UNIVERSIDADE FEDERAL DE MINAS GERAIS

Faculdade de Educação

Especialização em Gestão de Instituições Federais de Educação Superior

Reinaldo Vitor Pedroso

Engenharia social: o vínculo mais frágil da segurança

Belo Horizonte

2019

Reinaldo Vitor Pedroso

Engenharia social: o vínculo mais frágil da segurança

Artigo Científico de especialização apresentada à Faculdade de Educação da Universidade Federal de Minas Gerais, como requisito parcial à obtenção do título de Especialista em Gestão de Instituições Federais de Educação Superior.

Orientador: Prof. Dr. Marcelo Antônio Nero

Belo Horizonte

2019

UNIVERSIDADE FEDERAL DE MINAS GERAIS
FACULDADE DE EDUCAÇÃO
Curso de Especialização
Gestão de Instituições Federais de Educação Superior

GIFES

ATA DA DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Candidato: Reinaldo Vitor Pedroso

Registro DRCA: 2017769937

CPF: 039.032.056-05

Orientador (a): Marcelo Antônio Nero

Às 10 horas do dia 21/12/2019, reuniu-se na Faculdade de Educação da UFMG a Comissão Examinadora indicada pela coordenação do Curso de Especialização Gestão de Instituições Federais de Educação Superior, para julgar, em exame final, o trabalho intitulado ***"ENGENHARIA SOCIAL O VÍNCULO MAIS FRÁGIL DA SEGURANÇA"***, requisito final para obtenção do grau de Especialista. Abrindo a sessão, a banca examinadora, após dar conhecimento aos presentes do teor das Normas Regulamentares do Trabalho Final, passou a palavra ao candidato para apresentação de seu trabalho. Após a apresentação do trabalho, seguiu-se o julgamento e expedição do resultado final. Foram atribuídas as seguintes indicações:

Marcelo Antônio Nero indicou a

☒ APROVAÇÃO / ☐ APROVAÇÃO COM RESSALVA/ ☐ REPROVAÇÃO do candidato;

Leonardo Antônio Soares indicou a

☒ APROVAÇÃO / ☐ APROVAÇÃO COM RESSALVA/ ☐ REPROVAÇÃO do candidato;

Ludmila Olandim de Souza indicou a

☒ APROVAÇÃO / ☐ APROVAÇÃO COM RESSALVA/ ☐ REPROVAÇÃO do candidato;

Pelas indicações, o candidato foi considerado ☒ APROVADO / ☐ REPROVADO

O resultado final foi comunicado publicamente ao candidato pela banca examinadora. Nada mais havendo a tratar, a Comissão Examinadora encerrou a sessão, da qual foi lavrada a presente ATA.

Belo Horizonte, 21 de dezembro de 2019

Marcelo Antônio Nero

Leonardo Antônio Soares

Ludmila Olandim de Souza

Ludmila Olandim de Souza

Resumo

É fato que as organizações têm investido no progresso de seus parques tecnológicos, porém estão ausentando-se quanto ao fator humano. A engenharia social, como o próprio nome sugere, busca uma forma de apropriação de modo simples e eficaz, utilizando do sistema de informação mais vulnerável possível, o ser humano. Ela constitui-se de práticas realizadas para conseguir informações sigilosas de sistemas, de empresas ou de pessoas comuns; tais como senhas, utilizando para isso da confiança de seu alvo. Essa é a sua forma de ação mais prestigiosa. A engenharia social evidencia-se, cotidianamente, na sociedade, devido à superexposição de informações pessoais ou profissionais, principalmente em redes sociais. Cabe ressaltar que, os ataques realizados pela engenharia social não possuem fórmula nem método definido, pois podem usufruir de ataques físicos, *on-line* ou psicológicos. No primeiro, inquirem sobre o local de trabalho ou moradia, esmiúçam lixeiras, e, por telefone, se passam por outra pessoa, seja por meio de ligações, seja por aplicativos de mensagens. No *on-line* utilizam de técnicas e softwares, que através da internet possa ajudá-lo a colher informações. Por fim, nos ataques psicológicos, inquirem o lado emocional dos alvos em potencial. Esse artigo distendeu um estudo de caráter qualitativo, e tem como propósito uma pesquisa exploratória do tema Engenharia Social, principalmente quanto aos ataques advindos da tecnologia; ela facilita a vida de todas as pessoas, porém se for utilizada de maneira adequada.

Palavras-chave: Engenharia Social. Fator humano. Ataques. Informações.

Abstract

It is a fact that organizations have invested in the progress of their technology parks, but they are absent on the human factor. Social engineering, as its name suggests, seeks a form of appropriation in a simple and effective way, using the most vulnerable information system possible, the human being. It consists of practices carried out to obtain confidential information from systems, companies or ordinary people; such as passwords, using your target's confidence to do so. This is its most prestigious form of action. Social engineering is evidenced, daily, in society, due to the overexposure of personal or professional information, mainly in social networks. It should be noted that the attacks carried out by social engineering do not have a defined formula or method, as they can take advantage of physical, online or psychological attacks. In the first, they inquire about the place of work or home, break down trash bins, and, by telephone, impersonate another person, either through calls or through messaging applications. In online use techniques and software, which through the internet can help you gather information. Finally, in psychological attacks, they inquire into the emotional side of potential targets. This article extended a qualitative study, and its purpose is an exploratory research on the Social Engineering theme, mainly regarding the attacks coming from technology; it makes life easier for everyone, but if used properly.

Keywords: Social engineering. Human factor. Attacks. Information.

ENGENHARIA SOCIAL
O VÍNCULO MAIS FRÁGIL DA SEGURANÇA

Reinaldo Vitor Pedroso*
Marcelo Antonio Nero**

RESUMO

É fato que as organizações têm investido no progresso de seus parques tecnológicos, porém estão ausentando-se quanto ao fator humano. A engenharia social, como o próprio nome sugere, busca uma forma de apropriação de modo simples e eficaz, utilizando do sistema de informação mais vulnerável possível, o ser humano. Ela constitui-se de práticas realizadas para conseguir informações sigilosas de sistemas, de empresas ou de pessoas comuns; tais como senhas, utilizando para isso da confiança de seu alvo. Essa é a sua forma de ação mais prestigiosa. A engenharia social evidencia-se, cotidianamente, na sociedade, devido à superexposição de informações pessoais ou profissionais, principalmente em redes sociais. Cabe ressaltar que, os ataques realizados pela engenharia social não possuem fórmula nem método definido, pois podem usufruir de ataques físicos, *on-line* ou psicológicos. No primeiro, inquirem sobre o local de trabalho ou moradia, esmiúçam lixeiras, e, por telefone, se passam por outra pessoa, seja por meio de ligações, seja por aplicativos de mensagens. No *on-line* utilizam de técnicas e softwares, que através da internet possa ajudá-lo a colher informações. Por fim, nos ataques psicológicos, inquirem o lado emocional dos alvos em potencial. Esse artigo distendeu um estudo de caráter qualitativo, e tem como propósito uma pesquisa exploratória do tema Engenharia Social, principalmente quanto aos ataques advindos da tecnologia; ela facilita a vida de todas as pessoas, porém se for utilizada de maneira adequada.

Palavras-chave: Engenharia Social. Fator humano. Ataques. Informações.

* Autor
** Orientador

1. INTRODUÇÃO

Pode-se dizer que o termo engenharia social é usualmente utilizado para se referir às técnicas utilizadas por pessoas mal-intencionadas que abusam de relações sociais para obtenção de informações sigilosas ou o acesso a sistemas (Silva *et al*., 2013). Essa engenharia é uma das técnicas mais “simples” e usuais de roubo de informações importantes. É a hábil manipulação da tendência humana natural de confiar.

A engenharia social usa a influência e a persuasão para iludir pessoas (Leite, 2017). O engenheiro social pode aproveitar-se das pessoas para obtenção de informações, com ou sem o uso da tecnologia, uma vez que ele se passa por alguém que realmente não é ou por meio da manipulação de seu alvo (Coelho *et al*., 2013).

Com o surgimento e o avanço da internet, os crimes se manifestaram e se propagaram com intensa velocidade no meio digital. Logo, com o estelionato não foi diferente: a grande rede tornou-se um meio muito utilizado para a concretização deste delito.

Devido ao grande aumento de invasões sofridas pelas organizações em suas bases de dados, estas têm voltado atenção para a atualização de seus parques tecnológicos, como, por exemplo, aplicando as técnicas de criptografia, utilização de sistemas biométricos, e constantes atualizações de *firewalls*, porém deixando o fator humano em segundo plano.

2. TIPOS E ALVOS DE ATAQUES NA ENGENHARIA SOCIAL

A obtenção de informações confidenciais, secretas ou sigilosas não se dá apenas por meios tecnológicos. Os bandidos estão por toda parte e no mundo digital em que todos vivem, eles também estão neste ambiente para colher informações de suas vítimas, esperando praticar diversos crimes por meio de dados colhidos.

Uma empresa pode ter investido nas melhores tecnologias de segurança; pode ter despendido energia no treinamento, capacitação e orientação de seu pessoal, de modo a garantir o sigilo da empresa antes de deixar o expediente; e pode ter contratado segurança especializada com as melhores empresas desse setor disponíveis no mercado. Entretanto, essa empresa, mesmo tomando uma ou o conjunto de medidas

apresentadas, pode estar vulnerável à ação de engenharia social (Coelho, 2013).

O engenheiro social procura obter informações da vítima ou empresa como, por exemplo, agenda de compromissos, dados de conta bancária, número de cartão de crédito a serem usados para o ataque. Nesse tipo de “crime”, as pessoas podem aplicar protocolos de segurança recomendadas por especialistas; podem adquirir e instalar produtos de segurança e efetuar as configurações e atualizações indicadas para cada versão do hardware e/ou software destinadas às correções e aplicações dos devidos módulos de segurança. Vale ressaltar que, ainda assim, essas vítimas estarão suscetíveis às ameaças advindas da engenharia social.

Em grandes empresas, instituições financeiras, militares, órgãos do governo e, até mesmo, hospitais, a situação é semelhante. Só que, nesse caso, envolvem pessoas preparadas, os chamados *hackers*, e as formas de ataque utilizadas são mais audaciosas. A meta dos *hackers* é obter acesso não autorizado aos sistemas, sabotar informações, espionagem industrial, roubo de identidade ou simplesmente sobrecarregar os sistemas a ponto de tirá-los de operação.

Existem basicamente dois tipos de ataques: o direto e o indireto. A eficiência deles depende das habilidades pessoais do *hacker* e do quanto ele se identifica com os processos. Usualmente, é necessário utilizar uma combinação de ambos para obter o resultado almejado. Para chegar à abordagem direta, o invasor obteve uma bela coleção de informações obtidas de modo indireto. Estes modos de ataque serão discutidos a seguir.

2.1. Ataque Direto

O ataque direto é caracterizado pelo contato pessoal. Em geral são realizados por telefone, por meio de ligações ou mensagens de aplicativos (embora *hackers* mais confiantes ousam fazê-los pessoalmente) e exigem planejamento detalhado e antecipado, vários planos de emergência para cada uma das fases do ataque e um pouco de “dom artístico”, visto que um bom invasor possui maior chance de sucesso caso seja mais amigável e carismático. Esse tipo de ataque deve ser bem articulado para que seu planejamento não seja desmascarado, além de contar também com rotas de fuga bem articuladas para o caso de algo fora do planejado dê errado.

2.2. Ataque Indireto

O ataque indireto constui-se na utilização de ferramentas de invasão (como cavalos de troia e sites de código malicioso) e de impostura (e-mails, cartas e sites falsos com a aparência de verdadeiros) para obter informações pessoais. Os usuários individuais de quem o *hacker* extrai os dados são apenas vetores para a coleta de informações de uma entidade maior – empresa, organização ou governo. Sua intenção não é atacar cada um desses usuários, mas sim o organismo maior ao qual eles estão vinculados.

3. MANIPULANDO O FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO

A engenharia social, de modo simples, tem como ênfase explorar as fragilidades do ser humano; ou seja, consiste na habilidade de obter informações ou o acesso indevido a determinados ambientes e/ou sistemas, utilizando para isso técnicas de convencimento e/ou espionagem.

As técnicas de ataque são as mais variadas, sempre explorando a fragilidade e ingenuidade das pessoas. Nenhum artigo sobre ataques de engenharia social estaria completo sem citar o famoso e um dos maiores *hackers* de todos os tempos, Kevin Mitnick (Goodell, 1996). Iguais a ele, atualmente existem muitos e as táticas utilizadas são basicamente as mesmas.

As principais armas de um engenheiro social podem ser divididas em duas técnicas maiores: pesquisa e personificação/impostura. A pesquisa refere-se à fase de coleta de objetos e/ou informações a fim de descobrir quais são as pessoas que detém as informações almejadas. Por sua vez, a técnica da impostura baseia-se na concepção de um personagem, que é quando o engenheiro social interpreta ser alguém que não é. Na impostura, muitos engenheiros sociais chegam a estudar sobre os padrões de fala e quanto aos tipos de linguagens utilizadas por suas vítimas (Pereira & Martins, 2014).

Além das técnicas citadas, os ataques de engenharia social podem se dar através de aspectos distintos: o físico, como o local de trabalho ou até mesmo *on-line*, e o psicológico, que se refere à maneira como o ataque é executado, tal como a persuasão e o convencimento.

4. MEIOS DE ATAQUE

A tecnologia de ponta não é suficiente para impedir o roubo de informações, visto que dados eletrônicos ou não eletrônicos podem ser passados para outra pessoa de forma muito simples, por apenas uma conversa. A conversa que permite obter dados pode ocorrer em vários ambientes. Pode acontecer diretamente, de forma presencial, ou ocorrer por meio de ambientes virtuais, e-mails ou redes sociais.

A criatividade dos criminosos, que usufruem da ingenuidade das pessoas, encontra um campo fértil para roubo e furtos virtuais, haja vista que não há sistemas 100 % seguros. Contudo, com o auxílio desta mesma tecnologia, são criados meios eficazes de minimizar os riscos relacionados à segurança da informação (Coelho *et al*., 2013).

Os meios de ataques se dão das mais variadas formas possíveis. Podem ser considerados simples ou complexos, depende do meio utilizado e do alvo. Independente da forma utilizada, a finalidade é explorar sempre a ingenuidade e fragilidade das pessoas. Na sequência são listadas algumas das formas comuns que ajudam os hackers a provocar o ataque.

4.1. *Spam*

Através do uso de *spams* são disparados e-mails para um grande número de remetentes se passando por órgãos prestadores de serviço, como agências bancárias, receita federal, entre outros, utilizando dizeres como dívidas pendentes ou malha fina. Possuem abordagens características e, até mesmo, logotipos idênticos às organizações pelas quais se passam. Esses falsos e-mails são acompanhados por um *hiperlink* que redireciona para uma página falsa, que possuirá campos de entrada para preenchimento dos dados do usuário e, subsequentemente, o sequestro de tais informações (Silva *et al*., 2012).

Em algumas situações, os *spams* são mal executados e apresentam, surpreendentemente, erros de digitação, onde, por muitas das vezes, páginas falsas são criadas na internet com tais erros grotescos, muito recorrente em redes sociais ou até mesmo agências bancárias, disponibilizado por um *hiperlink* que direciona o usuário para entrar com login e senha ou a conta bancária e a senha. Contudo, um usuário que

está em um situação vulnerável, como a situação de débitos pendentes ou a possibilidade de se tornar um devedor, não leva em conta esses detalhes, tornando-se mais vulnerável ao ataque dessa categoria.

4.2. Telefonia

Antes do avanço da internet, a telefonia era o meio mais utilizado para obter informações (Mitnick & Simon, 2002). Entretanto, ainda nos dias atuais, continua sendo uma arma muito usual para aplicação de golpes por intermédio da engenharia social. As táticas utilizadas nesse meio são inúmeras, lançando mão da utilização, até mesmo, das músicas de espera características, na tentativa de se passar por funcionários de determinada empresa. Atualmente, esse golpe é muito aplicado também através dos aplicativos de mensagens, como o telegram e o whatsapp (Komo *et al*., 2018). No Brasil, uma população que vem sofrendo, recorrentemente, com esse tipo de ataque é a população de idosos aposentados, que são alvos fáceis dos engenheiros sociais (Rohr, 2012).

4.3. Local de Trabalho

O local de trabalho é um ambiente favorável para engenheiros sociais. Práticas cotidianas e comuns, como anotar senhas de sistemas, redes e/ou *e-mails* em *post-its* e anexar ao monitor ou gabinete do computador facilita a entrega de informações, muitas dessas inclusive, deveriam ser sigilosas e não ficar expostas ao ambiente de trabalho, em especial em locais de ampla circulação de pessoas.

Nomes, lista de ramais, endereços eletrônicos, organogramas e outros dados da empresa, comumente ficam expostos em lugares onde podem transitar terceiros. Um *hacker* pode, simplesmente, entrar na empresa como se fosse um técnico em manutenção ou consultor que tem livre acesso às dependências da instituição e, enquanto caminha pelos corredores, captar todas estas informações que porventura estejam expostas (Popper & Brignoli, 2010).

4.4. Lixo

O lixo das empresas pode até ser considerado por muitos como o local de

simples descarte de material que não são mais úteis. Porém, é considerado uma fonte muito rica de informações para um *hacker*. Vasculhar o lixo é um método muito usado pelos invasores, já que nele é comum encontrarmos itens como cadernetas e/ou anotações com números de telefones, organograma da empresa, manuais de sistemas utilizados, memorandos, relatórios com informações estratégicas, apólices de seguro e até anotações com *login* e senha de usuários.

As listas telefônicas muitas das vezes fornecem os nomes e números das possíveis vítimas; o organograma indica quem são as pessoas na liderança dos departamentos/diretorias; os manuais de usuário de sistemas orienta como acessar informações. Diante disso, ressalta-se que todo e qualquer lixo, que contenha dados e informações, pode ser de grande valia para um engenheiro social (Popper & Brignoli, 2010).

4.5. Senhas

As senhas são os principais pontos fracos das pessoas; logo, das empresas. É comum as pessoas compartilharem usuários e senhas em sistemas com colegas; ou escolherem senhas consideradas fracas, sem o menor receio. Muitos usam como senha palavras que constam no dicionário, seus apelidos, o próprio nome e sobrenome ou iniciais destes, que, com a utilização de um *software* gerenciador de senhas, torna-se possível decifrá-las em segundos (Alves, 2007).

A displicência dos usuários ao criar senhas fáceis de serem descobertas, que ficam longos períodos sem alterá-las, ou que utilizam a mesma senha para acesso a várias contas, facilita ainda mais o ataque. Dessa forma, o *hacker* não precisará elaborar ataques demasiadamente elaborados para adquirir as informações almejadas e obter consequente sucesso (Granger, 2001).

A segurança das senhas é um elemento fundamental para que os sistemas de informação sejam protegidos adequadamente. Ao tratar sobre segurança de senhas, entende-se que a senha precisa se forte o suficiente para impedir que alguém a descubra futuramente. Ou seja, a senha precisa ser atribuída com base em algo visando que dificilmente outra pessoa possa imaginar.

4.6. Redes Sociais

Nos dias atuais, as redes sociais são a porta de entrada para a realização de ataques de engenharia social, afinal esse ambiente é favorável a lidar com os valores humanos, tais como a amizade, a solidariedade e a compaixão, tudo isso é um arcabouço para o engenheiro social, que se faz de amigo, ganhar a confiança e credibilidade da vítima, e no final acabar conseguindo as informações importantes que almeja. A imprudência no comportamento perante as redes sociais é sem dúvida farta para os ataques de engenharia social.

A educação e bom comportamento em redes sociais visam a evitar aborrecimentos. Por exemplo, informações de momentos de lazer ou que não há ninguém em uma residência devem ser postadas somente após o evento, e nunca durante a realização do mesmo, visando garantir que criminosos não irão se valer destas informações para a prática de crimes.

A falta de proteção a dados e a superexposição pode ocorrer ainda por meio da troca de mensagens em redes sociais, situação na qual pessoas muitas vezes passam informações sigilosas para desconhecidos e expõem suas vidas pra pessoas de má índole, que podem utilizar destas informações para fins ilegais. Nem todas as pessoas que querem conhecer outras na internet estão mal intencionadas, no entanto é bom não passar informações confidenciais para quem não se conhece realmente.

Dentre as maneiras de ataques em redes sociais, as correntes do bem também são bem comuns. Criminosos se aproveitam de catástrofes e/ou mensagens de pessoas desaparecidas ou insalubres; daí os “telespectadores” se comovem e muitas das vezes depositam dinheiro na conta informada que nunca chegam ao destino que deveria. Fato é que se faz necessário o máximo de cautela no manuseio de informações por meio dessas redes.

4.7. Persuasão

A engenharia social utiliza-se de práticas para obter acesso a informações sigilosas em organizações e sistemas computacionais, por meio da exploração de confiança das pessoas com habilidades de persuasão. Para conseguir persuadir o alvo e conquistar sua confiança, o engenheiro social deve possuir algumas habilidades,

como ser ousado, ter capacidade de influenciar pessoas, além de procurar conhecer bem o alvo.

Muitos criminosos utilizam as técnicas de engenharia social antes de tentarem a invasão de sistemas; afinal, é muito mais fácil ser “bom de papo” do que dominar assuntos relacionados aos sistemas operacionais, redes, programação, entre outros. Os *hackers* vêm a engenharia social de um ponto de vista psicológico, enfatizando como criar o ambiente psicológico perfeito para um ataque.

O melhor método para conseguir a informação no ataque de engenharia social é ser amistoso. No caso de investidas em empresas, o local para tentativa de abordagem com êxito não necessariamente precisa ser nas dependências da mesma; pode se dar, por exemplo, em uma academia ou em um restaurante. O necessário é que o *hacker* conquiste a confiança do funcionário alvo, independentemente do local, a ponto de convencê-lo a prestar todo o auxílio requerido. Ademais, a maior parte das pessoas responde bem às gentilezas. Um *hacker* preparado sabe bem o momento de parar de tentar extrair informações antes que a vítima possa suspeitar que está sendo alvo de um assédio (Granger, 2001).

4.8. Engenharia Social Inversa

Um recurso mais avançado de conseguir informações ilícitas é com a engenharia social inversa. Isto ocorre quando um *hacker* cria uma personalidade que aparece numa posição de autoridade, de modo que todos os usuários lhe pedirão informação. Se pesquisados, planejados e bem executados, os ataques de engenharia social inversa permitem ao *hacker* extrair dos funcionários informações muito valiosas; entretanto, isto requer muita preparação e pesquisa.

Os três métodos de ataques de engenharia social inversa são, propaganda, ajuda e sabotagem. Na sabotagem, o *hacker* causa problemas na rede, então divulga que possui a solução para este, e se propõe a solucioná-lo. Na expectativa de ver o lapso corrigido, os funcionários passam para o *hacker* todas as informações por ele solicitadas. Após atingir o seu objetivo, o hacker elimina a falha e a rede volta a funcionar normalmente. Resolvido o problema os funcionários sentem-se satisfeitos e jamais desconfiarão que foram alvos de um *hacker* (Granger, 2001).

4.9. *Footprint*

Muitas das vezes o invasor não consegue coletar as informações desejadas através de um e-mail, telefonema ou uma conversa amigável, seja porque as pessoas não detêm o conhecimento necessário ou por não conseguir alcançar pessoas ingênuas.

A técnica conhecida como *footprint* tem o objetivo de levantar informações sobre um determinado alvo sem o perigo de detecção, ou seja, para que o invadido não perceba que o invasor está obtendo as informações; que, através de softwares específicos, consegue as informações necessárias ao ataque (Segurança da Informação, 2008).

Footprint é um perfil completo da postura de segurança de uma organização que se pretende invadir. Fazendo uso de uma combinação de ferramentas e técnicas, atacantes podem empregar um fator desconhecido e convertê-lo em um conjunto específico de nomes de domínio, blocos de redes e endereços IP individuais de sistemas conectados diretamente na Internet. Embora haja diversas técnicas diferentes de *footprint*, seu objetivo primordial é descobrir informações relacionadas a tecnologias de *internet*, acesso remoto e *extranet* (Veríssimo, 2002).

5. MÉTODOS DE PREVENÇÃO

É sabido que a engenharia social trabalha com as atitudes humanas, logo temos de partir do princípio de não confiar em quaisquer pessoas. Duvide de tudo. Seja cauteloso. Verifique os links no rodapé do navegador antes de clicar; no caso de dúvidas ligue para a empresa para confirmar o pressuposto do e-mail.

O estágio de exação de informações usando a técnica de engenharia social pode tornar-se intempestiva em um ambiente no qual as pessoas estejam conscientes e bem treinadas. As pessoas bem informadas e treinadas serão muito menos suscetíveis a ataques de engenharia social (Maulais, 2016). Cada organização deve compreender que a segurança não é somente uma questão de tecnologia; ela passa por uma gestão de processos e de pessoas. Faz-se necessário criar uma cultura de segurança dentro da empresa.

Os seres humanos são imperfeitos e possuem características variadas e

peculiares. Além do mais, situações de risco transfiguram seus comportamentos em instantes, e, decisões serão estreitamente baseadas em confiança e grau de criticidade da situação (Alves, 2007).

Para atenuar os riscos oriundos da engenharia social, é aconselhável que as empresas criem políticas de segurança centrada e bastante divulgada, fazendo com que todos os colaboradores saibam como poder contribuir para a proteção das informações que estão em seu poder. A divulgação dessas políticas pode dar-se através das *intranets*, como também de boletins periódicos *on-line* e outras formas disponíveis. O maior risco é de os funcionários tornarem-se complacentes e relaxarem na segurança; por isso a importância da insistência (Granger, 2001).

Na tabela 1, a seguir, estão expostas as principais áreas de risco junto às empresas, as habilidades mais comuns usadas pelos *hackers* e também as estratégias de combate.

TABELA 1 – Zonas de Risco, Habilidades do Hacker e Técnicas de Enfrentamento.

Zona de Risco	**Habilidades do *Hacker***	**Estratégias de Combate**
Suporte de informática	Performance e persuasão.	Aprimorar na empresa uma política de alteração de senhas para trocas periódicas; fazendo constar a validade de expiração, nível de complexidade para criação e sistema de bloqueio de contas. Faz-se necessário capacitar os funcionários para atender às regras dessa política; e também se conscientizarem da importância de não compartilhar senhas com terceiros.
Entrada nas Dependências da Empresa	Acesso físico não identificado e não autorizado.	Capacitar os funcionários da recepção e de segurança a não permitirem o acesso de pessoas não identificadas, além da verificação visual. É necessário que todos que circulam pela empresa portem o crachá de identificação, seja funcionários ou visitantes.
Escritórios	Percorrer os ambientes a fim de capturar informações.	Todos os visitantes devem ser acompanhados por um funcionário da empresa. Não digitar quaisquer senhas na presença de pessoas estranhas, caso não seja possível afastar a pessoa,

		deve-se bloquear a visão da pessoa de forma discreta. Manter os documentos confidenciais fora do alcance de pessoas não autorizadas.
Suporte telefônico	Utilização de disfarces no momento de pedir auxílio aos atendentes; geralmente fazendo-se passar por outra pessoa.	O atendente deve solicitar sempre um código de acesso e/ou mesmo CPF para identificar o solicitante e prestar o suporte solicitado. Ao atender a ligação deve-se fazer constar o senso crítico, pois essa é a arma para o combate de '*fake-news*' e possíveis golpes. Nunca se devem fornecer informações financeiras ou pessoais durante uma conversa telefônica com desconhecidos.
Sala dos servidores	Instalação de programas analisadores de protocolos, os quais são capazes de monitorar o tráfego de uma rede em tempo real; com isso objetivam capturar informações confidenciais.	Deve-se manter a sala dos servidores sempre trancada, de preferência com tranca biométrica. Chaves, mesmo que tetra, podem ser facilmente roubadas, assim como as trancas podem ser arrombadas. Essa segurança faz-se necessária, pois essa sala é o centro de armazenamento da inteligência da empresa, portanto seu acesso é limitado aos funcionários autorizados e qualificados. O inventário de equipamentos deve estar atualizado.
Depósito de lixo	Vasculhar o lixo.	O lixo da empresa deve estar guardado em lugar seguro até ser removido. Todo tipo de documento em papel deve ser triturado; as mídias magnéticas devem ser destruídas quando descartadas.
Internet e *intranet*	Criação e/ou inserção de softwares maliciosos na Intranet e/ou Internet para captação de senhas.	Criar senhas fortes e fazer uso consciente da mesma; alterando-as periodicamente. Os modems nunca devem ter acesso à *intranet* da empresa.

5.1. Plano de Resposta a Incidentes

É preciso estar consciente que não há infraestrutura de segurança da informação que venha garantir 100% de proteção, pois os deslizes sempre existirão, por mais remotos que sejam. Logo, as empresas devem estar preparadas para analisar, reconhecer e tratar os incidentes de segurança de maneira mais ágil possível quando acontecerem; isso é condição primordial para atenuar os estragos ou diminuir os custos

de restauração (Alves, 2007). A habilidade de usar essa informação para reparar ou prevenir ocorrências futuras e similares, aprimora a segurança geral a uma organização.

Cabe ressaltar que, o Plano de Resposta a Incidentes é um documento que descreve as diretrizes gerais e os procedimentos para tratamento dos principais incidentes de segurança que podem ocorrer na organização, proporcionando ao pessoal de suporte instruções sobre as medidas a serem tomadas para a definição e correção dos mesmos.

O tipo de tratamento dado aos incidentes de segurança varia de acordo com a sua intensidade e risco. Porém, o encaminhamento deve ser decidido em acordo com a alta direção da empresa e com o respaldo do departamento jurídico (Popper & Brignoli, 2010). As ações pertinentes podem abranger o relacionamento com entidades externas (como parceiros, clientes, provedores de serviços, dentre outros) ou mesmo requerer o acionamento de autoridades e órgãos policiais.

O conjunto de métodos de ataque de engenharia social é muito vasto, e os procedimentos de resposta aos incidentes apesar de indicados por especialistas, são particulares de cada empresa. Estas particularidades tende a variar de acordo com o ramo de atividade de cada empresa; o que pode ser considerado imprescindível para uma, pode ser dispensável para outra, e vice-versa. Entretanto, toda empresa, independente do ramo e/ou do porte, deve ter o seu Plano de Resposta a Incidentes.

6. Crimes Informáticos

A tecnologia facilita a vida de todas as pessoas se for utilizada de maneira adequada. Entretanto, com o advento da internet, os crimes se manifestaram e se propagaram intensamente no meio digital. Obviamente, com o estelionato não foi diferente, a rede mundial de computadores tornou-se o meio utilizado para a realização deste delito.

Segundo Cassanti (2014), no Brasil, os crimes de informática superam até o narcotráfico [...]. A praticidade da rede não atrai as pessoas apenas para o uso do internet *banking*, mas também para as compras virtuais, fato este que tem aumentado bastante os números de fraudes envolvendo cartões de crédito em todo o Brasil.

6.1. Do Estelionato Digital

No mundo digital, o crime de estelionato digital apresenta característica típica da era atual; com o avanço tecnológico suas maneiras de execução têm sido cada vez mais variadas.

Para Cassanti (2014):

> Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital.

As compras realizadas de modo *on-line* tem sido a principal isca para este tipo de crime. Páginas falsas, tanto de compras como de bancos, por exemplo, são usadas para obter dados sigilosos de usuários, os induzindo ao erro, e consequentemente a cair no golpe digital de transações bancárias e comerciais, obtendo vantagem ilícita mediante meio fraudulento, configurando o delito de estelionato digital (Vicente e Marcelino, 2017).

6.2. Legislação Penal acerca de Crimes Informáticos

Punir os responsáveis pelos ataques de engenharia social não é uma tarefa fácil, pois muitos dos delitos nem podem ser considerados crimes, por exemplo, a obtenção de informações encontradas no lixo ou expostas sobre a mesa, ou mesmo ouvir uma conversa em um lugar aberto.

Por outro lado, os crimes que ocorrem *on-line*, devido aos inúmeros fatores, dentre eles o anonimato, a exposição de informações em redes sociais, constantes da estrutura virtual também são difíceis de serem combatidos. Inicialmente porque a rede não respeita fronteiras entre países, o que dificulta administrar as diferenças culturais ou aplicar leis nacionais (Popper & Brignoli, 2010).

O maior incentivo aos crimes virtuais é dado pela falsa sensação de que o meio digital é um ambiente sem leis, entretanto, a internet não é uma terra sem leis. Cada vez mais há legislação com parâmetros para incriminar e condenar o culpado. É importante saber que quando o computador é uma ferramenta para prática dos delitos, suscita a possibilidade de se amoldar aos tipos penais já existentes.

A lista de crimes cometidos por meio eletrônico é extensa. Na grande maioria dos casos é possível adaptar os crimes virtuais à legislação vigente.

Cassanti (2014) afirma que:

> O judiciário vem coibindo diariamente a sensação de impunidade que reina no ambiente virtual e combatendo a criminalidade cibernética com a aplicação do Código Penal, do Código Civil e de legislações específicas como a Lei nº 9.296/96 – que trata das interceptações de comunicação em sistemas de telefonia, informática e telemática – e a Lei nº 9.609/98 – que dispõe sobre a proteção da propriedade intelectual de programas de computador.

Em 2012 entrou em vigor a Lei Federal nº 12.737/2012 (Brasil, 2012) que trata sobre os crimes de Internet; e foi apelidada de Lei Carolina Dieckmann, onde tipifica os crimes informáticos, com a inclusão no Código Penal. O art. 154-A do Código Penal, que foi inserido após a promulgação da referida lei nº 12.737/2012 (Brasil, 2012) versa sobre o crime de invasão de dispositivo informático, no qual o bem protegido é a inviolabilidade dos segredos, ou seja, os dados e informações armazenados no computador, podendo ser tanto de pessoas físicas quanto jurídicas de direito privado ou público (Tavares & Reis, 2014).

7. CONCLUSÃO

Na análise acerca da engenharia social é possível observar que o fator humano é o vínculo mais frágil da segurança. Assim, é possível afirmar que a maior parte dos desastres e/ou incidentes com a segurança da informação tem como fator predominante a intervenção humana. Para ser um engenheiro social basta conhecer e manipular o cérebro humano; trabalhar a reação e estudar os movimentos das pessoas.

Por meio da engenharia social, muitas pessoas através da prática de manipulação psicológica estão vulneráveis, deixando obter informações sigilosas e/ou importantes, enganando e inquirindo a confiança, seja ela por meio de fraudes, sequestros de dados ou outros crimes no meio digital, rompendo procedimentos de segurança. Muitas pessoas e/ou empresas que descobrem que foram atacadas, dificilmente admitem o fato, com receio de ter prejudicada a sua reputação. No entanto, a admissão das falhas podem conduzir à prevenção das mesmas no futuro.

É aconselhável que exista nas empresas uma política de segurança centralizada e bastante divulgada, para que todos saibam como se defender e a quem recorrer em caso de dúvidas e/ou tentativas de golpes. Cabe ter cautela e atentar-se para que as pessoas não se tornem paranóicas, mas que estejam sempre precavidas perante às

diversas solicitações que a elas sejam direcionadas, e que possam compreender o valor da informação pelas quais são responsáveis. Afinal, as pessoas precisam se educar e educarem aqueles que estão sob sua responsabilidade, pois o maior desafio da segurança da informação é o ser humano. Proteções físicas e lógicas existem muitas, mas o maior responsável por garantir a proteção da informação é o usuário, que necessita ser educado para o mundo virtual.

Por fim, cabe conscientizar-se que as ferramentas de engenharia social estão de posse de todos; o uso consciente e planizado delas é que faz a diferença. Quanto mais bem preparados estiverem os cidadãos e os colaboradores de uma empresa, mais segura todos estarão.

REFERÊNCIAS

ALVES, Cássio Bastos. **Segurança da informação Vs. Engenharia Social - Como se Proteger para não ser mais uma vítima.** Disponível em: <https://monografias.brasilescola.uol.com.br/computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm>. Acesso em: 19 de setembro de 2019.

CASSANTI, Moisés de Oliveira; **Crimes virtuais, vítimas reais.** 1. ed. Rio de Janeiro, 2014. *E-book*.

COELHO, Cristiano F. *Et al*. **Engenharia Social: Uma Ameaça à Sociedade da Informação.** 2013. Disponível em: <http://www.seer.perspectivasonline.com.br/index.php/exatas_e_engenharia/article/view/87/59> Acesso em: 17 de setembro de 2019.

GOODELL, Jeff. **O Pirata Eletrônico e o Samurai - A Verdadeira História de Kevin Mitnick e do Homem que o Caçou na Estrada Digital.** Rio de Janeiro. Editora Campus. 1996.Trad. Ana Beatriz Rodrigues. Título Original: The Cyberthief and the Samurai.

GRANGER, Sarah. **Social Engineering Fundamentals, Part I: Hacker Tactics.** Disponível em: <https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>. Acesso em 15 de agosto de 2019.

KOMO, Andrea E. *Et al.* **Aplicativo de troca de mensagens instantâneas utilizando comunicação P2P.** 2018. Disponível em: <https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/4143> Acesso em: 29 de setembro de 2019.

LEITE, Bruno Pacheco Coelho. **Gestão de Coleções Especiais e Livros Raros no Brasil: Um Estudo sobre Engenharia Social.** 2017. Disponível em: <https://portal.febab.org.br/anais/article/view/1985/1986> Acesso em: 19 de setembro de 2019.

MAULAIS, Claudio Nunes dos Santos. **Engenharia Social: Técnicas de ataque e defesa em empresas de micro, médio e grande porte.** Universidade FUMEC, 2016. Disponível em: <http://fumec.br/revistas/sigc/article/view/4723/2522>. Acesso em: 19 de setembro de 2019.

MITNICK, Kevin D.; SIMON, William. L. **Mitinick: A Arte de Enganar.** Pearson Education. São Paulo. 2002.

PEREIRA, Leandro de Deus; MARTINS, Daves Márcio Silva. **Engenharia Social: Segurança da Informação Aplicada à Gestão de Pessoas - Estudo de Caso.** 2014. Disponível em: <https://seer.cesjf.br/index.php/cesi/article/view/129/49> Acesso em: 01 de outubro de 2019.

POPPER, Marcos Antonio; BRIGNOLI, Juliano Tonizetti. **Engenharia Social - Um Perigo Eminente.** Instituto Catarinense de Pós Graduação. 2010. Disponível em: <https://www.academia.edu/38720641/ENGENHARIA_SOCIAL_Um_Perigo_Eminente >. Acesso em: 04 de setembro de 2019.

ROHR, A. **Conheça a relação entre hackers e a 'engenharia social'.** 2012. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/conheca-a-relacao-entre-hackers-e-a-engenharia-social.html). Acesso em 30 de agosto de 2019.

Segurança da Informação, 2008. Disponível em: <http://grupocsi.blogspot.com/2008/06/footprinting.html>. Acesso em: 29 de setembro de 2019.

SILVA, Clayton Silvestre *et. al*. **Engenharia social: o elo mais frágil da segurança nas empresas.** Revista Eletrônica do Alto Vale do Itajaí, 2012. Disponível em: < http://www.revistas.udesc.br/index.php/reavi/article/view/2840/2172> Acesso em: 15 de setembro de 2019.

SILVA, Narjara Bárbara Xavier *et. al*. **Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação.** Revista Ibero-Americana de Ciência da Informação, 2013. Disponível em: <http://periodicos.unb.br/index.php/RICI/article/view/1782> Acesso em: 15 de setembro de 2019.

TAVARES, Adriano Lopes; REIS, Rafael Rocha dos. **Crimes de Informática.** 2014. Disponível em: <http://revistas2.unievangelica.edu.br/index.php/revistajuridica/article/view/1070/1012>. Acesso em 01 de outubro de 2019.

VERÍSSIMO, Fernando. **Segurança em Redes sem Fio.** Monografia (Pós- Graduação em Programa de Engenharia de Sistemas e Computação). Rio de Janeiro. Universidade Federal do Rio de Janeiro, 2002.

VICENTE, Patrick, MARCELINO, Juliano Daniel. **Estelionato digital e engenharia social.** 2017. Disponível em: <https://jus.com.br/artigos/57198/estelionato-digital-e-engenharia-social> Acesso em: 30 de setembro de 2019.