ISSN: 2675-1828

ARTIGO

Impactos da Engenharia Social na Segurança da Informação

Impacts of Social Engineering on Information Security

Lucas Avanci de Souza Pereira[1]
Augusto Luciano Vicentine[2]
Andre Castro Rizo[3]

Resumo: *Atualmente existem diversos tipos de métodos de se obter dados, que podem ser de pessoas, equipamentos ou até mesmo empresas. Esses dados podem ser utilizados de diferentes modos, podendo variar de uma simples sugestão de compra para um cliente, até a exploração de vulnerabilidades de sistemas para obtenção de dados sigilosos de uma organização. Um dos métodos mais preocupantes para a segurança da informação, é o que chamam de engenharia social, pois não necessitam de conhecimento técnico e sim de poder de persuasão para conseguir informações importantes das próprias pessoas ou simplesmente uma pesquisa em redes sociais e lá obter dados, que para a pessoa, podem significar nada, mas para um atacante, pode ser o início da descoberta de uma vulnerabilidade. Esse artigo aborda os problemas que a engenharia social causa na segurança pessoal e empresarial, como podem ser tratados esses problemas e o que pode ser feito para mitigar os problemas causados por esses vazamentos de dados.*

Palavras-Chave: *atacante; dados; impacto; vazamento; vulnerabilidade.*

Abstract. *Currently, there are several types of methods of obtaining data, which can be from people, equipment or even companies. This data can be used in different ways, ranging from a simple purchase suggestion to a customer, to the exploitation of system vulnerabilities to obtain sensitive data from an organization. One of the most worrying methods for information security is what is called social engineering. It does not require technical knowledge, but rather persuasion to get important information from the people or simply a search on social networks and obtain data. To the person, the data may mean nothing, but to an attacker, it could be the beginning of discovering a vulnerability. This article addresses the issues that social engineering causes for personal and business security, how these issues can be addressed, and what can be done to mitigate the issues caused by these data leak.*

Keywords: *attacker; data; impact; leak; vulnerability.*

1. Introdução

Com a expansão de novos recursos tecnológicos, houve uma amplificação na troca de informações, possibilitando o crescimento de diversos pontos positivos na rotina das

[1] Faculdade de Tecnologia de Araraquara. E-mail: lucas.pereira94@fatec.sp.gov.br
[2] Faculdade de Tecnologia de Araraquara. E-mail: augusto.vicentine@fatec.sp.gov.br
[3] Faculdade de Tecnologia de Araraquara. E-mail: andre.rizo@fatec.sp.gov.br

pessoas, seja por sua eficiência, facilidade de utilização, produção e, claramente, comunicação.

Porém, junto a esta evolução, portas foram abertas para crimes digitais com o intuito de roubar informações, afetando a segurança dos usuários. Uma vez que há este risco, a preocupação de como as informações são manipuladas entre os usuários em uma rede, torna necessário tomada de medidas que visam a segurança da informação (COELHO;RASMA;MORALES, 2013).

De fato, a própria tecnologia é fundamental e extremamente eficiente para fornecer uma ótima segurança em uma rede de computadores, porém não garante totalmente sua proteção. Assim, possibilita a afirmação de que uma rede ou sistema não é totalmente seguro, mas é possível reduzir esses riscos por meio da segurança da informação (COELHO;RASMA;MORALES, 2013).

Com base em artigos e trabalhos acadêmicos, o presente trabalho está proposto em apresentar uma pesquisa teórica voltada à Engenharia Social e seus impactos que podem comprometer a segurança da informação, assim buscando também a contribuição para suas medidas preventivas.

2. Segurança da Informação

Com a evolução da tecnologia, o armazenamento e a movimentação de informações aumentaram de grande forma, tornando a SI (Segurança da Informação), a maior preocupação das organizações, pois são o alvo mais alvejado dos criminosos. A SI se define basicamente como meios de proteger a informação, através de normas, políticas, procedimentos e boas práticas.

Na SI, apresentam-se 4 princípios ou pilares. A confidencialidade, que garante que a informação é acessível somente por pessoas autorizadas. A integridade, garantindo que a informação não seja alterada indevidamente. A disponibilidade, que garante que os dados estão seguros e disponíveis para acesso. Por fim, a autenticidade, como a documentação de quando uma informação é manipulada por algum usuário de maneira autêntica (SOLUTIONS, 2022).

As informações necessitam de uma classificação para que seja definido o nível de segurança que tem de ser aplicado. Este tipo de classificação é feito através da função da informação na organização, seu custo, impacto em operação e seus riscos referentes a vazamento. E, uma vez que este levantamento é feito, é possível economizar recursos para garantir segurança para as informações sensíveis, o que reduz desperdício de recursos com informações públicas (KIM; SOLOMON, 2014).

Machado (2017) aponta que há quatro níveis de classificação, sendo elas: informações públicas, internas, confidenciais e restritas.

a) Informações públicas são aquelas que podem ser compartilhada com todos, pois não haverá impacto negativo, fazendo-se possível não atribuir um nível de segurança alto.

b) Internas são de competência interna de uma organização, restringindo o acesso externo a ela e, uma vez que ocorra o vazamento e venha a conhecimento público, não ocorre grandes prejuízos.

c) Confidenciais se classificam pelo fato de que sua exposição ao público que não seja da organização, pode impactar em prejuízos financeiros, de imagem, competitividade etc.

d) Restritas são caracterizadas por ter um valor tão alto que se algum membro da própria organização, que não deveria ter o acesso, acessar aquela informação, pode causar sérios danos ao negócio. Sendo assim, este tipo de informação deve ser protegida tanto de maneira interna como externa.

Obtendo o entendimento desses pontos, fica claro que toda informação, seja interna, confidencial ou restrita, precisa estar segura, sendo acessada somente por pessoas autorizadas conforme necessidade, mantendo sua autenticidade, para que não ocorram tais prejuízos às organizações.

3. Ameaças e Vulnerabilidades

Mesmo empresas que aderem a novas tecnologias de segurança para dificultar a exploração de vulnerabilidades, seus novos meios de proteção podem também abrir portas para novas ameaças. Nakamura (2007) aponta importantes preocupações que devem receber atenção: novas tecnologias acarretam novas vulnerabilidades; aumento de conexões abrangem novos caminhos para invasores, ataques direcionados e oportunistas; necessidade maior de conhecimento para defesa; amplificação de crimes digitais.

As ameaças são meios que dão origem a um ataque ou violação em sistemas, podendo ser de forma intencional, em que o usuário tem a intenção de prejudicar a organização; acidental, que geralmente ocorrem por descuido ou falta de informação; passivo, que não reflete impacto no negócio quando ocorrido; e por fim, ativas, que são a manipulação da informação, gerando conteúdo não válido.

Também há dois outros tipos de classificação para ameaças, sendo as internas

> "Internas: geralmente os responsáveis por danos causados internamente são funcionários insatisfeitos, que querem prejudicar o desenvolvimento do trabalho ou tirar vantagens financeiras. Outros responsáveis são prestadores de serviços e funcionários terceirizados. Como exemplo de ameaças internas destacam-se o roubo de informações, a alteração ou destruição de informações, os danos físicos a hardware e alteração de configurações e danos lógicos à rede." (GABBAY, 2003, p. 24)

E as externas, "ameaças externas são aquelas causadas por indivíduos que não pertencem a organização e/ou que estão efetuando ataques remotamente. Seus objetivos variam desde indisponibilizar serviços ou máquinas até a roubar informações sigilosas." (GABBAY, 2003, p. 24)

Uma vez que uma análise de ameaças sobre os ativos da empresa é feita, é possível identificar quais são suas vulnerabilidades, sendo assim, possibilitando o trabalho para suas correções. Santos e Soares (2019) apontam a importância desta ação, pois a

> "Vulnerabilidade é uma falha ou fraqueza de um bem, ativo ou processo, que, caso seja explorada por uma ameaça, irá causar algum impacto na organização, podendo ser considerada como a suscetibilidade do sistema ou ativo em relação à determinada ameaça."

Ameaças e vulnerabilidades aumentam em paralelo com a evolução da tecnologia, o que tornam indispensáveis as análises preventivas e corretivas, junto de planos de ação em uma empresa.

4. Fator Humano na Segurança da Informação

A utilização do meio tecnologico permite que a SI fique mais robusta, pois hoje existem recursos excelentes em questão de hardware e software, utilizados na proteção de dados e informações, porém, o invasor tem a ciência desses recursos e parte para o alvo mais vulnerável, o humano.

Apesar da SI ser formada pelas características apontadas anteriormente, não haverá eficiência se o fator humano não estiver preparado.

Lyra (2015, p. 47) reforça a importância desse fator, indicando que

> "A cooperação dos usuários é essencial para a eficácia da segurança. Eles exercem um forte impacto sobre a confidencialidade, a integridade e a disponibilidade da informação, pois, por exemplo, o usuário que não mantiver a confidencialidade da senha, não evitar o registro da mesma em papéis que não estão guardados em locais seguros, não utilizar senhas de qualidade ou ainda que compartilhe senhas individuais, compromete a segurança da informação."

Ainda assim, o ser humano é destacado por ceder informações com facilidade, devido a sua necessidade natural de (CORRÊA, 2006):

- Se sentir útil aos outros;
- Buscar novas amizades: é costume ser agradável receber elogios, e com isso a vítima fica mais vulneravel;
- Ganhar lucro facilmente;
- Conquistar confiança;

Gaspar (2015) completa essas características e afirma:

> "Estas fragilidades exploram a utilização de variados elementos sociais e humanos para intrusão nos sistemas, roubo de informação relevante ou para afetar a sua reputação ou produtividade das empresas. Estes ataques acabam por ser feitos por pessoas de dentro, podendo ainda ser divididos em ataques voluntários ou involuntários. São voluntários quando a pessoa tem plena consciência do ataque e involuntários quando sem se aperceber estão a lesar a empresa/organização onde estão inseridos."

Uma organização lida com diversos tipos de pessoas, o que para algumas é explicito o entendimento da importância da informação como para outras não. Sendo assim, o treinamento e a conscientização são primordiais, o que deve ser frequente e cultural nas empresas.

5. Engenharia Social

Uma vez que esses pontos são de conhecimento de pessoas mau intencionadas, métodos diferenciados de cometer crimes de roubo de informações são elaborados e utilizados para a exploração dessas fraquezas.

Para este tipo de exploração, se utiliza a Engenharia Social que, segundo Berti e Rogers (2004), abrange:

> "As tentativas bem-sucedidas ou fracassadas para influenciar uma pessoa a revelar qualquer informação ou agir de uma forma que possa resultar em acesso não autorizado, uso não autorizado de, ou divulgação não autorizada de um sistema de informação, de uma rede ou de dados."

De acordo com Mitnick e Simon (2002), um engenheiro social, de forma geral, é um indivíduo que através da manipulação, conquista a confiança de sua vítima para ter acesso a informações privadas. Sendo assim, as informações que a vítima fornece podem ser utilizadas para lhe causar prejuízo de diversas formas, como financeiro, psicológico, social e empresarial (CORTELA, 2013).

Segundo Araújo (2005), "geralmente o engenheiro social é um tipo de pessoa agradável. Ou seja, uma pessoa educada, simpática, carismática. Mas, sobretudo criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente".

De acordo com Zager (2002), existem quatro tipos de engenheiros sociais e cada tipo é caracterizado por determinado objetivo, sendo:

- **Casual**: composto com um grupo grande, motivado ao ataque por curiosidade e o desafio de invadir sistemas;
- **Político**: tomam ação por uma causa, utilizando suas habilidades com o intuito de divulgar esta causa ou prejudicar entes que representam o oposto de sua causa;
- **Criminoso**: elaborado por profissionais no crime;
- **Interno**: este é caracterizado por serem funcionários ou terceiros de uma organização, são os mais perigosos devido ao seu acesso padrão a informações da empresa.

Como mencionado anteriormente, este tipo de ataque vem se tornando comum devido a evolução da tecnologia. Segundo Lafrance (2004), os objetivos dos engenheiros sociais com esses ataques são principalmente:

- **Lucro financeiro**: motivo mais almejado pelo atacante;
- **Interesse proprio**: para fins exploratórios sem más intenções, porém podendo provocar danos;
- **Pelo desafio**: o invasor tem como objetivo testar suas capacidades ou provar algo, sem más intenções;
- **Vantagem competitiva**: obter informações para ganhar vantagem competitiva;
- **Pressão**: o proprio engenheiro social se sente pressionado a ponto de tentar exibir suas habilidades para chamar a atenção de algum grupo com o intuito de ser chamado para participar do mesmo, ou também para pressão de manter sua reputação.
- **Mitigar danos**: objetiva em ajudar as pessoas ou organizações, com o intuito de corrigir suas vulnerabilidades;

- **Política**: o atacante atua com o objetivo de dar vantagem a uma causa.

Geralmente as vítimas desse tipo de prática são usuários que não entendem o valor da informação da organização, então tendem a ceder com mais facilidade.

Nos últimos tempos, os atacantes têm tido muito sucesso ao executar este tipo de ação, o que acarretou o aumento contínuo deste tipo de ataque. A utilização de equipamentos eletrônicos e redes sociais, acompanhados do mau uso e falta de conhecimento, por parte das vítimas, agregam para o sucesso do engenheiro social. Em virtude disto, as empresas devem dar a devida atenção ao fator humano relacionado a segurança da informação, assim tendo funcionários bem treinados, resultando em uma empresa mais segura e consciente.

6. Estrutura do ataque de engenharia social

Os ataques de origem da engenharia social vêm ganhando espaço devido a dificuldade de mitigar este tipo de crime. Estes ataques, conforme apontado por Alves (2010), são divididos em dois grupos, direto e indireto.

Os ataques diretos ocorrem quando há o contato direto com a vítima, seja por ligação ou pessoalmente. Neste grupo é preciso que o engenheiro social faça o planejamento de como executar o ataque, pois o ataque de forma direta é o que exige mais contato com o alvo, onde o menor dos erros pode comprometer o plano.

Os ataques indiretos são caracterizados por utilizar outros meios para chegar ao seu objetivo, isso através de softwares ou ferramentas, por exemplo, virus, sites falsos, cavalos de troia ou por e-mails falsos (*phishing*). Sendo assim, através desses meios o atacante pode obter as informações que deseja.

Quando um engenheiro social utiliza o ataque de forma indireta, ele fica de certa forma mais seguro, pois como informado anteriormente, não há o contato direto com sua vítima e pode ser distribuído pela internet de forma com que atinja vários alvos. “Este método é bastante utilizado pelos engenheiros sociais, primeiro criam os sites e depois utilizam as redes sociais para fazerem a divulgação dos mesmos” (GASPAR, 2015).

Figura 1 - Estrutura do modelo de ataque de engenharia social

Fonte: GASPAR (2015)

Além do entendimento sobre tipos de ataques, também é necessário conhecer a estrutura do ataque utilizado pela engenharia social. Definido por Oosterloo (2008), essa estrutura é distribuida em quatro fases sendo elas: Preparação, Manipulação, Exploração e Execução. Essa estrutura está ilustrada conforme Figura 1.

Não é uma regra seguir esses passos um por vez, o engenheiro social pode repetir um passo quantas vezes for necessário até que ele obtenha o resultado da fase concluido, a partir daí seguir para as próximas fases. Para Gaspar (2015), os termos de cada fase se caracterizam:

- **Preparação**: consiste no pré-envolvimento do alvo, mais conhecido como *footprint*. Nesta fase é necessário recolher o máximo de informações possíveis sobre o alvo, como: negócio da organização, nome de funcionários, suas funções, telefones, e-mails e processos internos. Também, quais atributos (físicos) para seguir para a próxima fase.
- **Manipulação**: o engenheiro social utiliza suas técnicas e meios para conquistar a confiança do alvo e criar um ambiente credível. A manipulação pode ser de várias formas, como fisicamente, interação direta, ou por meios de comunicação indireta, sendo por telefones ou e-mails, tudo com o intuito de reunir e organizar informações.
- **Exploração**: após a confiança e influência que foram consquitadas na fase anterior, essas são utilizadas para adquirir informações mais afundo sobre o alvo, como nome dos servidores, aplicações, IPs, manuais, entre outras.
- **Execução**: nesta fase é realizado o ataque a partir de todas as informações obtidas nas fases anteriores. Definem-se as ações que devem ser tomadas para chegar ao objetivo final. O engenheiro social irá utilizar das suas habilidades técnicas, que demonstram sua perícia.

Para colocar em prática essas fases, é necessário utilizar táticas adequadas para cada situação. Gaspar (2015) aponta algumas delas:

- **Reconhecimento/Estudo**: Utilizada para se preparar, o atacante estuda o alvo, observando, frequentando os mesmos locais, ouve conversas e até mesmo segue sua vítima.
- **Pesquisa Web**: Recolhe informações através de informações que estão de forma pública na internet, principalmente por sites como: redes sociais, fóruns, sites de emprego, entre outros.
- **Vasculhar lixo**: Refere-se à análise do lixo que foi descartado pela organização, assim verificando se tem alguma informação útil que foi descartada de maneira incorreta.
- ***Phishing***: Normalmente utilizado por meio de correio eletrônico, telefone ou mensagens, onde o engenheiro se passa por outra pessoa de confiança, assim a vítima pode passar informações ou acessar *links* maliciosos.
- **Software malicioso**: São softwares que são encaminhados para as vítimas, através de e-mails (*phishing*) ou pendrives, que são instalados de forma com que o alvo não tenha seu conhecimento, assim o engenheiro social consegue extrair informações. Esses softwares geralmente possuem formatos como: vírus, *trojan*, *keylogger*.

Como mencionado anteriormente, os engenheiros sociais, seguindo estes padrões, obtêm bastante sucesso em seus ataques, o que se faz o motivo para a utilização destes meios serem os mais utilizados para roubo de informações. Assim, uma vez que é de conhecimento das pessoas e das organizações quais as vulnerabilidades do fator humano, é possível tomar medidas para mitigar os riscos que a engenharia social traz.

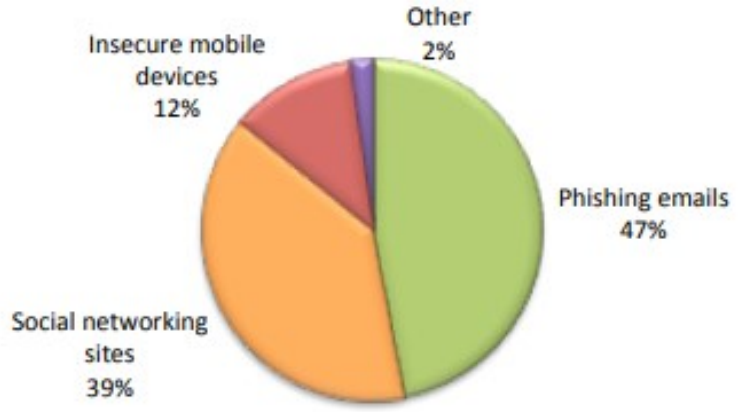
7. Discussões

Após feitos os levantamentos apontados nas sessões anteriores, é observado que as falhas humanas tornam este tipo de ataque (Enganharia Social) mais difícil de se controlar, diferente de equipamentos e softwares que são programaveis, mas que também podem ser afetados por consequência de falha humana.

Devido a este ponto, há muito tempo essa prática tem ocorrido de forma frequente e de forma gradativa. Um exemplo que mostra isso é uma pesquisa que foi feita em 2011, entre julho e agosto, pela *Check Point Software Technologies*, que aponta que quase a metade (48%) das organizações já sofreu algum tipo de ataque de engenharia social e que tiveram prejuízo financeiro com isso.

A Figura 2 ilustra também quais foram os métodos de engenharia social mais utilizados, sendo: 47% *phishing*, 39% publicações maliciosas em redes sociais, 12% em dispositivos moveis inseguros e 2% outros.

Figura 2 - Ameaças mais comuns



Fonte: RESEARCH (2011)

Essa pesquisa da *Check Point* constou 853 participantes da área de Tecnologia da Informações de diversos países: Estados Unidos, Reino Unido, Canadá, Austrália, Nova Zelândia e Alemanha.

Poucos anos após, foi mostrado um crescimento significativo desses dados a partir de um relatório da Symantec (2014), demonstrando:

- De 2012 para 2013, dados violados aumentaram em 62%;
- Identidade expostas aumentaram em 493%, com 552 milhões de vítimas;
- 1 a cada 196 e-mails possuem *malware*;
- 1 a cada 392 e-mails eram *phishing*;

De fato a engenharia social gera muitos impactos. Alguns dos principais são:

- Venda de informação sensível;
- Espionagem;
- Crescimento na distribuição de *malware* para obter informações e acessos indevidos;
- Exposição de privacidade;
- Vazamento de informações, afetando as pessoas, organizações e governo.

É extremamente crítico o fator humano quando se trata de segurança da informação e cada vez mais é explorado por pessoas má intencionadas. “Os ataques informáticos estão cada vez mais sofisticados, o lado humano é considerado como o elo mais fraco e as consequências dos ataques são cada vez maiores e abrangentes” (GASPAR, 2015).

8. Considerações finais

Visto que o ser humano é um ser passível de erros, a engenharia social sempre será uma ferramenta que irá possibilitar a exploração de uma das maiores vulnerabilidades possíveis, que é a do ser humano agir de forma emocional e acabar vazando informações importantes para que seja realizado um ataque.

Qualquer pessoa está vulnerável a cair em diferentes tipos de golpes, que visam o roubo de dados pessoais ou organizacionais, que podem ocorrer até mesmo por meio de uma conversa telefônica, sem a utilização de nenhum conhecimento técnico para a obtenção de dados.

Logo, uma empresa sempre será vulnerável a sofrer um ataque, mesmo que ocorra um alto investimento em seus equipamentos e softwares, para se obter um ambiente seguro. Utilizando-se da engenharia social, um hacker ainda conseguirá se aproveitar de um colaborador que, mesmo sem querer, irá fornecer informações importantes que irão ser utilizadas para realizar um ataque.

Assim, se faz necessário utilizar de métodos que proporcionam a mitigação desses ataques, sendo um deles o que deveria ser uma regra para qualquer organização: políticas de segurança. Essas políticas devem apresentar, de maneira clara, a importância da informação junto com suas orientações para preservá-las. Além disso, é importante manter as mesmas atualizadas e de conhecimento de todos, assim tendo uma organização alinhada com as políticas de segurança da empresa. Outros métodos são a utilização de cursos e palestras, visando o treinamento e conscientização dos colaboradores, seguindo a mesma linha das políticas de segurança, só que mostrando como e quais medidas devem ser tomadas nas devidas situações.

Referências Bibliográficas

ARAÚJO, Eduardo E. **A Vulnerabilidade Humana na Segurança da Informação**, 2005. 85f. Licenciatura Sistemas de Informação, Faculdade de Ciências Aplicadas de Minas, Uberlândia.

ALVES, Cássio B. **Segurança da Informação vs. engenharia Social**: como se proteger para não ser mais uma vítima. 2. ed. Brasília: Clube de Autores, 2010.

COELHO, Cristiano F.; RASMA, Eline T.; MORALES, Gudelia. **Engenharia Social**: uma ameaça à sociedade da informação. Exatas & Engenharias. Campos dos Goytacazes, v. 3, n. 5, 44p, 2013. ISSN 2236-885X. Disponível em: <https://ojs3.perspectivasonline.com.br/exatas_e_engenharia/article/view/87/59>. Acesso em: 22/05/2022. DOI: https://doi.org/10.25242/885X305201387.

CORRÊA, Ney C. C. **O uso indevido da Engenharia Social na Informática**, 2006. 61f. Licenciatura em Sistemas de Informação, Centro Universitário do Maranhão, São Luis.

CORTELA, João J. C. **Engenharia Social Aplicada ao Facebook**, 2013. 22f. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) Universidade Estadual de Londrina, Londrina.

GABBAY, Max S. **Fatores influenciadores da implementação de ações de Gestão de Segurança da Informação**: um estudo com Executivos e Gerentes de Tecnologia da Informação em empresas do Rio Grande do Norte, 2003. 153f. Dissertação (Mestrado em Engenharia de Produção) Universidade Federal do Rio Grande do Norte, Natal.

GASPAR, Jana E. H. M. **Análise comportamental sobre ataques de engenharia social**, 2015, 77f. Mestrado em Engenharia Informática. Escola Superior de Tecnologia e Gestão.

BERTI, John; ROGERS, Marcus. Social Engineering: The Forgotten Risk. In: TIPTON, Harold F; KRAUSE, Harold F. **Information Security Management Handbook**. 4. ed. New York: Auerbach, 2004, p. 51-53, v. 3.

KIM, David; SOLOMON, Michael G. **Fundamentos de segurança de sistemas da informação**. 1. ed. São Paulo: Grupo Editorial Nacional, 2014. v. 1.

LAFRANCE, Yves. **Psychology:** A Precious Security Tool. SANS Institute, p. 27, 2004.

LYRA, Mauricio R. **Governança da Segurança da Informação**. 1. ed. Brasília, 2015.

NAKAMURA, Emilio T.; GEUS, Paulo L. **Segurança de Redes em ambientes cooperativos**. 1. ed. São Paulo: Novatec Editora, 2007.

MACHADO, Marcel J. **Níveis de Classificação da Informação**. Segurança da Informação, 2017. Disponível em: <https://marceljm.com/seguranca-da-informacao/niveis-de-classificacao-da-informacao/#:~:text=Geralmente%20a%20informa%C3%A7%C3%A3o%20%C3%A9%20classificada,com%20a%20necessidade%20do%20neg%C3%B3cio>. Acesso em: 01/04/2022.

MITNICK, Kevin; SIMON, William. **Mitnick**: A arte de enganar. 1. ed. Brasil: Pearson Education, 2002.

OOSTERLOO, Bernard. **Managing Social Engineering Risk**: Making social engineering transparent, 2008, 130f. Master Industrial Engineering and Management, University of Twente, Enschede, Netherlands.

RESEARCH, Dimensional. **The risk of social engineering on information security**: a survey of it professionals, 2011. Disponível em: <https://www.pressetext.com/nfs/166/633/pdf/2.pdf>. Acesso em: 29/04/2022.

SANTOS, Eduardo E.; SOARES, Tamires M. M. K. **Riscos, ameaças e vulnerabilidades**: o impacto da segurança da informação nas organizações. Revista Tecnológica da Fatec Americana. Americana, v. 7, n. 2, p. 43-51, 2019. ISSN 2446-7049. Disponível em: <http://ric.cps.sp.gov.br/handle/123456789/4383>. Acesso em: 01/04/2022.

SOLUTIONS, Add I. C. **Pilares da Segurança da Informação**, 2022. Disponível em:< https://addit.com.br/pilares-da-seguranca-da-informacao/>. Acesso em: 28/04/2022.

SYMANTEC. **Internet Security Threat Report**, 2014. Disponível em: < https://docs.broadcom.com/doc/istr-main-report-v19-en>. Acesso em: 29/04/2022.

ZAGER, Masha. **Who are the hackers?** Infosec News, 2002. Disponível em: < https://seclists.org/isn/2002/Sep/78>. Acesso em: 25/03/2022.