ENGENHARIA SOCIAL

O QUE É E COMO EVITAR ESSES ATAQUES NAS EMPRESAS

Bianca Roziska Rosa
Fatec Assis
broziska@gmail.com

Gabriel Terciotti Malimpensa
Fatec Assis
gabrielterciotti@gmail.com

Fabio Eder Cardoso
Fatec Assis
fabioeder.professor@gmail.com

RESUMO

Engenharia social é a manipulação psicológica usada por criminosos cibernéticos para obter informações e prejudicar sistemas e pessoas. Com o avanço tecnológico, essas técnicas se tornaram mais sofisticadas, afetando muitos. O trabalho busca soluções para proteção contra esses ataques, destacando a importância da segurança da informação. Define tipos de ataques, mapeia riscos, descreve medidas de proteção e cria material educativo. Mesmo com investimentos em segurança, a dimensão humana é frequentemente negligenciada, causando prejuízos. Estudos mostram que profissionais de TI já enfrentaram ataques de engenharia social, destacando a necessidade de ações para mitigar riscos. Empresas investem em segurança, mas a conscientização e preparação contra-ataques de engenharia social são essenciais. A prevenção requer educação e conscientização das pessoas envolvidas.

Palavras-chave: Golpe. Ataques. Engenharia Social. Phishing.

ABSTRACT

Social engineering is the psychological manipulation used by cybercriminals to obtain information and harm systems and individuals. With technological advancement, these techniques have become more sophisticated, affecting many. The work seeks solutions for protection against these attacks, emphasizing the importance of information security. It defines types of attacks, maps risks, describes protective measures, and creates educational materials. Even with investments in security, the human dimension is often overlooked, causing damages. Studies show that IT professionals have already faced social engineering attacks, emphasizing the need for actions to mitigate risks. Companies invest in security, but awareness and preparedness against social engineering attacks are essential. Prevention requires education and awareness of the people involved.

Keywords: Scam. Attacks. Social Engineering. Phishing.

1. INTRODUÇÃO

A engenharia social é uma técnica de manipulação psicológica utilizada por criminosos cibernéticos para obter informações, invadir sistemas ou computadores, aplicar golpes, colocando em risco informações de empresas e pessoas físicas. Com o avanço da tecnologia, as técnicas de engenharia social também evoluíram, tornando-se cada vez mais sofisticadas e difíceis de detectar, que acarretam o maior número de pessoas atingidas (BIAZZOTTO, ANTICOLI e BOCCIA, 2020).

O avanço da tecnologia de *hardware* e infraestrutura de computadores, juntamente ao crescimento da demanda de *softwares* com as mais variadas finalidades e aplicações, acaba por levar a sociedade a um nível muito alto de dependência dessas tecnologias, pois sua utilização acaba gerando muitos benefícios. Com o amplo aumento da utilização da tecnologia, há também o aumento do número e das formas de ameaça às informações que trafegam nas redes de computadores, bem como aos usuários que delas se utilizam, sendo esse o problema de pesquisa a se propor soluções. Dessa forma, se torna cada vez mais evidente e necessário que se dedique atenção especial às formas e mecanismos que vise a segurança da informação e a prevenção de dados. (MARCIANO; MARQUES, 2006).

Este trabalho tem como objetivo geral apresentar os principais mecanismos e formas de se evitar ataques de engenharia social em empresas. Como objetivos específicos, busca-se definir os principais tipos de ataques mais comuns relacionados à engenharia social, mapear os principais riscos dos ataques e definir as principais formas de proteção contra os referidos ataques.

Cada vez mais, empresas do mundo todo estão buscando por novos investimentos em segurança, implementando camadas de segurança que vão desde o acesso aos seus softwares por outros sistemas até sua infraestrutura de redes e servidores para que nenhuma informação possa ser acessada ou captada indevidamente. Mesmo assim, um elo muito especial ainda é esquecido pela grande parte das empresas, o fator humano. Estudos apontam que dentre um grupo de 850 profissionais de TI entrevistados, 48% alegaram já terem sofrido algum tipo de ataque de engenharia social acarretando prejuízos às empresas afetadas. Diante de um número tão alarmante, torna-se necessário que sejam conhecidas e implementadas ações que visem mitigar esses prejuízos (ROSA, 2012).

2. REVISÃO BIBLIOGRÁFICA

Segundo Mitnick (2003), o fator humano é o elo mais frágil de uma organização, pois ela pode ter gasto muito dinheiro com as tecnologias mais avançadas, porém as pessoas continuam sendo vulneráveis.

> "Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis." – (MITNICK, 2003, p15)

Mitnick (2003) afirma que a habilidade social é um atributo importante para a maioria dos engenheiros sociais bem-sucedidos, que são capazes de estabelecer afinidade e confiança com facilidade. Esses indivíduos são charmosos e educados, utilizam estratégias e táticas para obter acesso a informações-alvo valiosas. Com isso, um engenheiro social experiente pode obter praticamente qualquer informação desejada.

2.1 PRINCIPAIS TIPOS DE ATAQUE DE ENGENHARIA SOCIAL

Os ataques de engenharia social são uma ameaça crescente no mundo da cibersegurança. Nesses ataques, os criminosos exploram a vulnerabilidade humana, em vez de explorar falhas técnicas. Usando técnicas de manipulação psicológica, como a persuasão e o engano, os atacantes conseguem obter informações confidenciais, como senhas e informações pessoais, de suas vítimas.

2.1.1. PHISHING

Phishing é uma técnica que se utiliza de métodos fraudulentos, tais como e-mails falsos, sites clonados, mensagens em redes sociais ou SMS, para obter informações sensíveis de forma ilegal. É evidente que esta prática acarreta um significativo risco à segurança da informação. (PIOVESAN, SILVA, SOUZA e TURIBUS, 2019)

Os indivíduos que empregam o método de *Phishing* estão cada vez mais aprimorando suas habilidades, aumentando assim as chances de êxito em seus ataques. Eles podem elaborar

textos no corpo de e-mails de maneira tão convincente que até mesmo profissionais da área ficam indecisos em afirmar se o e-mail é falso ou não. Além disso, podem direcionar um ataque diretamente a uma empresa ou pessoa física, o que é conhecido como ataque direcionado. Nesses casos, um Engenheiro Social pode ter sido contratado para executar o golpe e utilizará todas as suas ferramentas para obter sucesso. Esses são os tipos mais difíceis de ataques de *Phishing* para se defender, pois as informações contidas neles serão bem selecionadas e o mais verossímil possível. Tais e-mails podem ainda conter *malwares*, o que auxilia no roubo de informações. (PIOVESAN, SILVA, SOUZA e TURIBUS, 2019)

2.1.2. SPEAR PHISHING

Segundo Tieso (2020), o *Spear Phishing* é uma categoria distinta do *Phishing*, mas representa uma ameaça ainda mais perigosa. Esse tipo de ataque cibernético é altamente direcionado, concentrando-se em empresas e organizações específicas. Embora siga um padrão semelhante ao *Phishing*, o *Spear Phishing* é ainda mais sofisticado em suas abordagens, pois é personalizado para a vítima selecionada. Isso o torna um ataque altamente elaborado e personalizado.

2.1.3. VISHING

Parecido com o *phishing*, nesse ataque são empregados recursos de áudio, frequentemente acompanhados de mensagens de texto via SMS, que informam à vítima que seu cartão foi bloqueado e que ela precisa ligar para um número específico para solicitar a liberação. Os criminosos se aproveitam da tecnologia VoIP (*Voice over Internet Protocol*), que permite ocultar a identidade do autor da chamada com facilidade. (TIESO, 2020)

2.1.4. PRETEXTING

Os hackers frequentemente utilizam o *Pretexting* como método de ataque cibernético, que consiste em criar uma falsa situação para enganar a vítima e obter acesso às informações do sistema. Eles se passam por alguém com posição hierárquica superior à vítima e a intimidam para conseguir as informações desejadas. Para escolher a persona a ser assumida, os criminosos costumam recorrer às redes sociais, onde coletam informações importantes sobre a vítima, como local de trabalho, função, familiares e amigos. Com essas informações em mãos, eles podem enviar e-mails se passando por alguém conhecido pela vítima e solicitar o que desejam, muitas vezes sem que a vítima perceba que se trata de um golpe cibernético e ceda as informações desejadas. (TIESO, 2020)

2.1.5. TAILGATING

Segundo Leite (2019) o *Tailgating* trata-se de uma técnica antiga e ainda utilizada, inclusive em prédios residenciais, na qual o invasor segue de perto um funcionário até uma área controlada eletronicamente. Quando o funcionário abre a porta, o invasor se aproveita da situação, alegando estar atrasado ou utilizando algum objeto para impedir que a porta se feche sem chamar a atenção para sua presença.

2.1.6. BAITING

Um exemplo comum de *Baiting* é o uso de dispositivos USB, CDs, DVDs e cartões de memória infectados, deixados de propósito em locais públicos, como banheiros ou estacionamentos, na esperança de que alguém os encontre e os conecte em seu computador pessoal ou no computador da empresa. Ao fazer isso, a pessoa pode inadvertidamente instalar um malware ou um programa espião no sistema, permitindo que o invasor acesse informações confidenciais ou controle o computador remotamente. (LEITE, 2019).

3. METODOLOGIA

O presente trabalho realizou uma pesquisa bibliográfica a respeito do tema “Engenharia Social” com o objetivo de identificar os principais tipos de ataques à dados e pessoas relacionadas a esse contexto, além de seus riscos e consequências.

A pesquisa bibliográfica é um importante meio de se obter informações a respeito de um determinado assunto pesquisado. Segundo Lakatos e Marconi (1991, p.113), a pesquisa bibliográfica busca trazer esclarecimentos a respeito de um determinado problema ou tema por meio de referências teóricas já publicadas a respeito do tema independentemente do veículo de comunicação utilizado por tal publicação, dentre eles, revistas, livros, jornais e artigos.

Realização uma pesquisa de campo com 88 pessoas, por meio de formulário, contendo 20 perguntas pessoais sobre o comportamento delas no meio digital e profissional. Podendo assim chegar dados estatísticos sobre a segurança da informação nessa amostra.

4. RESULTADOS

4.1 ANÁLISE DOS DADOS COLETADOS

Após a realização da pesquisa de campo pode-se identificar que um dos fatores de risco de ataques está ligado com a forma com que usuários e organizações fazem a gestão de suas senhas de acesso, uma vez que 28,4% dos entrevistados compartilham as senhas utilizadas com outros funcionários para acessar informações da empresa; 21,6% alegaram que utilizam senhas pessoais iguais as senhas utilizadas no trabalho e 34,1% utilizam a mesma senha para todas as contas.

Outra observação importante que pode ser constatada com a aplicação do questionário, foi o crescente número de ataques disparados aos usuários. Como resultado obteve-se que 71,6% dos entrevistados alegaram já ter recebido mensagens de sorteios ou links suspeitos de remetentes desconhecidos e 51,1% do total de respostas afirmam terem recebido mensagens de pessoas se passando por algum conhecido solicitando dinheiro ou tentando aplicar golpes semelhantes.

Um aspecto importante a ser considerado está relacionado ao comportamento do usuário diante de situações de exposição a situações de risco à segurança da informação pois 43,2% dos entrevistados já baixaram algum arquivo por acidente ou por impulso, 21,6% costumam clicar em anúncios de promoção recebidos e 12,5% dos entrevistados alegam que clicam em qualquer botão nos sites.

A crescente obtenção de informações estratégicas de determinadas áreas e determinadas organizações tem ganhado espaço no universo da engenharia social. Isso se deu devido à grande exposição de informações referente às atividades profissionais desenvolvidas já que 65,9% dos entrevistados informaram que falam sobre o trabalho fora do local de trabalho, 61,4% afirmam já terem postado fotos em redes sociais com colegas de trabalho, 55,7% responderam que possuem a empresa e o cargo que ocupam em informados em redes sociais e 53,4% já postaram foto do seu local de trabalho.

Os dados coletados e analisados nos parágrafos acima foram obtidos através da análise da pesquisa realizada, cujas questões aplicadas e os percentuais de cada resposta obtida podem ser observadas abaixo.

Tabela 1 - Perguntas e porcentagem das respostas

Perguntas	% sim	% não
A senha que você utiliza no seu local de trabalho para acessar as informações da empresa, você compartilha com outros funcionários?	28,4	71,6
Suas senhas pessoais são iguais às que você utiliza no trabalho?	21,6	78,4
Você utiliza a mesma senha para todas as contas?	34,1	65,9
Você costuma receber ligações ou mensagens de remetentes desconhecidos? Com links ou sorteios suspeitos?	71,6	28,4
Você já recebeu mensagens de pessoas se passando por algum conhecido para aplicar golpes?	51,1	48,9
Você já baixou algum arquivo acidentalmente ou por impulso?	43,2	56,8
Você é do tipo que clica em qualquer botão nos sites?	12,5	87,5
Você costuma ser prestativo com as pessoas no local de trabalho? (Que não sejam os outros funcionarios)	85,2	14,8
Seu local de trabalho tem algum controle de acesso? (Segurança, porteiro, digital para entrar, crachás, etc)	68,2	31,8
Você fala sobre o trabalho fora do local de trabalho?	65,9	34,1
Você é uma pessoa facil de fazer amizade?	62,5	37,5
Você já passou telefone de outras pessoas para algum desconhecido que simplesmente pediu?	28,4	71,6
Nas suas redes sociais você possui a empresa e o cargo que você atua?	55,7	44,3
Você já postou foto do seu local de trabalho?	53,4	46,6
Você já respondeu aqueles Quiz, que fazem várias perguntas sobre você?	35,2	64,8
Você costuma clicar ao receber anuncios de promoções?	21,6	78,4
Você já caiu em algum golpe relacionado as midias digitais?	20,5	79,5
Você se sente capaz de orientar as pessoas sobre possíveis golpes ou anuncios e informações suspeitas?	80,7	19,3
Se sim a pergunta anterior, você clica já clicou em algum link?	20,5	79,5
Você ja postou fotos com colegas de trabalho?	61,4	38,6

Com base na pesquisa exploratória aplicada e demonstrada acima, pode-se orientar sobre algumas formas de evitar que as pessoas sejam vítimas desses ataques.

4.2 FORMAS DE EVITAR ATAQUES DE ENGENHARIA SOCIAL

Evitar ataques de engenharia social requer vigilância, conscientização e a implementação de medidas de segurança adequadas. Aqui estão algumas práticas e dicas para evitar ser vítima de ataques de engenharia social. Leite (2019, p.32) descreve algumas maneiras das pessoas ficarem atentas:

- Ficar atento aos links que vão ser acessados.
- Desconfiar de e-mails com origens estranhas ou até mesmo as origens conhecidas como bancos.
- Examinar os anexos nos e-mails sempre que receber, verificando a extensão do arquivo.
- Pensar nas informações que fornece em redes sociais (elas são públicas).
- Ao conversar com pessoas desconhecidas, não forneça muitas informações.

- Conscientização: Esteja ciente de que os ataques de engenharia social podem ocorrer em várias formas, incluindo e-mails falsos, telefonemas, mensagens de texto, redes sociais e até mesmo encontros pessoais. Desconfie de qualquer situação que pareça suspeita.
- Verificação de identidade: Sempre verifique a identidade da pessoa ou entidade que está solicitando informações confidenciais ou ação de sua parte. Ligue para números oficiais ou visite sites diretamente, em vez de seguir links ou números fornecidos em mensagens suspeitas.
- Proteção de informações pessoais: Não compartilhe informações pessoais, como senhas, números de cartão de crédito ou dados de identificação com estranhos ou em resposta a mensagens não solicitadas.
- Treinamento em conscientização: Receba treinamento em conscientização em segurança cibernética, se disponível, para aprender a reconhecer sinais de engenharia social e como responder adequadamente a eles.
- Políticas de segurança: As empresas devem implementar políticas de segurança cibernética que incluam diretrizes para lidar com solicitações de informações confidenciais e ações que exijam autenticação.
- Autenticação de dois fatores (2FA): Ative a autenticação de dois fatores sempre que possível. Isso adiciona uma camada extra de segurança, mesmo se um atacante obtiver suas credenciais.
- Senhas fortes: Use senhas fortes e exclusivas para cada conta. Isso reduz o risco de que uma única senha comprometida possa ser usada para acessar várias contas.
- Monitoramento e detecção: Esteja atento a atividades incomuns em suas contas e sistemas. Use ferramentas de monitoramento e detecção de ameaças, se disponíveis.
- Confirmação de solicitações: Sempre confirme solicitações de transferência de dinheiro, divulgação de informações sensíveis ou outras ações financeiras ou de segurança diretamente com a pessoa ou entidade apropriada antes de agir.
- Relate tentativas suspeitas: Se você receber uma mensagem ou abordagem suspeita, denuncie-a à sua equipe de segurança cibernética ou ao departamento de TI. Relatar tentativas de engenharia social ajuda a alertar outros e a tomar medidas preventivas.

5. CONSIDERAÇÕES FINAIS

A engenharia social é uma técnica utilizada por indivíduos mal-intencionados para manipular pessoas e obter informações confidenciais ou realizar atividades prejudiciais. Nesta

pesquisa, comprovou-se que o fator mais vulnerável nas organizações são as pessoas, visto que, elas fornecem os dados conscientemente ou inconscientemente.

Além disso, a constatação de que pelo menos 71% das pessoas já receberam mensagens suspeitas, indicando tentativas de ataques do tipo *phishing*, enfatiza a urgência de conscientização e educação em segurança cibernética. Para mitigar esses riscos, é crucial promover a conscientização sobre boas práticas de segurança da informação tanto entre indivíduos quanto no ambiente corporativo, a fim de proteger dados sensíveis e evitar possíveis consequências negativas para a privacidade e a integridade das informações.

A educação em segurança cibernética não deve ser encarada como um luxo, mas sim como uma necessidade crítica. A prevenção de ataques de engenharia social é uma responsabilidade compartilhada entre indivíduos, empresas e instituições. Ao adotar medidas proativas, como o treinamento e a conscientização em segurança, pode-se proteger os dados sensíveis e evitar consequências negativas para a privacidade e a integridade das informações. É um esforço contínuo e colaborativo para manter a segurança no mundo digital em constante evolução.

6. REFERÊNCIAS

BIAZZOTTO, Fabricio; ANTICOLI, Frederico Azevedo; BOCCIA, Gustavo Vilela. **Uso de tecnologias para minimizar ataques de engenharia social em ambientes corporativos**. 2020. Trabalho de conclusão de curso (Curso Superior de Tecnologia em Segurança da Informação) - Fatec São Caetano do Sul – Antonio Russo, São Caetano do Sul, 2020.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica.** 3. ed, p.113-116. São Paulo: Atlas, 1991.

LEITE, Iago Piccoli., & Coin Pereira, F. (2019). **Engenharia Social: Não seja mais uma Vítima**. PROJETOS E RELATÓRIOS DE ESTÁGIOS, 1(1), 1-30. Recuperado de http://raam.alcidesmaya.edu.br/index.php/projetos/article/view/59.

MARCIANO, J. L.; MARQUES, M. L. **O Enfoque Social da Segurança da Informação**. Revista Ciência da Informação, Brasília, v.35, n. 3, p. 89-98, set./dez. 2006.

MITNICK, Kevin D.; SIMON, William L.; **A arte de enganar**; Tradução: Kátia Aparecida Roque; revisão técnica: Olavo José Anchieschi Gomes. 2003.

PIOVESAN, Leonardo Gubert; SILVA, Edilmárcio Reis Costa; SOUSA, Jakson Ferreira de; TURIBUS, Sérgio Noleto. **ENGENHARIA SOCIAL: Uma abordagem sobre Phishing**. Volume 10, p 45-59. 2019. Revista Científica da Faculdade de Balsas.

RAMOS, Rosejheinny Farias. **Um estudo sobre as boas práticas de engenharia social e a percepção das pessoas sobre o seu conceito**. 2019. 163 f. Trabalho de conclusão de curso de graduação (Bacharelado em Sistemas de Informações) - Universidade Federal do Amazonas, Itacoatiara-AM, 2019.

ROSA, A. C. M. **ENGENHARIA SOCIAL: O ELO MAIS FRÁGIL DA SEGURANÇA NAS EMPRESAS**. Revista Brasileira de Contabilidade e Gestão, [S. l.], v. 1, n. 2, p. 29-40, 2012. Disponível em: https://www.revistas.udesc.br/index.php/reavi/article/view/2840. Acesso em: 20 abr. 2023.

TIESO, I. H. de S.; ESPIRITO SANTO, F. do. **ATAQUES DE ENGENHARIA SOCIAL**. Revista Interface Tecnológica, [S. l.], v. 17, n. 2, p. 206–218, 2020. DOI: 10.31510/infa.v17i2.947. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/947. Acesso em: 16 abr. 2023.