SAGRADA. **Gênesis, Capítulo 3**. Disponível em: <www.bibliaonline.com.br>. Acesso em: 7 ago. 2017.

BRASIL. **Lei 12737, de 30 de novembro de 2012**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 12 set. 2017.

BRASIL. **Marco Civil da Internet**, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 12 set. 2017.

CONSELHO NACIONAL DE METROLOGIA, NORMALIZAÇÃO E QUALIDADE INDUSTRIAL. **Resolução nº 07, de 24 de Agosto de 1992.** Disponível em: <http://www.inmetro.gov.br/legislacao/resc/pdf/RESC000017.pdf>. Acesso em: 6 set. 2017

DICIO.COM. **Astuto**. Disponível em: <https://www.dicio.com.br/astuto/>. Acesso em: 10 ago. 2017

ESTADÃO. **Crimes virtuais afetam 42 milhões de brasileiros**, 2017. Disponível em: <http://economia.estadao.com.br/noticias/releases-ae,crimes-virtuais-afetam-42-milhoes-de-brasileiros,70001644185>. Acesso em: 2 set. 2017.

FERREIRA, Aurélio Buarque Holanda. **Dicionário Aurélio da Língua Portuguesa**. 5a. ed. Rio de Janeiro : Nova Fronteira, 2010

FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS: **Mapa de Membros da FIRST**, 1995-2017. Disponível em: <https://www.first.org/members/map>. Acesso em: 6 set. 2017.

GOOGLE. **Google Forms.** Disponível em: <https://www.google.com/forms/about/>. Acesso em: 15 out. 2017.

INTERNET SOCIETY. **Global Internet Report 2016.** Disponível em: <https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf>. Acesso em: 12 jan. 2018

KARASINSKI, Lucas. Como identificar um ataque por phishing, 2 ago. 2011 *In.*: **Tecmundo**, 2018. Disponível em: <https://www.tecmundo.com.br/antivirus/12110-como-identificar-um-ataque-por-phishing.htm>. Acesso em: 10 jun.2018, às 18h

KONSULTEX Informática, 1993. Disponível em: <http://www.konsultex.com.br/>. *Apud* PINTAUDI, Mário César P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

LITTMAN, Jonathan, **O jogo do fugitivo**. Trad. Fernando Carlos Silva. Rio de Janeiro: Rocco, 1996.

MATSTON, William Moulton. **As emoções das pessoas normais**. Trad. Carlos Antônio Santos. São Paulo: Success For You, 2014.

MENEZES, Josué das Chagas. **Gestão da segurança da informação.** Rio de Janeiro: Jh Mizuno, 2006.

MODULO SECURITY, 2003**.** 9ª Pesquisa Nacional de Segurança da informação. *Apud* PINTAUDI, Mário César Peixoto, **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

NG, Reynaldo. **Forense computacional corporativa**. Rio de Janeiro : Brasport, 2007.

PINTAUDI, Mário César P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

PORTAL.G1. GLOBO.COM. **Facebook atinge os 2 bilhões de usuários**. Disponível em: <https://g1.globo.com/tecnologia/noticia/facebook-atinge-os-2-bilhoes-de-usuarios.ghtml>. Acesso em: 10 ago. 2017.

PORTAL.G1. GLOBO.COM. **Golpe do falso sequestro aplicado por telefones ganha nova versão**, 2015. Disponível em: <http://g1.globo.com/jornal-nacional/noticia/2015/07/golpe-do-falso-sequestro-aplicado-por-telefone-ganha-nova-versao.html>. Acesso em: 10 ago. 2017.

PORTAL.G1. GLOBO.COM. **HBO é hackeada; episódios e informações de 'Game of Thrones' são roubados**, 2016. Disponível em: <https://g1.globo.com/tecnologia/noticia/hbo-foi-hackeada-e-episodios-e-informacoes-de-game-of-thrones-foram-roubadas.ghtml>. Acesso em: 2 set. 2017.

PORTAL.G1. GLOBO.COM. **HBO ofereceu US$ 250 mil após roubo de dados, dizem hackers**, 2016. Disponível em: <https://g1.globo.com/tecnologia/noticia/hbo-ofereceu-us-250-mil-apos-roubo-de-dados-dizem-hackers.ghtml>. Acesso em: 2 set. 2017.

SYMANTEC CORPORATION. **Enterprise security:** filtro de conteúdo: treinamento de segurança na internet para funcionários**,** 1995-2007. Disponível em: <https://www.symantec.com/>. Acesso em: 17 abr. 2004. *Apud* NG, Reynaldo. **Forense computacional corporativa**. Rio de Janeiro : Brasport, 2007.