INTERFACE TECNOLÓGICA

ENGENHARIA SOCIAL E A IMPORTÂNCIA DA CIBERSEGURANÇA NA ATUALIDADE

SOCIAL ENGINEERING AND THE IMPORTANCE OF CYBERSECURITY TODAY

Diego Augusto Aparecido Falla – diegofalla2015@hotmail.com
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

Giuliano Scombatti Pinto – giuliano.pinto@fatectq.edu.br
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

DOI: 10.31510/infa.v20i2.1759
Data de submissão: 06/09/2023
Data do aceite: 16/11/2023
Data da publicação: 20/12/2023

RESUMO

Atualmente, a informação pode ser considerada como um dos maiores bens das organizações empresariais, assim como do público em geral, e, por este motivo, é mais visada e cobiçada por pessoas más intencionadas que têm como objetivo usufruir destas informações por meios não legais. Por este motivo existe uma grande necessidade de protegê-la. Este projeto tem como objetivo conscientizar pessoas de todas as faixas etárias e organizações sobre boas práticas e atitudes que devem ser tomadas em relação aos seus dados na internet, identificando os tipos de ataques e como reduzir as chances de ocorrência dos mesmos, bem como mostrar como identificar determinado ataque por meio de técnicas de engenharia social. A realização deste estudo baseou-se em pesquisas bibliográficas. Os resultados apontaram que a proteção de informações é uma preocupação crucial nos dias de hoje, dado o valor que os dados possuem tanto para organizações empresariais quanto para o público em geral. A crescente sofisticação dos ataques cibernéticos, juntamente com a proliferação de ameaças online, torna evidente a necessidade premente de conscientizar as pessoas de todas as faixas etárias e organizações sobre a importância de salvaguardar suas informações.

Palavras-chave: engenharia social, cibersegurança, prevenção de ataques, segurança da informação.

ABSTRACT

Currently, information can be considered one of the greatest assets of business organizations, as well as the general public, and, for this reason, it is more targeted and coveted by people with bad intentions who aim to take advantage of this information through non-legal means. For this reason there is a great need to protect it. This project aims to raise awareness among people of all age groups and organizations about good practices and attitudes that should be taken in relation to their data on the internet, identifying the types of attacks and how to reduce the chances of them occurring, as well as showing how identify a specific attack through social engineering techniques. This study was based on bibliographical research. The

results showed that information protection is a crucial concern nowadays, given the value that data has for both business organizations and the general public. The increasing sophistication of cyber attacks, along with the proliferation of online threats, makes clear the pressing need to raise awareness among people of all age groups and organizations about the importance of safeguarding their information.

Keywords: social engineering, cybersecurity, attack prevention, information security.

1 INTRODUÇÃO

Atualmente, a informação pode ser considerada como um dos maiores ativos de uma empresa, assim como do público em geral. Exatamente por esse motivo, ela se torna um dos maiores alvos de pessoas mal-intencionadas que têm como objetivo roubar essas informações. Seja por fins lucrativos, curiosidade ou até mesmo por diversão, devido a esses motivos, as pessoas devem cada vez mais estar atentas e preocupadas com a segurança das suas informações. Isso é válido tanto em ambientes corporativos como em nos lares. Se uma informação valiosa cair em posse de um cracker ou hacker, isso pode acarretar em diversos problemas pessoais ou até levar uma empresa com anos de mercado à falência.

O termo "engenharia social" (ou "*social engineering*" em inglês) refere-se à arte de manipular pessoas com o intuito de obter informações que possam ser utilizadas em diferentes estilos de ataques. Isso pode ocorrer através de uma ligação telefônica, troca de mensagens ou até mesmo em uma simples conversa. Segundo Mitnick e Simon (1963) e Mann (2011), a engenharia social envolve métodos para influenciar ou persuadir pessoas a fornecer informações sigilosas de uma organização ou informações pessoais.

Atualmente, existem diversos mecanismos de proteção, como antivírus, intranet, firewalls, tokens, sistemas de autenticação, entre outros. Embora essas tecnologias desempenhem um papel importante no cotidiano, ainda não são suficientes para garantir a segurança total dos dados.

Excluído: ,

Sendo assim, diariamente várias empresas e indivíduos se tornam vítimas de golpes elaborados por engenheiros sociais. Por esse motivo, este trabalho tem como objetivo abordar e apresentar algumas técnicas de engenharia social. A intenção é que o público em geral conheça situações reais do cotidiano e também compreenda métodos de prevenção utilizando a cibersegurança, a fim de evitar esses tipos de ataques.

O presente artigo será iniciado com a explanação do conceito de engenharia social, assim como o de cibersegurança. Além disso, será realizada uma análise detalhada de alguns

tipos de ataques que podem ser utilizados para obter informações. Por fim, serão apresentadas maneiras de prevenir esses ataques, seja por meio do uso da tecnologia ou sem o uso dela.

2 ENGENHARIA SOCIAL

A engenharia social pode ser definida como um conjunto de métodos e técnicas que tem como objetivo obter determinadas informações. Essas técnicas envolvem enganação, manipulação, investigação e até mesmo abordagens psicológicas, com o intuito de obter informações desejadas. Para realizar isso, o engenheiro social assume outra identidade, adaptando-se e se passando por outra pessoa. Ele pode estabelecer contato com parentes ou amigos da vítima, visando obter informações sigilosas (PARODI, 2008; HINTZBERGEN et al., 2018).

Na engenharia social, o ser humano é o elemento fundamental para o sucesso das técnicas utilizadas. Isso ocorre porque os indivíduos são frequentemente considerados o "elo fraco" na segurança de uma empresa ou na preservação da confidencialidade de informações pessoais. Por esse motivo, os ataques de engenharia social vêm crescendo exponencialmente no Brasil, conforme apontado por Mann (2011).

De acordo com Henriques (2016), a engenharia social envolve a exploração do senso comum das pessoas para obter informações valiosas de uma organização. Essas informações podem incluir senhas, logins, endereços de e-mail e detalhes organizacionais. Tudo isso é alcançado através de abordagens direcionadas a funcionários que possam estar despreparados para lidar com essas situações específicas.

2.1 Meios e técnicas utilizados

Os ataques de engenharia social abrangem uma variedade de canais, incluindo e-mails, chamadas telefônicas e plataformas de redes sociais.

Segundo Azzolin (2017) dentro desses ataques, diversas técnicas são empregadas, tais como observar atentamente, investigar o ambiente de trabalho, assumir identidades alheias por meio da impersonação, empregar técnicas persuasivas e conduzir conversas aparentemente despretensiosas.

Frequentemente, as estratégias de engenharia social se combinam com outras técnicas, como o trashing (revirar o lixo) e a Captura de Informações Livres. A fusão dessas abordagens pode resultar em problemas substanciais para as instituições visadas, uma vez que

informações obtidas por diferentes vias se entrelaçam, gerando dados mais substanciais e relevantes.

Independentemente do meio ou da técnica utilizada, os engenheiros sociais exploram algumas das principais características humanas, tais como reciprocidade, consistência, busca por aprovação social, simpatia, autoridade e medo. Isso é corroborado por Nakamura e Geus (2007). Além disso, conforme ressalta Assunção (2011, p.150), "os engenheiros sociais utilizam os sentimentos para manipulação e os casos mais comuns são: curiosidade, confiança, simpatia, culpa e medo"

2.1.1 Email

Conforme aponta Azzolin (2017), o correio eletrônico (e-mail) constitui uma das ferramentas mais utilizadas por engenheiros sociais, principalmente devido à sua ampla abrangência. As técnicas aplicadas para ataques por e-mail também podem ser extrapoladas para outros meios, como mensagens em dispositivos móveis, plataformas de mídia social e até correspondência física.

Uma tática frequentemente empregada é o envio de e-mails com remetente falso, na qual o engenheiro social recorre a programas capazes de gerar mensagens com endereços de remetentes genuínos. Esse estratagema ilude a vítima, fazendo-a acreditar que recebe uma mensagem de uma fonte confiável.

Outra abordagem é o e-mail manipulativo, no qual a mensagem é elaborada para explorar a curiosidade ou ganância do alvo. Geralmente, o conteúdo da mensagem aborda temas como "Você ganhou 10 mil reais" ou "Fotos comprometedoras vazadas". A pessoa destinatária é levada a interagir com anexos, links ou fornecer informações a fim de reivindicar o suposto prêmio, tornando-se assim mais uma vítima desse tipo de ataque.

2.1.2 Redes sociais

De acordo com as observações de Cavalcanti (2011), os sites de redes sociais, que têm como principal objetivo facilitar o relacionamento entre pessoas por meio da Internet, apresentam uma dualidade notável. Por um lado, essas plataformas oferecem uma maneira conveniente de fazer amizades, manter contatos e conhecer novas pessoas. No entanto, por outro lado, representam uma considerável ameaça à privacidade de seus usuários, uma vez que abrigam e expõem uma ampla gama de informações pessoais e profissionais. Essas

informações incluem detalhes sobre o ciclo de amizades, fotografias, locais frequentados, endereços residenciais, números de contato, cargos e empregos atuais, além de informações sobre familiares. Isso aumenta substancialmente o nível de visibilidade dos usuários na Internet, tornando-os mais suscetíveis a ataques de engenharia social e outras ameaças à segurança cibernética.

Essas redes sociais podem ser exploradas para a realização de ataques semelhantes aos realizados por e-mails, envolvendo trocas de mensagens manipulativas que levam a vítima a fornecer as informações desejadas. Além disso, essas plataformas também podem ser usadas para coletar informações de maneira mais sutil, explorando os perfis dos usuários em busca de detalhes como endereços, nomes, parentescos, profissões, locais de trabalho, endereços de e-mail e números de telefone das vítimas.

Além disso, criar um perfil falso em redes sociais populares, como o Facebook ou o WhatsApp, é uma tarefa relativamente simples. Apenas algumas fotos são suficientes para criar um perfil e adicionar pessoas à lista de contatos. Assim, um engenheiro social pode facilmente assumir a identidade de um conhecido ou parente e solicitar informações que normalmente só seriam compartilhadas com pessoas de confiança (AZZOLIN 2017).

2.1.3 Telefones

O telefone representa uma ferramenta frequentemente empregada pelos engenheiros sociais. Com apenas algumas informações, esses especialistas conseguem iniciar um diálogo que, por meio da manipulação das emoções da vítima, a levará a compartilhar as informações desejadas. Embora não seja uma técnica simples, pois exige habilidade e raciocínio astuto por parte do engenheiro, quando executada com sucesso, pode gerar consequências significativas para uma organização, tudo isso sem acarretar grandes riscos ou despesas para o autor do ataque (MAULAIS, 2016).

2.1.4 Ataques presenciais

Um exemplo clássico de ataque de engenharia social envolve o engenheiro social fazendo-se passar por um indivíduo de alto cargo que enfrenta questões urgentes relacionadas ao acesso ao sistema. Nesse cenário, o hacker atua como um ator que interpreta um papel específico para atacar o elo mais fraco da segurança de uma organização: os seres humanos.

Nesse tipo de abordagem, o atacante pode assumir várias identidades, como um colega conhecido, parente de um usuário, fornecedor ou qualquer outro papel que pareça legítimo. Isso lhe permite obter acesso a determinado local ou adquirir informações sobre a organização ou os indivíduos envolvidos (MAULAIS, 2016). A partir desse ponto, o engenheiro social pode explorar o ambiente e outras vulnerabilidades, potencialmente comprometendo a segurança da organização.

2.1.5 Exploração do Ambiente

Explorar o interior de uma organização é muitas vezes a única maneira de adquirir informações que não estão disponíveis nos meios digitais, como, por exemplo, informações sensíveis sobre planos de ação. Além disso, ao investigar o ambiente físico, é possível obter outras informações valiosas, como senhas, logins e documentos que podem estar expostos em mesas de trabalho ou armazenados nos computadores. Esse tipo de abordagem permite ao atacante obter dados que podem não ser acessíveis por meios virtuais, aumentando assim o potencial de comprometimento da segurança (AZZOLIN 2017).

2.2 Medidas preventivas

As medidas preventivas descritas nesta seção abrangem os conjuntos de recomendações numerados de 1 a 5, visam prevenir os ataques de engenharia social direcionados a usuários finais e empresas e serão apresentadas pelos Quadros numerados de 1 a 5.

QUADRO 1 – Ataques por e-mail

TÉCNICA	MEDIDA PREVENTIVA
E-MAIL FALSO OU MANIPULATIVO	Mantenha sempre uma atitude de desconfiança em relação a mensagens provenientes de instituições financeiras, propostas que pareçam muito vantajosas, anúncios de prêmios irresistíveis e conteúdos que afirmam ter "fotos comprometedoras".
	Evite fornecer informações sigilosas, mesmo para usuários de confiança
	Mensagens de conhecidos nem sempre são confiáveis (o campo de remetente do e-mail pode ter sido falsificado, ou podem ter sido enviadas de contas falsas ou invadidas. (CERT.BR, 2017).
	Utilizar exclusivamente o correio eletrônico corporativo para troca de mensagens relativas ao serviço. (DCT, 2011).
	Não clicar em links ou abrir arquivos recebidos por e-mail, a menos que se tenha absoluta certeza da origem e integridade do mesmo. Ter em mente que um arquivo enviado por uma pessoa de confiança pode não ter sido realmente enviado por ela. (DCT, 2011).
	Não utilizar a conta de correio corporativo funcional em cadastros de sítios na Internet. Se necessário, manter uma conta em provedor público (Gmail, Yahoo, Hotmail, etc) para esta finalidade.

Fonte: AZZOLIN (2017).

QUADRO 2 – Ataques por telefone

TÉCNICA	MEDIDA PREVENTIVA
Coleta de informações	Os atendes devem evitar se identificar de imediato ao atender a ligação
Persuasão	Sempre confirmar a veracidade de informações recebidas
	Evite fornecer ou confirmar informações que não se relacionem com as suas responsabilidades dentro da organização ou quando você não tem certeza sobre a identidade da pessoa do outro lado da linha.

Fonte: AZZOLIN (2017).

QUADRO 3 – Redes Sociais

TÉCNICA	MEDIDA PREVENTIVA
Coleta de informações livres	Manter suas contas com configurações de privacidade mais restritas possíveis (evitar a configuração pública).
	Evitar expor informações pessoais como telefone, e-mail, endereço e até mesmo as relações familiares existentes com outros usuários
	Desconfiar de perfis desconhecidos que solicitam permissão para se tornar "amigo" nas redes sociais.
Persuasão	Evitar diálogos com perfis desconhecidos que exponham informações pessoais ou relacionadas com o trabalho em "chats" das diversas redes sociais existentes.
	Desconfie também de perfis de conhecidos solicitando informações (contas podem ser falsificadas facilmente).

Fonte: AZZOLIN (2017).

QUADRO 4 – Ataques físicos

TÉCNICA	MEDIDA PREVENTIVA
Vasculhamento das Instalações	Nunca deixar documentos sigilosos sobre as mesas ou de fácil acesso, assim como senha e login expostos.
	O controle de entrada e saída de pessoas pela guarda deve ser criterioso.
Instalações	Indivíduos externos à empresa devem sempre estar acompanhados por um membro da equipe ou representante da empresa.
	Evite digitar senhas na presença de outras pessoas
Persuasão	Não forneça informações a recém conhecidos.
Acesso a máquinas/sistemas	Senhas e login de usuários não devem estar expostas.
	Evitar deixar senhas e login salvos nos navegadores, pois as senhas podem ser facilmente obtidas com recursos básicos de informática.
	Executar rigoroso controle das máquinas e dos usuários que podem ter acesso à rede de computadores da OM. Não permitir que máquinas de visitantes sejam conectadas à rede local. (DCT, 2011).
	Não possua senhas "universais" (iguais para todos os sistemas).
	Manter o sigilo das senhas utilizadas nos sistemas computacionais. As senhas são pessoais, não podendo, portanto, ser compartilhadas. (DCT, 2011).
	Os cadastros de usuários que acessam os sistemas devem ser mantidos atualizados e supervisionados pela contrainteligência da OM. (DCT, 2011).
	Estabelecer uma política clara e supervisionada relativa ao descredenciamento de usuários que tenham sido transferidos de OM ou de função. (DCT, 2011).
Vasculhamento do lixo	Não jogue fora documentos com informações sigilosas. Separe e elimine de forma eficiente.

Fonte: AZZOLIN (2017).

É essencial estabelecer em cada organização medidas que restrinjam a circulação interna de funcionários nas áreas administrativas. Acreditar automaticamente na segurança total do ambiente de trabalho é um equívoco frequentemente cometido por possíveis alvos. Qualquer incidente suspeito ou ataque deve ser imediatamente comunicado ao departamento responsável, a fim de que sejam tomadas as devidas providências, informando os membros da equipe e pessoal de serviço, visando prevenir possíveis futuros ataques.

3 PROCEDIMENTOS METODOLÓGICOS

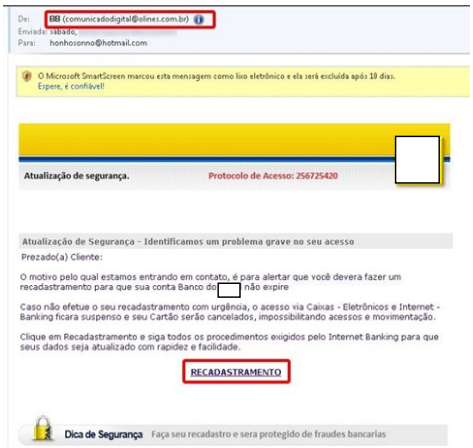
A metodologia utilizada no presente artigo foi a pesquisa bibliográfica realizada em livros, artigos e sites. Como em qualquer pesquisa direcionada ao meio acadêmico, a realização de um trabalho bem sucedido também depende de uma ampla investigação. Mesmo quando existem poucas fontes disponíveis sobre o tópico em análise, uma pesquisa não começa do zero. Nesse sentido, a pesquisa bibliográfica teve o foco no entendimento do conceito de Engenharia Social, o qual delimitou o escopo da pesquisa e conferiu fundamentação acadêmica, garantindo confiabilidade e veracidade às informações e fatos abordados. De acordo com Gil (2006), a pesquisa bibliográfica consiste na utilização de materiais previamente existentes, permitindo ao pesquisador explorar o histórico passado e os aspectos contemporâneos do campo de estudo.

4 RESULTADOS E DISCUSSÃO

A figura abaixo exemplifica uma prática enganosa por e-mail (*phishing*) geralmente retrata um cenário em que um remetente malicioso envia uma mensagem eletrônica falsa, aparentando ser de uma fonte confiável. Nessa imagem, é comum ver elementos como logotipos de empresas legítimas, textos persuasivos e links aparentemente autênticos. Entretanto, se examinado atentamente, a figura também pode revelar indícios de falsificação, como erros gramaticais, endereços de e-mail suspeitos ou URLs que direcionam para sites fraudulentos. Essa representação visual destaca a importância de manter a vigilância ao lidar com e-mails, verificando sua autenticidade antes de interagir com seu conteúdo ou fornecer informações pessoais, a fim de evitar ser vítima de fraudes online.

INTERFACE TECNOLÓGICA

Figura 1 – Exemplo de ataque por e-mail



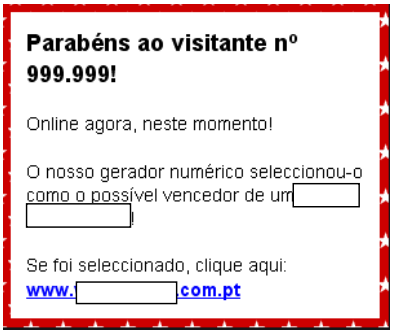
Fonte: https://www.dinamio.com.br/blog/2020/12/07/tipos-de-ataques-de-enganacao-e-como-se-prevenir/

A análise da Figura 1 revela uma falha de segurança substancial, destacada pelo endereço de e-mail utilizado ("@olines.com.br"), o qual contrasta com o padrão empregado por instituições financeiras, essa discrepância levanta suspeitas quanto à legitimidade do e-mail, uma vez que instituições financeiras não costumam se comunicar com seus clientes através de tais endereços. A situação se agrava devido ao fato de que esse tipo de e-mail suspeito é distribuído para um amplo público, incluindo indivíduos que possivelmente não possuam vínculo com a instituição.

Adicionalmente, vale salientar que as práticas seguras das instituições financeiras desaconselham fortemente a solicitação de informações sensíveis através de e-mails. A orientação é respaldada pela Federação Brasileira de Bancos (FEBRABAN), a qual ressalta que bancos não costumam enviar mensagens não solicitadas contendo anexos para serem instalados ou links para serem abertos. A FEBRABAN também enfatiza a importância de verificar a procedência de um link enviado por e-mail, confiando somente em remetentes reconhecidos. Em caso de dúvida, a recomendação é contatar diretamente o gerente da conta ou a Central de Atendimento do banco, conforme as diretrizes estabelecidas pelo órgão

regulador. Essas medidas visam mitigar o risco de cair em armadilhas de *phishing* e proteger os clientes contra tentativas de fraude.

Figura 2 – Exemplo de "Baiting Attacks"



Fonte: https://www.dinamio.com.br/blog/2020/12/07/tipos-de-ataques-de-enganacao-e-como-se-prevenir/

Conforme apresentado na figura 2, é exemplificado uma prática de ataques de "*baiting*" em um contexto de pesquisa cibernética frequentemente ilustra um cenário onde um atacante habilidoso, por meio de artifícios enganosos, oferece um estímulo atrativo, como um arquivo ou link aparentemente benigno, com o objetivo de induzir a vítima a uma interação indesejada. A figura pode incorporar elementos como mensagens persuasivas, promessas de recompensas ou informações exclusivas, todos projetados para despertar a curiosidade ou a ganância do alvo. No entanto, subjacente a essas iscas, residem armadilhas virtuais, tais como malware, *spyware* ou outras formas de código malicioso, cujo propósito é comprometer a integridade do sistema do usuário. Essa representação visual destaca a complexidade e a astúcia inerentes aos ataques de "*baiting*", bem como a necessidade premente de medidas preventivas e de conscientização para combater esse tipo de ameaça na paisagem cibernética contemporânea.

A prevenção e detecção eficazes de ataques de "*baiting*" são essenciais para garantir a segurança no cenário digital. Para prevenir esses ataques, é crucial que os usuários adotem uma abordagem cautelosa ao lidar com mensagens e conteúdos online. Isso envolve a

verificação cuidadosa da autenticidade das fontes, especialmente ao receber mensagens não solicitadas de remetentes desconhecidos. Evitar clicar em links suspeitos ou fazer o download de anexos de origens não verificadas é fundamental.

Além disso, é recomendável manter todas as aplicações e sistemas operacionais atualizados com as últimas correções de segurança, bem como a utilização de software antivírus e firewalls confiáveis. Educar os usuários sobre práticas seguras de navegação na internet e conscientizá-los sobre os perigos associados aos "*baiting*" também desempenha um papel vital na prevenção.

Para a detecção precoce de ataques de "*baiting*", a vigilância contínua é essencial. Observar cuidadosamente os sinais de alerta, como mensagens com erros de gramática, solicitações incomuns ou conteúdo fora de contexto, pode ajudar a identificar tentativas de engano. Além disso, a implementação de soluções de segurança que usem análise de comportamento e aprendizado de máquina pode auxiliar na identificação de anomalias e na detecção proativa desses ataques. Em última análise, uma abordagem multifacetada que combina conscientização, educação e tecnologia é fundamental para fortalecer a defesa contra os ataques de "*baiting*" no ambiente digital.

5 CONCLUSÃO

A engenharia social emerge como um dos principais desafios enfrentados pelos profissionais de Segurança da Informação. Para uma gestão eficaz da segurança, é imperativo que os responsáveis possuam um profundo entendimento das práticas de segurança, mantenham-se atualizados quanto às mudanças tecnológicas e táticas de ataque, e estejam equipados com a capacidade de identificar os sinais de um engenheiro social mal-intencionado.

No entanto, para garantir a proteção das organizações contra esses ataques, a implementação de políticas e procedimentos se faz essencial. Essas diretrizes devem definir claramente os papéis e responsabilidades de todos os usuários, indo além dos profissionais de segurança e abrangendo todos os níveis da organização. Embora as soluções técnicas, como aquelas baseadas em software e hardware, estejam significativamente avançadas, por si só, não são suficientes no âmbito da Segurança da Informação. Isso ocorre porque a engenharia social direciona seus ataques ao ponto mais vulnerável: os indivíduos.

Por fim, é crucial que as organizações adotem uma abordagem que fortaleça sua postura de segurança, incorporando não apenas as medidas técnicas, mas também uma perspectiva centrada nas pessoas. A conscientização e a educação dos usuários, juntamente com a implementação de políticas claras, são fundamentais para mitigar o risco associado aos ataques de engenharia social, reconhecendo o aspecto humano como uma peça crucial na complexa matriz da segurança de informações.

REFERÊNCIAS

ASSUNÇÃO, M. F. A. **Segredos do Hacker Ético**. 4. ed. Florianópolis: Visual Books, 2011

AZZOLIN, M. M. **Ataques de Engenharia Social**: Medidas Preventivas para a segurança da informação, **Revista O Comunicante**, v. 7 n.3 (2017), p. 56-64, 2017. Disponível em: http://www.ebrevistas.eb.mil.br/OC/article/view/1674. Acesso em: 27 ago. 2023.

BRASIL. Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações. 1. Ed. 09f. [S.I.]: Departamento de Ciência e Tecnologia, 2011

CAVALCANTI J. **Engenharia social nas redes sociais**. 2011. 48 f. Monografia (Especialização em Desenvolvimento de Sistemas para Web) – Departamento de Informática, Universidade Estadual de Maringá, Maringá, 2011.

CORTELA, J J C. **Engenharia Social Aplicada ao Facebook**. 2013. Trabalho de conclusão de curso (Graduação em Ciência da Computação) – Universidade Estadual de Londrina, Londrina, 2013.

FEBRABAN. **Federação Brasileira de Bancos**. Disponível em: https://portal.febraban.org.br/paginas/81/pt-br/. Acesso em: 27 mar. 2023

FONSECA, M. **Engenharia Social**: conscientizando o elo mais fraco da segurança da informação. 2017. Trabalho de conclusão de curso (Pós-Graduação em Especialização em Inteligência em Segurança Pública) - Universidade do Sul de Santa Catarina, Brasília, 2017.

FONSECA, P F. **Gestão de Segurança da Informação**: O Fator Humano. 16f. Artigo Científco. Curitiba: Pontifícia Universidade Católica do Paraná, 2009
BRASIL. Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações. 1. Ed. 09f. [S.I.]: Departamento de Ciência e Tecnologia, 2011.

GIL, A C. **Métodos e técnicas de pesquisa social**. São Paulo: Editora Atlas 2006

HINTZBERGEN, J.; SMULDERS, A.; HINTZBERGEN, K.; BAARS, H. **Fundamentos de Segurança da Informação**: com base na iso 27001 e na iso 27002. Tradução: Alan de Sá. Rio de Janeiro: Brasport, 2018.

HENRIQUES, F A F. **A influência da Engenharia Social no fator humano das organizações**. 2016. Dissertação (Pós-Graduação em Ciência da Computação) – Universidade Federal de Pernambuco, Recife, 2016

MANN, I. **Hacking the human**: social engineering techniques and security countermeasures. Aldershot, England ; Burlington, VT: Gower, 2008. ISBN 978-0-566- 08773-8.

MAULAIS, C N S**. Engenharia Social**: técnicas e estratégias de defesa em ambientes virtuais vulneráveis. 2016. Projeto de Pesquisa (Mestrado em Sistema de Informação e Gestão de Conhecimento) – Universidade Fumec, Belo Horizonte, 2016.

MITNICK, K D.; SIMON, W L. **A arte de enganar**: ataques de hackers: controlando o fator humano na segurança da informação. Tradução: Kátia Aparecida Roque. São Paulo: Pearson Education, 2003.

NAKAMURA, E T; DE GEUS, Paulo Licio. **Segurança de redes em ambientes cooperativos**. 1. ed. São Paulo: Novatec, 2007.

PARODI, L. **Manual das fraudes**. Rio de Janeiro: Brasport, 2008.