ENGENHARIA SOCIAL: A PORTA DE ENTRADA PARA INFORMAÇÕES CONFIDENCIAIS

LUIZ TIAGO SOUZA PINTO[1]
ORLANDO LEONARDO BERENGUEL[2]

RESUMO

Indústrias e instituições investem em segurança da informação utilizando tecnologias como: antivírus, firewall, IPS, proxy, sistema de autenticação por biometria ou cartões. Essas tecnologias elevam os custos da tecnologia da informação (TI), porém são necessárias para manter a confidencialidade, integridade e disponibilidade das informações. Mas esse custo pode se tornar inútil se o fator humano não for levado em consideração. A utilização de senhas com baixa complexidade, falta de treinamento dos colaboradores que utilizam os sistemas da empresa e a não adoção de uma política clara de prevenção a ataques de engenharia social, deixam as organizações vulneráveis. A engenharia social usa da psicologia e fatores comportamentais humanos para explorar falhas de segurança e conseguir acesso a sistemas ou dados sigilosos. Esse artigo propõe através de revisão bibliográfica exibir técnicas e destacar a importância que as empresas e instituições devem dar quando se trata de ataques.

Palavras-chave: segurança, engenharia social, tecnologia, pessoas.

[1] - Graduado em Gestão da Tecnologia da Informação na Fatec Jornalista Omair Fagundes de Oliveira Bragança Paulista, Brasil. E-mail: l.t.souza14@gmail.com.
[2] - Doutor em Ciências pela Universidade Estadual de Campinas, UNICAMP, Brasil. E-mail: oberenguel@ifsp.edu.br.

SOCIAL ENGINEERING: THE DOORWAY TO CONFIDENTIAL INFORMATION

ABSTRACT

Industries and institutions invest in information security using technologies such as antivirus, firewall, IPS, proxy, biometric authentication system or cards. These rise the information technology (IT) costs, but are necessary to maintain the confidentiality, integrity, and availability of information. But that cost can become useless if the human factor is not taken into account. The use of passwords with low complexity, lack of training of employees who use company systems, and the non-adoption of a clear social engineering prevention policy, leave organizations vulnerable. Social engineering uses psychology and human behavioral factors to exploit security gaps and gain access to sensitive systems or data. This article proposes through literature review to show techniques and highlight the importance that companies and institutions should give when it comes to attacks.

Keywords: *security, social engineering, technology, people.*

1. INTRODUÇÃO

A engenharia social, no contexto da tecnologia da informação refere-se às técnicas de manipulação de pessoas com a finalidade de ultrapassar barreiras de segurança. São formas de conseguir informações nas quais quem está sendo atacado, ou seja, o alvo raramente nota esse tipo de ação. Entre as formas mais utilizadas estão os telefonemas, correios eletrônicos, salas de bate papo, redes sociais e o contato direto. Segundo Mann (2011), a maioria das organizações visa quase completamente à segurança técnica. Os agressores sabem disso e com frequência utilizam uma rota mais simples para o acesso a dados confidenciais, as pessoas.

É importante destacar que, seja qual for a solução de segurança adotada, independente do hardware e software utilizados, o elemento de maior vulnerabilidade continuam sendo as pessoas, devido a comportamentos e traços psicológicos que podem as tornam susceptíveis a ataques de engenharia social. A porta para a invasão pode estar em situações muito comuns, tais como a vontade de ser útil, busca por novas amizades, propagação de responsabilidades e persuasão.

Em 2014 entre todas as tentativas de invasões e quebras de segurança registradas, 43% se deram através da engenharia social, isso corresponde a quase metade dos incidentes. Dentro deste percentual de abordagem, 66% foram iniciados com uso de e-mail com conteúdo malicioso (SOCIAL-ENGINEER, 2017).

Thomas (2007) destaca que não é suficiente depositar toda a confiança apenas em produtos de segurança, caso o faça estará fadado à mera ilusão da segurança. O uso da engenharia social não é uma novidade e nem é exclusivamente utilizada por alguém que possui conhecimentos técnicos em TI.

O objetivo geral do artigo é explicar a engenharia social, em que contexto é utilizada, de que forma pode passar desapercebida pela maioria das vítimas, e contribuir para evitar ataques a dados sigilosos ou estratégicos através da conscientização. São objetivos específicos analisar as principais formas de ataque e de prevenção na perspectiva das políticas de segurança para elevar o nível de confiabilidade e confidencialidade das informações.

A engenharia social é um campo de estudo de muita relevância na medida em que todas as pessoas e empresas possuem dados, informações e conhecimentos que não devem ou não podem ser compartilhados e que, em um mundo totalmente digital cada vez mais são necessário cuidados específicos para manter privados os seus dados. Desta forma, é importante o conhecimento mesmo que mínimo do que se trata a engenharia social, como o engenheiro age, como é possível se prevenir e proteger de muitos casos de invasão de privacidade e ataques cibernéticos. Esta hipótese é reforçada com argumentos do maior “hacker” da história, Mitnick, que através do seu livro “A arte de enganar (2003)”, tenta conscientizar a todos do quanto estamos vulneráveis e não percebemos a gravidade do problema.

Para o desenvolvimento da pesquisa foi realizada revisão bibliográfica para a construção do referencial teórico, artigos publicados e recuperados em bases indexadas.

2. REFERENCIAL TEÓRICO

Existem várias definições de engenharia e engenheiro social, além de diferentes modelos e estratégias de ataque, abaixo seguem definições utilizadas para o desenvolvimento desse trabalho.

2.1 Conceitos de engenharia social

Comumente a engenharia social é definida como, a ciência do uso da interação social como um meio de convencer um indivíduo ou uma organização a cumprir uma solicitação específica de um invasor, onde a interação social, a persuasão ou a solicitação envolve uma entidade relacionada ao computador (MOUTON, 2016). A "arte" de influenciar pessoas e divulgar informações confidenciais é conhecido como engenharia social e o processo de fazer isso é denominado como um ataque de engenharia social.

Quebrar o “firewall humano” quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo” (MITNICK, 2003, pág.16).

Basicamente, conceitua-se “engenharia social” (em inglês “social engineering”) como a arte de manipular indivíduos com objetivos previamente definidos a fim de contornar dispositivos de segurança, sendo assim, uma técnica para obtenção de informações por parte do agressor com uso de telefone, correio eletrônico, correio tradicional ou até mesmo contato direto (CARVALHO, 2015).

Em outras palavras (CARVALHO, 2015, pág. 129), “a engenharia social é baseada na utilização da força de persuasão e na exploração da ingenuidade dos utilizadores, fazendo-se passar por uma pessoa da casa, um técnico, um administrador etc.”.

Um engenheiro social é – na maior parte dos casos – bom em lidar com pessoas, agindo de forma charmosa, educada e agradável, o que facilita estabelecer uma afinidade e uma relação de confiança com a vítima. Um atacante experiente que possua tais características pode ter acesso a qualquer informação se fazendo uso dessas estratégias e táticas (MITNICK; SIMON, 2003).

O engenheiro social busca as mais diversas informações de suas vítimas, variando desde nomes de familiares, números de documentos, telefones, informações sobre filhos e rotinas do dia a dia, como também informações profissionais que se referem à atuação e relacionamentos do alvo dentro da empresa, documentos oficiais, manuais etc. Essas informações fornecerão a ele mais assertividade para estabelecer relação de confiança com sua vítima, considera-se uma das etapas mais determinantes para sucesso de um ataque de engenharia social.

O engenheiro social explora a natureza humana de confiar nas pessoas até que se prove o contrário, estabelece uma relação entre o agressor e a vítima. Criar uma relação com o alvo é considerado um ponto crítico, pois, a qualidade do relacionamento construído pelo invasor determina o nível de cooperação e até onde o alvo estará disposto a ir para ajudar o invasor na obtenção do seu objetivo.

Segundo Mitnik e Simon, (2003, pág. 33) “nós como seres humanos, somos todos sujeitos a ser enganados, porque a confiança das pessoas pode ser usada de forma errada se for manipulada de determinadas maneiras”.

Ainda pela a ótica dos autores,

> [...] o engenheiro social prevê a suspeita e a resistência, e ele está sempre preparado para transformar a desconfiança em confiança. Um bom

> engenheiro social planeja o seu ataque como um jogo de xadrez, e prevê as perguntas que o seu alvo pode fazer para estar pronto para dar as respostas corretas. Uma dessas técnicas comuns envolve a criação de uma sensação de confiança por parte da sua vítima. (MITNIK; SIMON, 2003, pág. 33)

O próximo passo no escopo do ataque é a exploração, durante essa etapa é que o engenheiro social usa as informações previamente coletadas para explorar ativamente o alvo. Assim, o atacante está focado em manter o momento de conformidade e o relacionamento que foi construído na fase anterior, sem despertar desconfiança. A exploração neste momento pode ocorrer através de divulgação, venda de informação confidenciais ou aparentemente sem relevância, ou o acesso pode ser transferido para um outro indivíduo com interesse no alvo.

Por último é realizada a execução do ataque, esta é a etapa em que o objetivo final é alcançado ou por várias possíveis razões, o atacante encerra de forma natural para não levantar suspeita sobre o que acabara de acontecer. Também é nesta etapa que quaisquer pontas soltas são corrigidas, como por exemplo, remoção de pegadas digitais que possam identificar a ação ou o invasor. Uma estratégia de saída bem planejada e suave é sempre visada pelo atacante como seu ato final.

2.2 Vetores de ataque – Técnicas empregadas na engenharia social

Há diversas técnicas utilizadas por engenheiros sociais para a obtenção da informação desejada em um ataque. Estas estão diretamente condicionadas ao grau de dificuldade e tipo de vulnerabilidade a ser explorada, sempre considerando seu alvo. Desta forma, seguem descritas algumas das principais técnicas adotadas:

a) dumpster diving (análise do lixo): Considerada uma das fontes mais ricas para um engenheiro social, o lixo pode fornecer informações importantes e relevantes, pois é ali que são descartados materiais de pessoas físicas ou jurídicas sem a menor preocupação na maioria dos casos. Neles pode-se encontrar nomes de usuários e senha, papeis timbrados vazios, memorandos internos, rascunhos, documentos financeiros etc.

b) tailgating: ou conhecido também como *Piggybacking*, é uma técnica física de engenharia social, que se concentra em obter acesso a um edifício protegido, mesmo que possua dispositivos de segurança como autenticação por cartões inteligentes ou biometria. Pode acontecer quando o engenheiro social segue indivíduos autorizados, ou utiliza da boa-fé de terceiros para conseguir a entrada em locais de acesso restrito.

d) shoulder surfing: Chamadas de surfe de ombros, essa técnica consiste no engenheiro social observar e coletar informações simplesmente olhando por cima dos ombros da vítima. As informações podem variar de Ids de usuários, senhas e dados confidenciais. Como objeto de observação, pode considerar computadores, notebooks, smartphones e tablets, dentro e fora do ambiente corporativo.

e) abordagem pessoal: Esta técnica consiste no engenheiro social realizar uma visita na empresa alvo, podendo se passar por um fornecedor, colaborador terceirizado, amigo do diretor, prestador de serviço, entre outras possibilidades. Durante essa "visita" através do poder de persuasão e falta de treinamento dos funcionários, o atacante consegue sem muita dificuldade convencer um segurança, secretária, recepcionista por exemplo a liberar o acesso ao datacenter ou um local de acesso restrito, onde possivelmente conseguirá as informações que procura (RAFAEL, 2013).

f) phishing: Phishing é a técnica mais utilizada na engenharia, consiste em um ataque cujo objetivo é roubar informações privadas, como por exemplo: login e senha de contas de acesso a sistemas corporativos, dados bancários, informações sensíveis, dados de redes sociais etc. Está técnica também pode ser utilizada para instalar softwares maliciosos no equipamento alvo. Para isso, o invasor se passa por pessoa ou entidade confiável e tenta persuadir a vítima. O ataque usa como veículo principal e-mails e mensagens por redes sociais, solicitando alguma ação urgente, assim ao dar continuidade ao processo, a vítima é direcionada para um site de *phishing*, que possuem aparência familiar, ou baixa um anexo com conteúdo malicioso. (UNICAMP, 2012)

g) internet e redes sociais: Esta técnica é o início de um estudo detalhado sobre a vítima, traçando um perfil e levantando possíveis vulnerabilidades para abordagem. Como citado por Rafael (2013), a pesquisa online é um vetor de ataque utilizado para conhecer melhor o seu alvo, coletando informações disponíveis na internet. Iniciando a pesquisa pelo site da corporativo que geralmente disponibilizam informações sobre localização física, produtos e serviços oferecidos, números para contato, biografia de executivos e diretores da empresa.

Facebook, Twitter, LinkedIn e outras plataformas de mídia social ajudam as pessoas a se conectarem, mas também ajudam a descobrir preferências, família e hobbies. Com essas informações, engenheiros sociais podem criar e-mails de *phishing* ou chamadas de *vishing* com os gatilhos emocionais certos para atingir seu objetivo com êxito. Essas táticas de engenharia social são altamente psicológicas e na prática funcionam melhor, quando as informações coletadas sobre uma pessoa específica são usadas para obter mais informações sobre a organização para a qual elas trabalham.

h) vishing (contato telefônico): É definido como a prática de obter informações ou tentar influenciar ações por telefone. O objetivo desse método é obter dados valiosos que possam contribuir para o comprometimento direto de uma organização ou pessoa física, explorando a boa vontade das pessoas em ajudar. De acordo com Rafael (2013), é uma técnica subsequente a etapa de levantamento de informações, quando é realizada a abordagem via telefone o engenheiro social já possui informações sobre o alvo como, nome de secretárias, gestores até colaboradores envolvidos com TI. Durante um ataque de vishing, o engenheiro social impersonifica alguém que possa criar um elo de confiança com a vítima, como um funcionário do atendimento ao cliente ou suporte.

i) watering holes: “Um ataque watering hole é um exploit de segurança em que o atacante procura comprometer um grupo específico de usuários finais [...], infectando sites que eles normalmente visitam” (PROOF, fonte online). Como meio de abordagem desta técnica, o atacante pode infectar um site de uso cotidiano de um grupo ou de um indivíduo alvo. Isso não levantará suspeita, já que para o usuário o

ambiente acessado é seguro, uma vez que o ataque for realizado o engenheiro social retira o conteúdo malicioso da página sem deixar rastros.

j) smishing: Esta abordagem é realizada através de envio de mensagens SMS ou aplicativos de mensagens para telefones celulares, geralmente contendo um link que direciona a vítima à um formulário, solicitando algumas respostas que podem variar, como a atualização de um cadastro, resgates de prémios entre outros. Essa técnica tem como objetivo principal a coleta de informações pessoais como: endereço, CPF, dados de cartão de crédito, senhas de acesso a banco, credenciais de acesso a redes sociais e contas de e-mails.

k) trojan horse (cavalo de tróia): Alguns engenheiros sociais exploram a curiosidade ou a ganância das pessoas e utilizam softwares mal-intencionados como forma de ataque e exploração da vítima. O criminoso envia um e-mail com um anexo ou link que se apresenta como algo gratuito ou urgente. O anexo pode ser rotulado como, número de rastreamento de uma encomenda postal, um prêmio vencedor ou um boleto a ser pago etc. Ao abrir o anexo ou clicar em um link o alvo está aceitando que esse Trojan seja carregado e executado no computador ou dispositivo móvel.

De acordo com Fonseca (2017), um Trojan é um software mal-intencionado disfarçado como legítimo que pode realizar enormes malefícios, desde o roubo de senhas até a destruição de dados sensíveis, roubo de informações bancárias e abrir portas para acesso e controle remoto de dispositivos.

3. TENDÊNCIAS E UTILIZAÇÃO DE ATAQUES

Como apontado por Frumento (2018), A Engenharia Social como forma de ameaça à segurança digital está evoluindo há alguns anos em um ritmo acelerado. Até o final do século passado, a engenharia social era uma forma avançada, porém de nicho de atacar sistemas dedicados, hoje é uma metodologia comum em ataques cibernéticos. O nível de complexidade dos ataques para explorar o elemento humano é incrivelmente alto.

O “Relatório de tendências de atividade de phishing. Unificando a resposta global ao cyber crime, APWG” (2017), divulgado periodicamente, evidencia esse comportamento.

Tabela 1 – Tipos de infecção e porcentagem de efetividade.

Tipos de infecção	% de efetividade
Trojans	74.99%
Vírus	1.55%
Worms	1.50%
Adware/ Spyware	0.51%
PUPs (programas não desejados)	21.45%

Fonte: Autoria própria

A tabela acima mostra que os ataques que não necessitam de atuação humana, e são totalmente automatizados, os vírus e *worms* representam apenas 3,05%. Enquanto ameaças que necessitam de algum tipo de consentimento ou ação do alvo para que sejam realizados totalizam 96,95% de quebras de segurança no período.

Estimativas percentuais exatas podem variar de estudo para estudo, mas a maioria dos ataques cibernéticos é projetada para tirar proveito dos erros humanos durante o processo de infecção e infiltração, e não de falhas em hardware ou software como meio de acesso a dados não públicos. De acordo com a (ProofPoint 2018) as vulnerabilidades humanas são mais perigosas para as organizações modernas do que as falhas de técnicas.

Utilizando de tempo e paciência, um engenheiro social vai eventualmente encontrar um ponto de vulnerabilidade a ser explorado em um determinado alvo. A barreira de defesa contra esse tipo de ataque é a conscientização e medidas de prevenção tomadas por funcionários. Os colaboradores devem ser treinados e testados por profissionais em segurança. A empresa também deve disponibilizar documentação, incluindo detalhes de como são realizadas as tentativas ataques e as consequências de ataques de engenharia social bem-sucedidos.

4. MELHORES PRÁTICAS PARA PREVENÇÃO

O primeiro passo a ser considerado quando se desenvolve e implementa uma política de segurança para mitigar ataques de engenharia social, está na conscientização de todos os colaboradores da empresa, até mesmo terceirizados ou visitantes. Promover atividades que elucidem as maiores e menores dúvidas, criar uma base de conhecimento sobre a técnica – que acontecem das mais diversas formas – para que os funcionários se sintam respaldados em duvidar sempre que algo aparentemente esteja errado. É importante deixar claro aos colaboradores que é comum desconfiar e solicitar confirmação de credenciais, permissões etc., esse ato não significa não querer colaborar com o andamento dos processos da empresa, mas sim agregar mais segurança a tudo e todos.

Segundo Kumar et al (2015), os colaboradores da empresa devem ser educados em como serem relutantes na revelação de informações por meio de treinamento. É imprescindível também a criação e disseminação das políticas de como lidar com informações sobre a empresa e os funcionários, implementar auditorias periódicas, política de descarte consciente de documentos físicos da organização. E por fim, a empresa deve atentar-se ao que disponibiliza na internet sobre si mesmo, pois isso pode ser o início de um ataque.

De acordo com Social Engineer (2019), é importante a garantia de que as políticas foram claramente comunicadas aos colaboradores, e que haja recompensa aos indivíduos que as seguem a fim de haver incentivos e compartilhamento do esforço em praticar.

Ainda de acordo com a Social Engineer (2019), como há uma grande quantidade de ataques estabelecidos por *vishing*, é fundamental a orientação aos seus colaboradores sobre o que é esta técnica, e quais são os meios de prevenção. Como em caso de suspeita, realizar a solicitação de mais informações, verificação de permissões. Em caso de dúvida persistente, comunicar o interlocutor que até que seja efetuada uma comprovação de sua identidade, não será possível continuar com a comunicação, pois se trata de uma política da empresa. E reportar ao superior imediatamente.

Em caso de *phishing*, recomenda-se fortemente a conscientização dos usuários em não abrir e-mails e mensagens eletrônicas aparentemente suspeitas, orientar através de passos simples como verificar ortografias, URLs, e até mesmo passar o ponteiro do mouse em cima do link afim de ver para onde será direcionado após um clique.

A prevenção contra os mais diversos tipos de ataques deve ser unanime dentro de uma organização, pois, se uma pessoa for vítima de alguma forma, todo o resto fica vulnerável e exposto. De tal forma, abaixo lista-se algumas ações preventivas que devem ser adotadas, de acordo com Kumar et al (2015):

- Use logins diferentes para cada serviço e proteja suas senhas: nunca use a mesma senha para todos os serviços. Certifique-se de que as senhas sejam fortes e complexas.
- Use a autenticação de dois fatores: isso dificulta o acesso de atacantes à suas contas, mesmo que seu nome de usuário e senha esteja comprometido.
- Use a criatividade nas perguntas de segurança: sites que solicitam que você preencha perguntas de segurança adicionais supostamente agregam mais uma linha de defesa, mas essas perguntas costumam ser facilmente descobertas, como por exemplo, onde você nasceu?
- Use cartões de crédito com sabedoria: cartão de crédito é a maneira mais segura de pagar pela internet, melhor que cartões de débito ou sistemas de pagamento online como Paypal. Por haver fortes medidas de proteção utilizadas pelas financeiras. Se um hacker tiver acesso ao número de um cartão de débito, toda a conta bancária pode ser drenada. Você pode proteger ainda mais seu cartão de crédito optando por não armazenar o cartão números em sites.
- Monitorar com frequência suas contas e dados pessoais, estar atento ao roubo de identidade e a fraudes de cartão, checar seus saldos em conta e pontuação de crédito regularmente. Vários serviços oferecem monitoramento de roubo de identidade gratuito. Você pode até usar o Google Alerts como um alerta para roubo de identidade, criando um alerta de SMS a cada vez que sua conta fizer um login.
- Remova suas informações de bancos de dados de informações públicas: Sites que publicam informações privadas online como ZabaSearch e People Finders.

Entretanto, conclui Kumar (2015), a melhor maneira de prevenção que há na luta contra a engenharia social é o questionamento, duvide e desconfie de tudo e todos, pois são nas ações mais comuns e frequentes do dia a dia que o engenheiro social irá agir. Para o atacante, é indispensável que sua ação pareça uma ação rotineira e sem importância.

5. CONSIDERAÇÕES FINAIS

Técnicas de engenharia social tem sido utilizada a muito tempo, mas só se tornaram uma ameaça à segurança com o desenvolvimento da tecnologia da informação, em um contexto onde os dados se tornaram o principal ativo e motivo de preocupação no mundo corporativo.

Com o amadurecimento das tecnologias de informação, a dependência pelo mundo digital tem crescido exponencialmente. O mercado de cyber segurança tem evoluído rapidamente, no entanto os indivíduos continuam sendo o elo mais vulnerável do sistema de proteção a dados e informações armazenados de forma digital. Explorando isso, a engenharia social se torna o vetor de ataque predominante dentro do mundo da tecnologia da informação.

Um estudo recente publicado pelo *Anti Phishing Working Group* (APWG) (2017), mostra que apenas cerca de 3% dos malwares tentam explorar uma falha exclusivamente técnicas. Enquanto 97%, dos ataques utilizam alguma participação dos usuários. As tentativas de *hacking* se concentram cada vez mais nas vulnerabilidades humanas de um sistema, ao invés da quebra de segurança por meio de vulnerabilidades em software ou hardware. Esta é uma tendência crescente.

O entendimento sobre como esses ataques podem afetar a confiabilidade do negócio com seus clientes, fornecedores e participação no mercado. Sendo claro na política de segurança da empresa, e periodicamente relembrado através de lembretes na intranet da companhia e mensagens de e-mail periódicas. É importante ressaltar em todos os níveis do negócio a estratégia para proteção contra esses ataques, a não ser que todos façam sua parte, a empresa e seus dados continuam vulneráveis a engenharia social.

Educação para potenciais vítimas é a chave para o combate a engenharia social, procedimentos, normas e políticas de segurança são a parte mais importante na diminuição e mitigação do impacto desses ataques.

REFERÊNCIAS

APWG. **Unifying the global response to cybercrime**. Phishing Activity Trends Report 4th, 23 fev. 2017. Disponível em: http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf. Acesso em: 22 jun. 2019.

BRODY Richard G; Brizzee, William B; CANO, Lewis, Flying under the radar: Social engineering. **International Journal of Accounting and Information Management**, 2012.

CARVALHO, Cristiane Rodrigues Brandão De; GALVÃO, Angel Pena. Engenharia social: Uma análise de ameaças e cuidados aos funcionários das agências bancárias de santarém e itaituba – pará. **Revista EM FOCO - Fundação Esperança/IESPES**, [S.l.], v. 2, n. 24, p. 127-141, abr. 2016. ISSN 2319-037x. Disponível em: http://iespes.edu.br/revistaemfoco/index.php/Foco/article/view/61/51. Acesso em: 21 Mai. 2019.

CHITREY, Anubhav; SINGH, Dharmendra; BAG, Monark, SINGH, Vrijendra. A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. **International Journal Information and Network Security**, 2012.

FONSECA, Marcelo. **Engenharia social: Conscientizando o elo mais fraco da segurança da informação**. [*S. l.*], 5 maio 2017. Disponível em: https://riuni.unisul.br/bitstream/handle/12345/2402/TCC_versao_final_1.pdf?sequence=1&isAllowed=y. Acesso em: 21 maio 2019.

FRUMENTO, Enrico. **Social Engineering: an IT Security problem doomed to get worse**. [*S. l.*], 24 jul. 2018. Disponível em: https://medium.com/our-insights/social-engineering-an-it-security-problem-doomed-to-get-worst-c9429ccf3330. Acesso em: 09 setembro 2019.

HONG**,** Jason. The state of phishing attacks. **Communications of the acm**. 2012.

KHER, Tejasvini; KARIYA, Swati. A Survey on Social Engineering: Techniques and Countermeasures. **International journal of Scientific Research and Development**. 2016.

KUMAR, Anshul; CHAUDHARY, Mansi; NAGRESH, Nagresh. Social Engineering Threats and Awareness: A Survey. **European Journal of Advances in Engineering and Technology**, www.ejaet.com, 2015.

MANN, I. **Engenharia social: série prevenção de fraudes.** São Paulo: Blucher, 2011.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar:** ataques de hackers – controlando o fator humano na segurança da Informação. São Paulo: Makron, 2003.

MOUTON, Francois; LEENEN, Louise; VENTER, H.s. Social engineering attack examples, templates and scenarios. **Computers & Security**. 2016.

PROOF. **Spear Phishing: uma das ameaças mais efetivas**. [*S. l.*]. Disponível em: https://www.proof.com.br/blog/spear-phishing/. Acesso em: 28 maio 2019.

RAFAEL, Gustavo de Castro. **Engenharia Social: as técnicas de ataques mais utilizadas**. [*S. l.*], 24 out. 2013. Disponível em: https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/. Acesso em: 21 maio 2019.

SOCIAL-ENGINEER. **2017 verizon DBIR Social Engineering Breakdown.** Disponível em: https://www.social-engineer.com/2017-verizon-dbir-social-engineering-breakdown/. Acesso em: 20 maio. 2019 às 16h15min.

THOMAS, T. **Segurança de redes: primeiros paços.** Rio de janeiro: Ciência moderna, 2007.

UNICAMP. **Ataques de phishing**. [*S. l.*], 22 ago. 2012. Disponível em: https://www.sg.unicamp.br/help-desk/knowledgebase.php?article=5&rated=1. Acesso em: 21 maio 2019.