Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i4.25345

ENGENHARIA SOCIAL - AS TÁTICAS QUE EXPLORAM NOSSAS FRAQUEZAS

Maria Regina Lopes Leal[1]

RESUMO: A engenharia social representa uma das mais difundidas causas de incidentes de segurança cibernética, é um tipo de manipulação que envolve técnicas que se baseiam na psicologia humana para enganar indivíduos e obter informações sensíveis. Alguns tipos comuns desta técnica incluem *phishing* (envio de e-mails ou mensagens fraudulentas), *vishing* (tentativas de fraude por meio de chamadas telefônicas), *smishing* (uso de mensagens de texto – SMS com links maliciosos), *pretexting* (criação de uma identidade falsa ou cenário para obter informações de alguém), *baiting* (oferecimento de um item atrativo para enganar a vítima), dentre outros. Em crescente disseminação, quando usadas para manipulação negativa, têm causado prejuízos financeiros e riscos à segurança de empresas e indivíduos. Os impactos podem ser graves, resultando em perdas financeiras, roubo de identidade, danos à reputação e compromissos legais. Como um fundamento em comum, todas elas se aproveitam de gatilhos emocionais, confiança e vulnerabilidades humanas, muitas vezes utilizando meios digitais, físicos ou combinações de ambos. Mecanismos de defesa e prevenção que podem ser aplicados são a conscientização e a educação, reforçando a importância de práticas seguras e verificações criteriosas de forma contínua. Implementação de medidas de segurança, treinamento de usuários para reconhecimento de fraudes e criação de uma cultura organizacional voltada à proteção são essenciais para mitigar os riscos desses ataques manipulativos. O combate às investidas maliciosas das técnicas engenharia social requer integração de pessoas, processos e tecnologia, em um esforço conjunto e, sobretudo, frequente.

Palavras-chave: Confiança. Educação. Fraude. Manipulação. Phishing. Psicologia. Segurança.

INTRODUÇÃO

A engenharia social é uma técnica insidiosa que explora a vulnerabilidade humana em vez de depender de brechas tecnológicas. Em um mundo onde a tecnologia desempenha um papel central em nossas vidas diárias, essa forma de manipulação se tornou uma das maiores ameaças à segurança da informação. Em vez de invadir sistemas por meio de códigos maliciosos ou *exploits*, que são comandos que se aproveitam de uma falha ou de alguma vulnerabilidade em um aplicativo ou sistema para causar a ocorrência de comportamentos não intencionais ou não antecipados, os engenheiros sociais utilizam a persuasão, o engano e a manipulação psicológica para obter informações sensíveis e acesso não autorizado a dados e sistemas.

A persuasão, capacidade de convencer ou influenciar (INFOPÉDIA, 2024) e a manipulação, interferência ou influência indevida exercida sobre determinado processo

[1] Especialização em Privacidade e Segurança da Informação na Universidade de Brasília-UNB.

(INFOPÉDIA, 2024), são componentes fundamentais em todo o processo. Aplicando técnicas psicológicas baseadas em princípios como escassez, autoridade, compromisso e consistência, afinidade e consenso (CIALDINI, 1984), o engenheiro social realiza a abordagem de forma planejada, para obter informações pessoais e credenciais confidenciais de forma ilegal. Os golpistas usam mensagens fraudulentas que parecem críveis para enganar as vítimas e induzi-las a tomar uma ação que lhes dá acesso às informações.

Os ataques de engenharia social podem assumir diversas formas, como *phishing*, *pretexting* e *baiting*, cada um projetado para explorar a confiança e a curiosidade das vítimas. À medida que a sofisticação desses ataques aumenta, é essencial que indivíduos e organizações compreendam não apenas os métodos utilizados, mas também a psicologia que os fundamenta, para que possam se proteger de maneira eficaz. Este artigo explora os principais tipos de engenharia social, os princípios psicológicos associados, seus impactos e as melhores práticas para prevenção, destacando a importância da conscientização e da educação na defesa contra essas ameaças.

DISCUSSÃO DO PROBLEMA

A engenharia social é uma técnica de manipulação que explora as vulnerabilidades humanas para obter informações confidenciais ou acesso não autorizado a sistemas. Diferente de ataques cibernéticos focados em brechas tecnológicas, a engenharia social depende da interação humana, tornando-se uma ameaça crescente em um mundo digital interconectado. A popularização do termo "Engenharia Social" é atribuída ao hacker Kevin Mitnick, que o definiu ainda nos anos 1990. Mitnick explorou o conceito de que o elo mais fraco de um sistema de segurança é representado por pessoas. Para Mitnick e Simon (2003), a engenharia social usa a influência e a persuasão para enganar as pessoas, convencendo-as de que o engenheiro social é alguém que na verdade não é, ou manipulando-as. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter informações, com ou sem o uso da tecnologia. É um método de ataque não violento que visa fazer com que a vítima realize ações prejudiciais a si mesma, como divulgar informações sensíveis ou transferir dinheiro para desconhecidos.

Os engenheiros sociais exploram as vulnerabilidades das pessoas, como confiança, medo, curiosidade, ingenuidade, entre outros. A maioria dos ataques de engenharia social depende da comunicação real entre os atacantes e as vítimas. Um exemplo comum de ataque de engenharia social é o *phishing*, que envolve o envio de mensagens destinadas a enganar ou coagir o alvo a realizar alguma ação. Atualmente, o *vishing*, conhecido como *phishing* de voz, vem ganhando

escala, propulsionado pelas evoluções do uso de robôs, de mecanismos tecnológicos avançados e de Inteligência Artificial, que permitem grande desempenho para efetuar ligações e para manipular os dados e áudios colhidos. Conforme o site Kaspersky (2024), as fraudes de cartões de crédito em 2015 movimentaram um total de US$ 16 bilhões em todo o mundo, e o *vishing* chegou a US$ 1 bilhão, de acordo com a BBC. Basicamente, o *vishing* pode ocorrer sempre que os criminosos têm acesso às informações pessoais das vítimas.

Muito embora a engenharia social muitas vezes tenha uma conotação negativa, referindo-se a atividades fraudulentas, ela também pode ser usada em contextos positivos, como conscientização sobre segurança, comercialização ou marketing, por exemplo. Entretanto, este trabalho mantém seu foco e desenvolvimento apenas no viés do primeiro perfil citado, a engenharia social como atividades que objetivam fraudes.

Psicologia embarcada na engenharia social

A Psicologia está profundamente enraizada nas técnicas de engenharia social, que possui dependência da compreensão e exploração do comportamento humano. Os engenheiros sociais manipulam as reações emocionais e os processos cognitivos das vítimas para influenciar suas decisões. A eficácia da engenharia social reside na sua capacidade de explorar comportamentos e emoções humanas. Algumas táticas comuns incluem:

- **Urgência -** Criar um senso de emergência que leva a vítima a agir rapidamente, sem tempo para pensar nas consequências. Isso pode ser feito através de mensagens que indicam que uma ação imediata é necessária para evitar problemas.
- **Exploração de fragilidades -** Se valer da necessidade ou mesmo da ganância do alvo para estabelecer contato e gerar confiança. Um exemplo desta tática são as falsas ofertas de emprego ou cursos gratuitos.
- **Validação social -** Indivíduos se baseiam no comportamento dos outros para guiar suas próprias ações. Um e-mail falso pode simular que vários colegas já tomaram uma ação específica, encorajando a vítima a fazer o mesmo.
- **Escassez -** Quando algo é percebido como raro ou disponível por tempo limitado, as pessoas são mais inclinadas a agir impulsivamente para não perder a oportunidade. Um exemplo é um e-mail fraudulento com ofertas "urgentes" de produtos ou serviços.
- **Autoridade -** Utilizar a aparência de um superior ou de alguma autoridade para intimidar a vítima e fazê-la cumprir ordens. As pessoas são mais propensas a seguir instruções de

figuras tidas como autoridades. Um engenheiro social pode se passar por um chefe ou agente de segurança para induzir comportamentos desejados.

- **Compromisso e consistência -** Pessoas tendem a agir de acordo com compromissos assumidos anteriormente. A técnica "pé na porta" é um exemplo, onde um pequeno pedido inicial é seguido por um maior, utilizando o compromisso anterior como uma forma de pressão.
- **Reciprocidade -** Oferecer algo de valor à vítima com a expectativa de que ela retribua, muitas vezes compartilhando informações em troca. Se alguém faz um favor a outrem, o favorecido sente a necessidade de retribuir. Um engenheiro social pode começar oferecendo uma "ajuda" ou "presente" para depois pedir algo em troca.
- **Empatia tática (afinidade e consenso) -** Estabelecer uma conexão emocional, fazendo a vítima sentir-se confortável em compartilhar informações. O golpista pode usar histórias pessoais ou circunstâncias difíceis para gerar simpatia. As pessoas são mais facilmente persuadidas por aqueles de quem gostam. Um atacante pode desenvolver um relacionamento amigável ou usar humor para construir afinidade.

A engenharia social é um campo fascinante, mas perigoso, que ilustra como a psicologia humana pode ser manipulada. A conscientização e a vigilância são essenciais para se proteger contra essas táticas.

O Engenheiro Social

Um engenheiro social é um profissional que utiliza técnicas de manipulação psicológica para enganar pessoas e obter informações confidenciais, acesso a sistemas ou realizar ações que beneficiem o atacante. Seu perfil engloba habilidades de persuasão, com perspicácia no uso da linguagem e do comportamento para criar uma conexão com o alvo, conhecimento psicológico, com entendimento profundo de como as pessoas pensam e reagem em diferentes situações e potente criatividade. Tais habilidades permitem identificar quais táticas podem ser mais eficazes. Cada ataque pode exigir uma abordagem única. Engenheiros sociais frequentemente criam cenários convincentes para induzir a vítima a agir. O engenheiro social é aquele que conquista a confiança da vítima para ter as informações que precisa (MITNICK; SIMON, 2003). A engenharia social explora a confiança humana e as fraquezas emocionais.

Tipos de Engenharia Social

Existem diversos tipos de engenharia social, que podem ser usadas isoladamente ou em combinação, dependendo do objetivo do atacante. Não há um número fixo de tipos de engenharia social, pois novas técnicas podem surgir com o tempo, no entanto, os principais tipos incluem:

- **Phishing – Um "bombardeio de iscas" para captura de informações**

O *phishing* se caracteriza pelo envio de e-mails ou mensagens que parecem ser de fontes confiáveis, solicitando informações pessoais ou financeiras. O objetivo é induzir a vítima a clicar em links maliciosos, induzindo as pessoas a fornecerem informações confidenciais, como senhas, números de cartões de crédito e dados pessoais. Os golpistas criam e-mails ou mensagens que imitam comunicações de empresas conhecidas, como bancos, provedores de serviços ou plataformas online. As mensagens geralmente contêm links que levam a sites falsos, onde as vítimas são incentivadas a inserir suas informações pessoais. Muitas vezes, os golpistas criam um senso de urgência ou medo, sugerindo que a conta da vítima pode ser suspensa ou que uma ação imediata é necessária. Conhecer os casos famosos de *phishing* na realidade nos ajuda a entender a gravidade desse problema e a importância de adotar medidas de proteção para garantir nossa segurança online (TISEC, 2024). Em 2020, o Banco Central do Brasil foi alvo de um ataque de *phishing* sofisticado que resultou em cerca de R$3 milhões transferidos para contas controladas por criminosos. O processo foi feito a partir de e-mails falsos, porém convincentes, enviados a funcionários da instituição, solicitando justamente atualização de informações de *login* para um sistema de uso interno (PROLINX, 2024).

- **Pretexting – Criando uma falsa identidade para gerar confiança (personificação)**

O atacante cria uma situação falsa para obter informações confidenciais de outra pessoa. O termo é frequentemente associado a fraudes e práticas enganosas, sendo comum em contextos como segurança da informação e proteção de dados. Por exemplo, fingir ser um funcionário de suporte técnico que precisa de dados para resolver um problema. O engenheiro social que usa essa técnica, pode se passar por um funcionário de uma empresa, um amigo ou até mesmo uma autoridade, fazendo perguntas que parecem inocentes ou legítimas. O objetivo é fazer com que a vítima confie nele e revele informações sensíveis, como senhas, dados pessoais ou informações financeiras. Em um golpe de *pretexting*, por meio de e-mails que apresentavam documentação,

aparentemente legítima, os hackers se passaram por fornecedores do Condado de Cabarrus (NC-USA) e solicitaram que os pagamentos já programados fossem realizados em uma nova conta bancária. O caso ocorreu em 2018 e o prejuízo foi de USD 1,7 milhão (TOTALPRIVACY, 2021).

- **Baiting – 'Se o serviço é de graça, você é o produto'**

Baiting é uma técnica de engenharia social onde um atacante oferece algo atrativo para seduzir a vítima e induzi-la a agir de maneira que comprometa sua segurança. Essa "isca" pode ser um arquivo, um software gratuito, um produto ou até mesmo um link em um site aparentemente confiável. A ideia é que a vítima, atraída pelo que está sendo oferecido, acabe revelando, inadvertidamente, informações sensíveis ou instalando malware em seu dispositivo. Embora *baiting* e *phishing* pareçam ser o mesmo tipo de ataque, não é a realidade. O *phishing* envolve cibercriminosos fingindo ser alguém que a vítima conhece, já o *baiting* não apresenta nenhuma dissimulação, ou disfarce. As investidas podem ser através de formas simples, do tipo, dispositivos como *pen drives* infectados deixados em locais públicos, esperando que alguém os encontre e os conecte a um computador, ofertas de d*ownloads* gratuitos de *software* ou arquivos que parecem interessantes, mas que na verdade contêm vírus ou *softwares* nocivos, ou anúncios enganosos de produtos populares que direcionam os usuários para sites maliciosos.

- **Tailgating – Um "ataque de cauda"**

Este tipo de ataque privilegia elementos físicos aos virtuais. Caracteriza-se pelo acesso físico não autorizado a áreas restritas, seguindo uma pessoa autorizada sem seu conhecimento. É comum em ambientes corporativos. Isso geralmente acontece em locais com controles de segurança, como escritórios ou instalações empresariais, onde o acesso é restrito por cartões magnéticos ou senhas. O atacante pode esperar que um funcionário autorizado use seu cartão para abrir uma porta e, em seguida, se infiltrar logo atrás dele, sem ser notado. Essa técnica se aproveita da cortesia humana — as pessoas tendem a segurar portas abertas para outras, especialmente se não suspeitam de más intenções. O *tailgating* pode levar a várias consequências negativas, como acesso a informações sensíveis, vazamentos de segurança ou danos de imagem ou reputação. Embora muitos esforços de segurança cibernética se concentrem na segurança de sistemas e redes, é importante não esquecer que a segurança física desempenha um papel crítico em qualquer programa de segurança cibernética (INFOSEC, 2020).

- **Vishing (Voice Phishing) – "Os bancos não ligam para pedir dados pessoais."**

O *vishing*, uma combinação das palavras "*voice*" e "*phishing*", é uma técnica de engenharia social em que golpistas usam chamadas telefônicas para enganar as vítimas e obter informações pessoais ou financeiras. Essa abordagem pode envolver o uso de números falsificados para parecer que a ligação é de uma instituição legítima, como um banco ou uma empresa de serviços públicos. Os golpistas geralmente se apresentam como representantes de uma empresa ou autoridade e podem usar táticas como urgência, ofertas tentadoras, máscara de números para impedir a identificação, dentre outras. Como vários outros tipos de ataques, pode culminar em roubo de identidade, com as Informações obtidas sendo usadas para fraudes, causando perdas financeiras. Diante do aumento exponencial de uma espécie de *vishing*, direcionado a clientes de instituições bancárias, a Federação Brasileira de Bancos (FEBRABAN) e seus bancos associados têm investido constantemente e de maneira massiva em campanhas de conscientização e esclarecimento com a população por meio de ações de marketing em TVs, rádios e redes sociais. Além da realização de campanhas educativas, os bancos investem cerca de R$ 4 bilhões por ano em sistemas de tecnologia da informação (TI) voltados para segurança – valor que corresponde a cerca de 10% dos gastos totais do setor com TI, para garantir a tranquilidade de seus clientes em suas transações financeiras cotidianas (SECURITY REPORT, 2024).

- **Smishing (SMS Phishing) – Milhas expirando, mercadoria retida pela Receita Federal, quem avisa é o inimigo!**

O *smishing* é um tipo de p*hishing* via mensagens de texto, onde o golpista envia SMS fraudulentos solicitando que a vítima clique em links ou forneça dados pessoais ou financeiros. Sua denominação é uma combinação das palavras "SMS" e "*phishing*". Assim como outras formas de *phishing*, o smishing envolve a manipulação emocional e a criação de urgência para levar a vítima a agir rapidamente. Os golpistas geralmente enviam mensagens de texto que parecem vir de instituições confiáveis, como bancos, provedores de serviços ou empresas conhecidas. As mensagens podem conter links maliciosos, solicitações urgentes ou às vezes, a mensagem pede que a vítima ligue para um número, que pode ser de um golpista. Como os demais ataques podem gerar acesso indevido a informações pessoais, que podem ser usadas para fraudes ou criação de contas falsas, consequentemente causando perdas financeiras. Segundo o site Kaspersky (2024), os atacantes costumam usar um dos dois métodos para roubar esses dados: uso de malware - o link da URL de *smishing*, técnica para persuadir o usuário para baixar

um software malicioso que é instalado no celular; ou o uso de site malicioso - o link na mensagem de *smishing* pode levar a um site falso que solicita informações pessoais sensíveis.

- **Impersonation – Simulando uma autoridade**

Impersonation, ou "imitação", é uma técnica de engenharia social onde um atacante se passa por outra pessoa, frequentemente alguém em uma posição de autoridade ou um conhecido da vítima, com o objetivo de estabelecer confiança, enganar e obter informações confidenciais ou acesso não autorizado a sistemas e recursos. Os golpistas podem criar perfis falsos em redes sociais ou enviar e-mails que parecem vir de uma fonte confiável, como um colega de trabalho ou um cliente. Realizar chamadas telefônicas, se passando por um representante de suporte técnico, para induzir a vítima a fornecer senhas ou dados pessoais, ou até criar documentos ou identificações falsas para ganhar a confiança da vítima em situações presenciais.

- **Quizzes e Surveys – Responda rápido!**

Os *quizzes* e os *surveys* são questionários interativos que podem testar conhecimentos, coletar dados ou entreter. Os *quizzes* geralmente são curtos e os *surveys* são questionários mais longos e abrangentes. Ambos podem apresentar uma variedade de tópicos. Em um contexto ilegítimo, eles podem ser usados para podem ser manipulados para roubar informações pessoais e traçar perfis detalhados das vítimas, coletar informações financeiras ou incluir links maliciosos que direcionam as vítimas a sites fraudulentos. Golpistas criam questionários ou pesquisas aparentemente inofensivas que, na verdade, coletam informações sensíveis. Um vídeo que usa a imagem de uma personalidade famosa, apresenta uma falsa promoção com recompensa por responder um quiz de avaliação da determinada marca. O conteúdo é compartilhado com a seguinte legenda: "*Responda e Ganhe! 25 anos da FARM. Atenção, amantes de malas! Os estoques são limitados e estão acabando rápidos! Não perca esta oportunidade única de expressar sua opinião e ser recompensado por isso*" (UOL, 2024). Neste caso, segundo relatos, são cobrados entre R$ 30,00 a R$ 75,00 pelo falso frete, os respondentes ficam sem o suposto brinde e sem o dinheiro pago pelo frete.

- **Dumpster Diving – A importância do descarte correto**

Dumpster diving, ou "mergulhar em lixeiras", é uma técnica de coleta de informações que envolve a busca em lixo ou materiais descartados para encontrar dados valiosos. Muitas vezes são informações que podem ser usadas para fraudes, roubo de identidade ou engenharia

social. Os atacantes podem procurar por documentos pessoais, como contas, extratos bancários, currículos e documentos legais que contenham informações sensíveis; materiais corporativos, do tipo relatórios ou propostas e documentos internos que possam revelar segredos comerciais ou dados de clientes; números de cartões de crédito ou chaves de acesso. Em seu livro Arte de Enganar (2003), Mitnick relata ter falsificado bilhetes de transporte de ônibus em Los Angeles, conseguindo passagens em branco descartadas em lixeiras e devidamente ajustadas por ele com a maestria de um hacker em formação, ainda adolescente:

> A obtenção das passagens em branco foi como passear no parque: as lixeiras dos terminais de ônibus estavam cheias de blocos de passagens parcialmente usados, os quais eram jogados pelos motoristas no final de seus turnos. Com um bloco de passagens em branco e o furador, podia marcar minhas próprias baldeações e viajar para qualquer parte aonde fossem os ônibus de Los Angeles. (MITNICK E SIMON, 2003)

- **Watering Hole Attack – Uma ameaça à espreita**

Um *watering hole attack* é uma técnica de ciberataque onde os hackers comprometem um site que é frequentemente visitado por um grupo específico de pessoas ou uma organização-alvo. A ideia é que, ao infectar um site que os alvos já visitam, possam introduzir malware em seus dispositivos sem que eles saibam. Os atacantes analisam quais sites são usados por um grupo ou organização específica, e exploram vulnerabilidades nesse site para inserir código malicioso, como scripts ou malware. Quando os membros do grupo visitam o site comprometido, seu dispositivo é infectado automaticamente, permitindo que os atacantes acessem informações confidenciais ou controlem o sistema da vítima. As consequências de um *watering hole attack* podem ser graves, partem de roubo de dados, acesso à rede corporativa, até alcançarem riscos de imagem, resultando em perda de confiança e danos à reputação. Em um golpe de *watering hole attack*, no ano de 2019, que ficou conhecido como Holy *Water Campaign* (Campanha de Água Benta), os cibercriminosos miraram grupos religiosos e de caridade na Ásia. Nesse caso, as vítimas foram influenciadas a atualizar o Adobe Flash, o que foi o gatilho para a ameaça, que entrou para a história devido à sua rápida evolução. Os motivos para o crime, entretanto, permaneceram desconhecidos (BACKUPGARANTIDO, 2021).

Impactos da Engenharia Social

Os impactos de um ataque de engenharia social podem ser devastadores, tanto para indivíduos quanto para organizações. As consequências podem incluir:

- **Perda Financeira** - Acesso não autorizado a contas bancárias ou cartões de crédito, resultando em perdas diretas.

- **Roubo de Identidade -** Uso de informações pessoais para fraudes, como abertura de contas bancárias ou solicitação de empréstimos em nome da vítima.
- **Danificação da Reputação -** Empresas podem sofrer danos significativos à sua imagem após vazamentos de dados, resultando em perda de clientes e confiança.
- **Comprometimento de Segurança -** Acesso a sistemas corporativos que pode resultar em ataques mais sofisticados, como *ransomware* (sequestro de dados com exigência de resgate).
- **Impacto Legal e Regulatório -** Organizações que falham em proteger os dados de seus clientes podem enfrentar ações legais e multas regulatórias.

Prevenção e conscientização

A Engenharia Social explora características humanas, com ganância, desejo, curiosidade, senso de oportunidade e muitas outras que dependem do meio social e do estilo de vida que o usuário possui, por isso o enfrentamento a estes ataques com ações de prevenção e/ou mitigação se torna mais complexo. Assim, dado que muitos ataques exploram fraquezas humanas em vez de vulnerabilidades técnicas, uma estratégia de defesa é fortalecer as reações humanas. A melhor defesa contra a engenharia social é a conscientização e a educação. Para proteger indivíduos e organizações, é essencial adotar uma abordagem proativa que combine educação, práticas seguras e o uso de tecnologia. Na tabela 1 apresentamos as principais medidas que podem ser implementadas para prevenir ou minimizar os riscos associados à engenharia social, capacitando as pessoas a reconhecer e resistir a tentativas de manipulação.

Tabela 1 – Principais medidas que podem ser implementadas para prevenir ou minimizar os riscos associados à engenharia social

Medidas de Educação Corporativa	
Medidas	**Descrição**
Treinamento de Funcionários	• Promover workshops sobre como reconhecer e responder a tentativas de engenharia social. Realizar treinamentos regulares sobre segurança da informação e reconhecimento de sinais de comprometimento em sites, ligações ou abordagens maliciosas. Simulações de ataques podem ser úteis para praticar a identificação de fraudes.
Educação sobre engenharia social	• Manter atualizações sobre as técnicas de engenharia social e compartilhar essas informações com a rede de relacionamento, família, amigos e colegas de trabalho.
Cultura de Segurança	• Fomentar um ambiente onde os funcionários se sintam à vontade para relatar atividades suspeitas sem medo de represálias.
Medidas de Proteção dos Ativos	
Medidas	**Descrição**
Autenticação de dois fatores	• Habilitar a autenticação de dois fatores adiciona uma camada extra de segurança, tornando mais difícil para os golpistas acessarem as informações.

Controle de acesso físico	• Instalar portas de segurança que exijam que cada pessoa tenha seu próprio meio de acesso para entrar.
Mecanismos de Monitoramento	• Implementar sistemas de monitoramento de acesso, como sensores de movimento ou câmeras de segurança.
Uso de Bloqueadores	• Instalar ferramentas de segurança, como antivírus e firewalls, podem ajudar a detectar e bloquear tentativas de malware.
Controle de Vulnerabilidade	• Incentivar o uso de VPNs e outras práticas seguras de navegação, especialmente ao acessar sites potencialmente arriscados.
Atualização de Sistemas e Políticas	• Manter software e sistemas atualizados. Revisar periodicamente políticas de segurança para garantir que estejam alinhadas com as melhores práticas.
Medidas Comportamentais	
Medidas	**Descrição**
Verificação de Identidade	• Implementar protocolos rigorosos para verificar a identidade de pessoas que solicitam informações sensíveis. Orientações de como entrar em contato com a instituição pelo número oficial ou como reconhecer a fonte da mensagem são primordiais. • Mesmo que a identidade do chamador ou remetente seja validada, não compartilhar informações pessoais por telefone, e-mail ou mensagem. Por medida de cautela, não fornecer senhas, números de cartão de crédito ou informações sensíveis por estas vias.
Desconfiança, controle psicológico e temporal	• Desconfiar de ofertas "boas demais para ser verdade", de chamadas inesperadas, ou de solicitações urgentes. • Sempre verificar a fonte e a legitimidade do produto que está sendo oferecido. • Não ceder aos gatilhos emocionais, postergar decisões e avaliar consequências. Fraudes muitas vezes usam a urgência como uma tática para pressionar a vítima.
Navegação segura	• Verificar se o endereço do site é legítimo (checar as URLs). Digitar o endereço do site diretamente na barra de endereço do navegador, sem clicar nos links sugeridos. • Ficar alerta aos riscos de links e anexos dos e-mails, SMSs, mensagens de mídias sociais e demais, sem ceder aos estímulos psicológicos embarcados nas mensagens. • Buscar sinais de autenticidade, como logotipos e informações de contato. • Observar o conteúdo das mensagens: erros de ortografia, endereços de e-mail desconhecidos ou mensagens alarmantes que pedem informações pessoais. Ignorar e deletar mensagens suspeitas. **Se for conveniente, formalizar denúncia aos canais competentes.**

Fonte: Síntese elaborada pela autora

CONCLUSÃO

Engenharia social é um conjunto de técnicas que utiliza a psicologia para enganar indivíduos, levando-os a revelar informações sensíveis, como senhas, dados financeiros ou acesso físico a instalações. Representa um dos principais responsáveis por incidentes de ataques cibernéticos e podem alcançar prejuízos financeiros incalculáveis. Representa uma técnica manipulativa e um desafio crescente na segurança da informação. À medida que as tecnologias evoluem, os métodos de manipulação se tornam mais sofisticados. A chave para mitigar esses riscos está na educação e na criação de uma cultura de segurança robusta, onde todos os

indivíduos estejam atentos e informados sobre as ameaças que enfrentam. Combater essas investidas crescentes é, antes de tudo, um esforço conjunto que envolve tecnologia, processos e, principalmente, pessoas.

A eficácia dos métodos de engenharia social se baseia em sua capacidade de explorar a psicologia humana, portanto, a conscientização e a educação são fundamentais para ajudar as pessoas a reconhecerem e resistir a essas ameaças. Implementar medidas de segurança robustas e fomentar uma cultura de segurança dentro das organizações são passos cruciais para proteger informações sensíveis contra esses ataques.

Já no século XIX, Frédéric Bastiat (1850) defendia a teoria de que muitas decisões podem gerar consequências indesejadas que não são visíveis de imediato. Em sua obra "O que se vê e o que não se vê" (BASTIAT,1850) apresentou casos práticos da época em que demonstrou a necessidade de considerar efeitos colaterais e impactos no longo prazo das escolhas, ou seja, de estar atento não só "ao que se vê", mas também, e principalmente, "ao que não se vê". Guardadas as proporções, na essência, as salvaguardas seguem fundamentos semelhantes: realizar análises friamente, verificar com cuidado e em fontes seguras, duvidar de ofertas milagrosas, não ceder aos gatilhos emocionais e postergar decisões para efetuar, no devido tempo, as verificações necessárias.

REFERÊNCIAS BIBLIOGRÁFICAS

BACKUP GARANTIDO. Watering hole attack. Disponível em: https://backupgarantido.com.br/blog/watering-hole-attack/. Acesso em: 24 out. 2024.

BASTIAT, Frédéric; JAKOBSMUSCHEL, L. O que se vê e o que não se vê. Título original: Ce qu'on voit et ce qu'on ne voit pas. Tradução em português de Jakobsmuschel, L. Montecristo Ed., São Paulo, 2021. ISBN 978-1-61965-252-1.

CIALDINI, R. B. Influence: Science and Practice. Harper Collins, 1984.

INFOPEDIA. Persuasão. Disponível em: https://www.infopedia.pt/dicionarios/lingua-portuguesa/persuas%C3%A3o. Acesso em: 24 out. 2024.

INFOSEC. Pentest físico. Disponível em: https://www.infosec.com.br/pentest-fisico/. Acesso em: 20 out. 2024.

KASPERSKY. Vishing. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/vishing. Acesso em: 20 out. 2024.

MITNICK, Kevin D.; SIMON, William L. A arte de enganar. São Paulo: [s.n.], 2003.

PORTAL TOTAL PRIVACY. Engenharia social: casos reais. Disponível em: https://www.totalprivacy.com.br/post/engenharia-social-casos-reais. Acesso em: 20 out. 2024.

PROLINX. Riscos cibernéticos. Disponível em: https://prolinx.com.br/riscos-ciberneticos/#:~:text=Em%202020%2C%200%20Banco%20Central,para%20contas%20controladas%20por%20criminosos. Acesso em: 26 out. 2024.

SECURITY LEADERS. FEBRABAN alerta para ligações de criminosos com falsas gravações para aplicar golpes. Disponível em: https://securityleaders.com.br/febraban-alerta-para-ligacoes-de-criminosos-com-falsas-gravacoes-para-aplicar-golpes/. Acesso em: 20 out. 2024.

TISEC. Phishing: casos famosos da vida real. Disponível em: https://tisec.com.br/phishing-casos-famosos-da-vida-real/. Acesso em: 20 out. 2024.

UOL. Mala FARM: falsa promoção. Disponível em: https://noticias.uol.com.br/confere/ultimas-noticias/2024/06/27/mala-farm-falsa-promocao.htm. Acesso em: 20 out. 2024.