

JOSÉ ELIAS OLIVER

O USO DA ENGENHARIA SOCIAL PARA A PRÁTICA DE CRIMES CIBERNÉTICOS

Artigo científico apresentado ao Centro Universitário São Lucas Ji-Paraná, para obtenção de grau na disciplina Trabalho de Conclusão – Projeto de Pesquisa, em Direito.

Professora. Orientadora: Rosicler Carminato Guedes de Paiva

Ji-Paraná
2024

Dados Internacionais de Catalogação na Publicação - CIP

O48u

Oliver, José Elias Oliver.

O uso da engenharia social para a prática de crimes cibernéticos. / José Elias Oliver. – Ji-Paraná, 2024.
23 p.

Artigo Científico (Curso de Direito) – Centro Universitário
São Lucas Ji-Paraná, 2024.

Orientadora: Prof.^a Esp. Rosicler Carminato Guedes de
Paiva.

1. Engenharia social. 2. Crimes cibernéticos. 3. Fraude. 4.
Segurança da informação. I. Paiva, Rosicler Carminato Guedes
de. II. Título.

CDU 351.74:681.51

Ficha Catalográfica Elaborada pelo Bibliotecário Giordani Nunes da Silva CRB 11/1125

O USO DA ENGENHARIA SOCIAL PARA A PRÁTICA DE CRIMES CIBERNÉTICOS

José Elias Oliver¹

Rosicler Carminato Guedes de Paiva²

RESUMO: A engenharia social é uma técnica muito usada em crimes cibernéticos, utiliza a manipulação psicológica para induzir as pessoas a revelar informações confidenciais e realizar ações. Essa prática é baseada na manipulação da confiança humana, em vez de usar as vulnerabilidades técnicas em sistemas. Os objetivos da engenharia social variam de roubar informações pessoais e golpes financeiros a invadir sistemas corporativos e governamentais. Entre as metodologias comuns empregadas, destacam-se o phishing, onde atacantes enviam e-mails fraudulentos que imitam comunicações legítimas para induzir vítimas a fornecer informações sensíveis. Que envolve criar um cenário falso para persuadir indivíduos a compartilhar dados confidenciais, outras táticas incluem o baiting, onde arquivos ou links maliciosos são disfarçados como (presentes) para enganar a vítima. E o pretexting que consiste em espionar alguém para ganhar acesso a dados sensíveis normalmente usados no ramo empresarial. Os resultados desses ataques podem ser devastadores, até mesmo em perda financeira, comprometimento de informações pessoais, danos à reputação e impactos operacionais significativos para empresas e instituições. Em muitos casos, as vítimas enfrentam dificuldades na recuperação de seus dados. Conclui-se que a engenharia social é uma ameaça significativa, uma vez que explora as vulnerabilidades humanas, as quais são mais difíceis de proteger do que as vulnerabilidades técnicas de informática. Portanto, a prevenção e a redução desses ataques exigem uma combinação de conscientização, treinamento e educação no meio digital. Uma vez entendendo como funciona um ataque cibernético utilizando a engenharia social, podemos nos proteger e minimizar os riscos enquanto utilizamos a internet.

Palavras-chaves: Engenharia social. Crimes cibernéticos. Fraude. Segurança da informação

THE USE OF SOCIAL ENGINEERING TO PERMIT CYBER CRIMES

¹Acadêmico do 10º período do curso de Direito no Centro Universitário São Lucas Ji-Paraná/RO – AFYA. E-mail: bf4_ps3_2015@hotmail.com

² Professora. Orientadora: Rosicler Carminato Guedes de Paiva, professora e Coordenadora do Curso de Direito do CENTRO UNIVERSITÁRIO SÃO LUCAS JI-PARANÁ, RONDÔNIA, ministrando as disciplinas de Estágio Supervisionado II e Clínica de Direitos Humanos; Orientadora de Trabalho de Conclusão de Curso II - TCC II. Membro do NDE - Núcleo Docente Estruturante e do CONSEPE - Conselho Superior de Pesquisa. Representante das Coordenações de curso no CONSUP - Conselho Superior. Membro Efetivo da COMISSÃO DO ENSINO JURÍDICO da Ordem dos Advogados do Brasil - OAB, Subseção de Ji-Paraná, Rondônia, Trainer Practitioner em Programação Neurolinguística - PNL, Pós-graduada em Direito Penal e Direito Processual Penal, pela Faculdade Vale do Rio Doce/MG; em Inovação, Gestão e Práticas Docentes no Ensino Superior, Faculdades Santo Agostinho, Itabuna/BA, e em Educação, Bem-estar e Felicidade, Faculdades Santo Agostinho, Itabuna/BA. E-mail: Rosicler.paiva@saolucasjiparana.edu.br

ABSTRACT: Social engineering is a technique widely used in cybercrime, using psychological manipulation to trick people into revealing confidential information and taking action. This practice is based on manipulating human trust, rather than exploiting technical vulnerabilities in systems. The goals of social engineering range from stealing personal information and financial scams to hacking into corporate and government systems. Common methodologies used include phishing, where attackers send fraudulent emails that mimic legitimate communications to trick victims into providing sensitive information. This involves creating a false scenario to persuade individuals to share confidential data. Other tactics include baiting, where malicious files or links are disguised as (gifts) to deceive the victim. And pretexting, which involves spying on someone to gain access to sensitive data typically used in the business sector. The results of these attacks can be devastating, including financial loss, compromise of personal information, reputational damage, and significant operational impacts for companies and institutions. In many cases, victims face difficulties in recovering their data. It is concluded that social engineering is a significant threat, since it exploits human vulnerabilities, which are more difficult to protect than computer vulnerabilities. Therefore, preventing and mitigating these attacks requires a combination of awareness, training, and education in the digital environment. Once we understand how a cyber attack using social engineering works, we can protect ourselves and minimize the risks while using the Internet.

Keywords: social engineering. Cyber crimes. Fraud. Information security

INTRODUÇÃO

A engenharia social pode ser definida como, manipulação psicológica de pessoas para obter informações confidenciais, acessar sistemas sem permissão ou fazê-las executar ações que beneficiem o cibercriminoso.

Portanto a engenharia social é uma técnica amplamente utilizada em crimes cibernéticos, onde os criminosos manipulam psicologicamente indivíduos para obter informações confidenciais ou acesso a sistemas protegidos, em que o cibercriminoso atua para ganhar a confiança da vítima.

A eficácia da engenharia social reside na exploração das fraquezas humanas, como a tendência de confiar em pessoas aparentemente legítima ou a falta de conhecimento sobre práticas de segurança no ambiente digital, tornando-a uma das estratégias mais perigosas e eficazes dos cibercriminosos.

O delito tem aumentado muito por conta da facilidade da prática, tendo em vista que pode ser realizada em qualquer local do mundo, contra qualquer indivíduo, sendo uma prática com alto nível de impunidade por conta da falta de contingente e difícil rastreio, levando em conta os meios usados como exemplo VPN (Virtual Private Network), e perfis falsos.

Assim como, o meio de comunicação e negócios, acabam sendo usados a dark web como ponto de negociação entre os criminosos, como se fosse uma área fora de qualquer tipo de restrição ou leis, muito utilizada como safe zone (lugar seguro), para quem quer realizar qualquer ato ilícito no ambiente digital, tornando praticamente impossível de ser rastreado, por tais motivos é muito empregado pelos cibercriminosos.

Neste novo ambiente, a engenharia social aprimorou-se e tornou possível variados ataques, incluindo o phishing, baiting, pretexting, termos utilizados para enganar possíveis vítimas por meio de infinitas possibilidades proporcionadas pela criatividade e ousadia dos cibercriminosos.

Portanto, a pesquisa envolveu a análise de casos judiciais e legislativos relevantes, examinando a aplicação e a eficácia das leis vigentes no combate aos crimes cibernéticos, estudos de caso foram verificados para mostrar as táticas de engenharia social mais comuns e suas consequências jurídicas e financeiras.

1. ENGENHARIA SOCIAL

A engenharia social é um método empregado por criminosos cibernéticos para manipular pessoas e conseguir acesso não autorizado a informações sigilosas ou sistemas informáticos e dados pessoais. Ela se apoia na psicologia humana e na interação social para enganar as vítimas e explorar suas vulnerabilidades, ao invés de usar apenas métodos convencionais de hacking, por meio de programas.

Portanto, a ligação entre a engenharia social e o crime cibernético pode ameaçar significativamente a segurança da informação e a integridade das

instituições, organizações e indivíduos que operam nesse espaço, visando danos financeiros e morais para suas vítimas.

Sendo assim, não é suficiente ter uma compreensão teórica dos mecanismos técnicas dos ataques cibernéticos, é necessário abordar mais de perto os aspectos psicológicos e sociais do comportamento criminoso, que utiliza os princípios da engenharia social, as formas mais comuns de estratégias usadas pelos cibercriminosos.

Os principais meios são, e-mail, mensagens no celular (Whatsapp), ligações se passando por empresas ou como falso sequestrador, já que o objetivo central é fazer a vítima acreditar no ato que o cibercriminoso criou. Podendo assim atingir seu abjetivo sem a necessidade do uso qualquer meio de programas de hacking, apenas explorando o erro humano, onde apenas com dados disponibilizados por meio das redes sociais.

Frequentemente facilitadas por técnicas de engenharia social, destacam a relevância da conscientização e educação digital como formas de prevenção desse tipo de crime, enfatizando que a legislação deve acompanhar a evolução tecnológica e comportamental da sociedade.

A aplicação dessas leis e o desenvolvimento de mecanismos adequados são essenciais para a proteção dos direitos dos cidadãos na era digital, ressaltando a necessidade de uma interpretação dinâmica e moderna do direito penal para combater com eficácia a cibe criminalidade.

O estudo enfatiza a necessidade de programas de conscientização, visando treinar os usuários finais para identificar e responder adequadamente aos esforços maliciosos da engenharia social. De uma perspectiva tecnológica, a adoção de mecanismos avançados de segurança, como sistemas de autenticação multifatorial, filtros antiphishing e inteligência artificial para detectar e combater ameaças em tempo real.

Da perspectiva legal, a pesquisa estuda a eficácia e, especialmente, os meios de modernização desses crimes, apresentar propostas de segurança pública possíveis melhorias legislativas e estruturais como, equipamentos de hardware e software, fechando vulnerabilidades abusadas por criminosos.

Além de como diminuir a incidência de crimes cibernéticos, cometidos por meio de engenharia social, e desenvolver estratégias que combinem aspectos tecnológicos, e legais para criar um ambiente digital mais seguro.

Identificar as vulnerabilidades humanas e técnicas que são exploradas por cibercriminosos e propor medidas preventivas eficazes. Isso envolve, primeiramente a análise aprofundada dos métodos de engenharia social utilizados, como phishing, pretexting, baiting, para entender como esses ataques que exploram a confiança e a falta de conhecimento das vítimas.

Para melhorar a eficácia das autoridades para o combate aos crimes virtuais, a necessidade de cooperação entre os Estados e até mesmo internacional, para enfrentar a natureza transnacional dos crimes cibernéticos, visando criar um quadro abrangente de defesa contra crimes cibernéticos, integrando educação, tecnologia e legislação eficaz para reduzir a incidência desses crimes e proteger melhor os indivíduos e organizações no ambiente digital.

A importância em fornecer uma compreensão dos mecanismos usados em crimes cibernéticos, facilitados pela engenharia social, bem como demonstrar soluções práticas e aplicáveis para diminuir essas ameaças, como a não utilização de senhas interligadas com objetos ou pessoas a sua volta, nomes de conhecidos, datas, nome de pets. Não negociar produtos com valor de mercado muito a baixo do normal, pode prevenir para não se tornar mais uma vítima.

Em um mundo cada vez mais digitalizado, onde dados sensíveis e operações digitais são constantemente alvo de cibercriminosos, a relevância de uma prevenção e resposta se torna indiscutível, com isso a pesquisa buscou abordar metodologias, iniciando com os meios e técnicas utilizados pela engenharia social, com o objetivo

de aprimorar a cibersegurança permitindo trazer conhecimento que aumentam a compreensão do assunto.

Com tudo, Mitnick e Simon (2003, p. 4) deixam a seguinte afirmação sobre Engenharia Social:

À medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a “firewall humana” quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo.

A combinação dessas diversas metodologias garantiu uma abordagem ampla, proporcionando clareza ao tema que podendo informar políticas públicas, estratégias corporativas de cibersegurança, de forma educacional, e pro uso cotidiano comum, com o objetivo de construir uma defesa mais robusta e na diminuição no número de ocorrências no ambiente digital, contra a crescente ameaça dos crimes cibernéticos.

Através de uma variedade de estratégias persuasivas, os criminosos podem induzir as pessoas a revelar senhas, números de cartões, informações pessoais ou até mesmo executar ações prejudiciais em seus próprios sistemas, acessar e-mails, links, fazer download de arquivos maliciosos, usando a curiosidade humana.

Como por exemplo, deixar um pen drive com malware em locais públicos para que despertar a curiosidade de alguém e queira conectar em seu computador, propagandas falsas de produtos, notícias falsas, sendo uma infinidade de opções, bastando uma mente criativa e com má índole para cometer os cibercrimes.

Uma nova técnica empregada pelos cibercriminosos é o uso da inteligência artificial. Por ser uma tecnologia muito recente, ainda não é usado com muita frequência, tendo alguns casos sendo relatados ao redor do mundo, mas suas possibilidades de emprego são preocupantes, pois criar um cenário com IA, além de facilitar muito o trabalho dos engenheiros sociais, tendo em vista que é muito convincente para enganar suas vítimas.

Podendo criar rostos, vídeos, pessoas, literalmente qualquer coisa, certeza será muito explorado pelos cibercriminosos, pois essa tecnologia com seu fácil uso e acesso, é visto como brecha para a criminalidade no âmbito virtual, tendo em vista seu potencial gigantesco, podendo gerar alusões em incontáveis possíveis cenários.

Geralmente o meio mais eficaz de combater uma IA, é justamente criando outra, pois qualquer ferramenta feita por programação tem um meio operacional padrão, seguindo linhas de códigos que são facilmente detectados com ferramentas que procuram esses padrões, como se fossem um leito de código de barras, visando achar e proteger os meios virtuais.

Outro método que saiu do controle nos últimos anos foi a clonagem de Whatzapp, que consiste em ativar uma conta em outro dispositivo, assim se passando pela pessoa, e aplicar golpes em seus contatos adicionados, geralmente com as informações das mensagens antigas do número clonado, é possível obter informações para facilitar e ser mais convincente.

Existem maneiras de se proteger contra essas práticas de clonagem, uma delas é simplesmente ativando a confirmação em duas etapas em seu aplicativo, outro meio de se proteger é evitar deixar seu número pessoal disponível de forma muito acessível, em perfis de rede social, em grupos desconhecidos, em sites de compras e vendas como, OLX, marketplace, e caso seu número seja clonado sempre tente comunicar o mais rápido possível o fato para seus contatos, e procure a delegacia mais próxima para relatar o ocorrido.

Conclui-se que, sempre vai haver interações sociais por meio da internet, mas visando uma navegação segura e saudável, temos que ter responsabilidade com nossas ações pois, são elas que podem nos colocar em risco mesmo que mínimos, não podemos nos dar ao luxo de contar com a sorte, navegar na internet deve sempre ser da forma mais segura possível.

1.1 PHISHING

O Phishing é um dos métodos mais usados pelos engenheiros sociais por ser, mais eficaz pois esse tipo de ataque cibernético tem um alvo específico, é um ataque direcionado, com foco em empresas e organizações, por ter uma vítima específica ele é mais elaborado nas abordagens, sendo um ataque personalizado.

Junto com a manipulação de diversos sentimentos, onde os criminosos exploram sentimentos como medo, curiosidade ou ganância para motivar as vítimas agir conforme desejado, isso pode incluir o envio de e-mails, sites clonados, mensagens que parecem ser de instituições legítimas, frases com clickbait que estimulam um simples click, pedindo às vítimas que acessem links maliciosos ou forneçam informações confidenciais.

Mesmo esse método não tendo quase sempre das vezes um alvo específico, ele acabou se tornando o mais usado pelos cibercriminosos, por ter um alcance muito grande e ser mais fácil pois, não necessita de horas de preparação, apenas jogam na rede e deixam o maior número de pessoas caírem em suas armadilhas.

Um caso que ficou famoso ocorreu na eleição presidencial de 2016 nos Estados Unidos.

Um dos casos mais emblemáticos de engenharia social é a eleição presidencial dos Estados Unidos em 2016. Ataques de phishing levaram ao vazamento de e-mails e informações do Partido Democrata que podem ter influenciado o resultado da eleição, com a vitória de Donald Trump sobre Hillary Clinton. Os hackers criaram um e-mail falso no Gmail, convidando os usuários, por meio de um link, a alterar as suas senhas devido a atividades incomuns. Os fraudadores então tiveram acesso a centenas de e-mails contendo informações confidenciais sobre a campanha de Clinton.

Atualmente existem vários mecanismos de defesa contra o phishing, normalmente são realizados por inteligência artificial, são marcados como Spam ou até mesmo são bloqueados antes mesmo de chegar ao alcance das pessoas, mas como a tecnologia avança para o bem, também existe avanço para o mau.

Portanto, não podemos esperar que a tecnologia seja a nossa única salvação, sendo necessário a nos adaptar e aprender a lidar com essas ameaças diariamente

pois, nenhum programa ou método virtual irá nos proteger a todo tempo, sendo necessário um conjunto de fatores que se forem seguidos, vão tornar o tempo de exposição a internet bem mais seguro.

1.2 PRETEXTING

O pretexting é muito comum no âmbito empresarial pois, consiste em criar um falso cenário para induzir a vítima a disponibilizar dados sensíveis, geralmente esse ataque é feito pelo cibercriminoso se passando por um membro da empresa com um cargo superior, assim fazendo com que o alvo fique coagido pela posição hierárquica, e acabe cedendo aos pedidos por medo ou simplesmente por estar sendo convencido.

Existem outras táticas, onde os criminosos se fazem passar por uma figura de autoridade ou como um funcionário de suporte técnico, um funcionário da mesma empresa, mas de outra filial, a fim de obter acesso a sistemas ou informações sensíveis. “Quanto mais a tecnologia e os dispositivos de segurança evoluem dificultando assim a exploração de vulnerabilidades, mas os invasores explorarão o fator humano” (MARCELO; PEREIRA, 2005, p. 3).

Com apenas uma informação simples é possível ganhar a confiança de alguém ainda mais se tratando do ramo empresarial. Um exemplo básico e comum é saber o nome de alguns funcionários saber se estão de férias ou estão viajando, fazer pedidos em nome deles para parecer mais convincente, sendo simples e bastante eficaz, já que hoje pode ser considerado fácil obter informações pessoais, apenas acessando as redes sociais de quem pretende ter essas informações.

Infelizmente ainda não é cultura das empresas investirem no treinamento e na conscientização dos seus funcionários, afinal eles também fazem parte da segurança da informação, mas as empresas acabam deixando de lado outro aspecto tão importante quanto à tecnologia (BASTOS, 2010, p. 18).

Os funcionários de empresas que não receberam treinamento adequado em segurança da informação, ou até mesmo aqueles que tem um sentimento em ser muito prestativo são uma das características que tornam as pessoas mais vulneráveis, além disso podem ser usados informações privilegiadas para diminuir as suspeitas,

como por exemplo entrar em contato com um funcionário e dizer o nome de alguém com cargo superior e dizer que está cumprindo a pedido dessa pessoa.

Portanto, se tratando do uso de engenharia social para a prática de crimes virtuais, é ainda mais essencial para as empresas manter seus dados protegidos, por ser um possível alvo a qualquer momento, devendo sempre adotar políticas internas rigorosas sobre informações importantes da empresa e relacionados.

1.3 BAITING

O baiting consiste em usar uma isca para atrair a atenção de seus alvos, é uma técnica parecida com o Phishing, porém, ela é mais atrativa pois, usa o impulso da ganancia ou da curiosidade ainda mais, sendo quase irresistível para a vítima, como se fosse um cavalo de Troia, inicialmente parece ser inofensivo, todavia, é o que o cibercriminoso quer que pareça.

Esses ataques normalmente são para alvos selecionados, para uma maior precisão, e gerando menos desconfiança da parte das vítimas, podendo ser disfarçados de presentes ou super promoções, sendo esses itens CDs, pen drives, imaginando que se apenas um desses objetos sendo conectados a um computador, para que possam infectar a rede com malware e ceder informações importantes.

Imaginando um cenário envolvendo um ataque de engenharia social, uma empresa do ramo de tecnologia, muito grande e com centenas de funcionários, alguém com acesso ao inteiro dessa empresa espalha vários, pen drives infectados com malware, se caso a empresa não tenha fornecido treinamento sobre esses perigos para os funcionários, a chance de algum desses pen drive ser usado em algum computador da empresa é muito provável.

Nesses casos a necessidade de um conhecimento básico sobre essas técnicas, podem evitar danos materiais e morais, apenas sabendo como funciona esses ataques de engenharia social, e não se deixando agir por impulso enquanto estiver em ambiente digital.

Pois os ataques de engenharia social, ora dependem de um certo descuido por parte das vítimas, são breves momentos de descuido sejam esses, apenas clicando em um link, baixando um arquivo, preenchendo um formulário, comprando algo na internet, são esses descuidos que são explorados pelos engenheiros sociais.

“A falta de consciência das pessoas a respeito das técnicas de Engenharia Social e o seu excesso de autoconfiança são os principais aspectos que favorecem o sucesso da Engenharia Social” (BASTOS, 2010, p. 17). As vítimas mais vulneráveis a esses ataques são geralmente aquelas que possuem pouca consciência sobre os riscos de segurança cibernética e são mais suscetíveis a manipulações psicológicas.

Isso pode incluir indivíduos inexperientes em tecnologia, idosos, crianças, onde seus alvos preferidos do cibercriminosos são pessoas com grandes fortunas, principalmente os que espõem suas riquezas em redes sociais despertando o interesse dos criminosos, visando sempre um alto ganho.

Cada ataque de engenharia social é único, podendo abranger várias etapas ou até mesmo incorporar técnicas de ataque mais convencionais para alcançar o resultado final pretendido. Além disso, existem outras formas e métodos comuns, como a busca de informações em lixos corporativos ou residenciais, que podem colocar em risco a segurança.

Como papeis com informações importantes, CDs, pen drives, sempre utilizando-se de falhas humanas para obter informações sem a necessidade do uso de programas ou conhecimento de hacking para invadir sistemas, assim devendo sempre desconfiar de coisas que fogem do comum e buscar verificar cada ação realizada.

O uso de técnicas de engenharia social sempre almeja a persuasão da vítima, seja ela de maneira aparentemente amigável ou com ameaça, sempre com o mesmo abjetivo, por meio da enganação como um teatro onde o criminoso tenta levar vantagem, na maioria das vezes econômica, e independente do resultado do ataque ele simplesmente desaparece sem deixar rastros.

Assim diminuindo a ligação entre o criminoso e a vítima já que usa apenas informações dadas pela própria vítima ou colhida pela internet, evitando qualquer ligação por meio eletrônico com a vítima, diminuindo os riscos de ser encontrado, podendo levar investigações muito longas e complexas, afastando até mesmo a possibilidade das autoridades de localizar o criminoso.

Para grande parte da doutrina nacional, a maioria dos crimes consumados na rede de computadores recai, da mesma maneira no mundo concreto.

Neste sentido, conceitua Pinheiro:

A Internet surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória, bem como às necessidades de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio. (PINHEIRO, p.36. 2010).

A falta de impunidade para os criminosos cibernéticos muitas vezes encoraja esses ataques, visto que os mesmos podem operar com relativa segurança por se tratar de crimes a distância, muitas vezes podendo ser realizado de outros países dificultando muito a localização dos criminosos, onde sempre se escondem atrás de aplicativos para redirecionar o IP da rede. Com o uso de contas bancárias de laranjas, e documentos falsos.

Existindo a possibilidade do uso de uma decoy termo para distração que nada mais é um ou mais IPs, sendo esses que levam a endereços errados de forma que atrase as investigações, levando a impunidade em muitos casos.

Sendo que em quase todos os casos por falta de conhecimento ou de noção da vítima como comprometimento de informações e arquivos postos na rede de forma irresponsável comprometendo a segurança de terceiro ou a própria segurança. “O rápido crescimento do uso do computador e a difusão da Internet têm contribuído para um crescimento de crimes de computador e uma diversidade significativa de criminosos de computador” (PIPKIN, 2003, p.8).

A falta de informação sobre os riscos associados ao uso da internet é uma preocupação significativa, especialmente considerando o aumento da dependência digital em todas as esferas da vida, muitos usuários não têm consciência dos perigos potenciais que estão expostos, como malware, phishing, roubo de dados e fraude online. “A partir destas vulnerabilidades ocorridas no sistema as ameaças agem tentando adentrar em uma rede ou sistema, buscando falhas na parte de usuários, sendo o elo mais fracos na segurança da informação” (GONÇALVES, 2022, P.10).

Isso pode levar a comportamentos de risco, como clicar em links suspeitos, compartilhar informações pessoais em redes sociais ou baixar aplicativos ou arquivos de fontes não confiáveis, aumentando assim sua exposição a riscos desnecessários, uma das melhores formas de utilizar a internet de forma segura é sempre desconfiar antes de cada click pois.

Outro ponto importante para se manter seguro no meio virtual, é não deixar dispositivos eletrônicos com acesso à internet com crianças, pois são alvos muito vulneráveis, sempre deixe os aparelhos offline para evitar exposição a riscos desnecessários, da mesma maneira indivíduos com pouca afinidade com eletrônicos.

Simples informações colocadas na rede podem ser o pontapé inicial para um ataque, qualquer informação pessoal ou de outra pessoa colocada à disposição na rede, que pode ser usada para quebrar senhas, a depender do padrão normalmente usados como, nome de animais de estimação, nomes dos pais, datas importantes, lugares, dentre uma infinidade de possibilidades, que podem ser usadas em ataques de engenharia social.

Portanto, para que o ataque no meio digital tenha sucesso, sempre haverá participação da própria vítima, uma vez que se tratando de uso da engenharia social pois, a única forma do cibercriminoso acesso a certas informações cruciais é obtendo elas diretamente do seu alvo.

Um dos maiores problemas hoje em dia na segurança da informação está relacionado ao ser humano e sua ignorância. Práticas que permitem o acesso não autorizado a dados, lugares, objetos e entre outros, fragiliza qualquer esquema de segurança da informação, uma vez que as pessoas acabam tendo acesso a informações indevidas, colocando em risco a segurança da

informação. A questão comportamental pode afetar significativamente as demais medidas de segurança, por mais modernas que elas sejam. (SILVA, M.; COSTA, 2009)

Além disso, os criminosos cibernéticos muitas vezes operam em plataformas descentralizadas da internet, como a dark web, onde podem comprar e vender informações roubadas, malware e serviços de hacking, esses mercados clandestinos fornecem um ambiente seguro para atividades ilícitas, onde os criminosos podem permanecer anônimos.

Por esse motivo traz uma segurança para o cibercriminoso, operando a distância até mesmo em outros países, utilizando meios que dificultam até mesmo impossibilitam sua localização pelas autoridades, sempre estando à frente, evitando a aplicação de medidas de combate a esses tipos de crimes.

Com a ajuda da natureza descentralizada e anônima da dark web e o uso das cripto moedas, se torna extremamente desafiador para as autoridades, rastrear e interromper atividades criminosas, contribuindo assim para a impunidade dos cibercriminosos, que operam tranquilamente.

Em síntese, a engenharia social representa uma ameaça no cenário cibernético atual, explorando a vulnerabilidade humana para a prática delituosa, com o objetivo de diminuir esses riscos, é essencial aumentar a conscientização sobre segurança cibernética para a população, fornecer treinamento adequado para funcionários e empresas.

Sendo que atualmente é quase impossível ficar imune a ataques virtuais, porém existem maneiras que tornam o trabalho dos cibercriminosos mais difícil, formas simples como, não repetir a mesma senha em mais de um aplicativo, não usar senhas simples, sempre usar mecanismos de autenticação em duas etapas, usar um antivírus de qualidade, manter todos os softwares atualizados, utilizar esses simples passos podemos nos tornar muito menos suscetíveis a ataques no meio virtual.

Uma tática muito utilizada pelos cibercriminosos é se passar por alguém como por exemplo, informar que depositou um valor na conta errada, então pedem para

devolver o valor depositado, sendo que na verdade a pessoa acabou de fazer um empréstimo em seu nome, e precisa depositar o valor em sua conta para posteriormente poder transferir para a do criminoso, em forma de devolução.

Fazendo com que muitas pessoas acabam acreditando e sendo vítimas desses métodos simples e muito eficazes na maioria das vezes, por conseguirem a confiança da vítima, se torna uma prática corriqueira utilizada pelos criminosos em meio virtual.

São técnicas empregadas por criminosos virtuais para induzir usuários para revelar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados, explorando a boa vontade e a falta de conhecimento do usuário. (MARCIANO E LIMA-MARQUES, 2006, p.14),

Sendo de uso regular o uso da engenharia social, no contexto dos crimes cibernéticos, uma das maneiras mais usadas pelos cibercriminosos para o sucesso dos ataques é a obtenção de dados pessoais para facilitar a prática de delitos.

Diante dessa informação em 2021 a Serasa Experian teve o maior vazamento de dados pessoais da América Latina e um dos maiores de todo o mundo, sendo um total de 220 milhões de brasileiros, até mesmos dados de pessoas falecidas, dados como, CPF, nome, data de nascimento, foto de rosto, gênero, endereço, telefone, e-mail, salário, score de crédito.

“A segurança da informação é a preservação da confidencialidade, integridade, disponibilidade, autenticidade e o não repúdio das informações e dados que são indispensáveis para uma organização ou um indivíduo” (SOUZA, 2022, p.3). Medidas de aplicação da lei para responsabilizar os cibercriminosos, somente através de uma abordagem ampla e colaborativa podemos enfrentar eficazmente os desafios apresentados pela engenharia social e proteger nossas informações e sistemas contra ataques cibernéticos.

Tendo em vista a quantidade de sites e empresas com bancos de dados de seus clientes, podendo a qualquer momento acontecer um vazamento desses dados sensíveis, deixando milhares até mesmo milhões de pessoas vulneráveis a ataques,

essa pratica não é nada bom para a segurança da informação, sendo um risco altíssimo para todos que tem dados armazenados.

Com todos esses dados pessoais disponíveis na rede deixam os brasileiros vulneráveis a ataques e golpes fraudulentos, facilitando imensamente a prática dos crimes pelos cibercriminosos, por ter tantos dados a sua disposição, podendo até mesmo fazer uma lista com os dados de pessoas com mais renda, aumentando muito a taxa de sucesso para os cibercriminosos.

Uma pesquisa inédita feita pelo DataSenado em parceria com o Nexus ouviu 21 mil pessoas e revela que 1 em cada 4 brasileiros foi vítima de golpes digitais só nos últimos 12 meses. Esse é o levantamento mais amplo já feito sobre o assunto, que mostra também que mais da metade das vítimas ganham até dois salários mínimos.

Como já citado anteriormente, os cibercriminosos acabam se tornando mais seletivos, visando cada vez mais golpes maiores, quanto maior for o patrimônio a pessoa tem maior é o interesse. Outro ponto importante é a quantidade de vítimas, se tornando um dos crimes mais praticados no país.

2. LEGISLAÇÃO ACERCA DE CRIMES CIBERNÉTICOS

Com os dados necessários dão início a prática dos crimes cibernéticos, onde tal prática se encontra completamente tomado de esquemas de phishing, e outras formas de fraudes eletrônicas, assim configurando crime previsto no Código Penal brasileiro, em específico, o artigo 171§ 2º-A, que trata do crime de estelionato, pode ser aplicado quando a engenharia social é utilizada para, induzir a vítima ao erro e obter vantagem ilícita.

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)

Podemos citar o caso da atriz Carolina Dieckmann, que em 2011 por meio de ataques cibernéticos, teve fotos e vídeos de vários tipos inclusive íntimos, após a

repercussão do caso houve a criação da Lei nº 12.737/2012 em 2012, que veio tratando de crimes cibernéticos que na época existiam pouquíssimos artigos de lei tratando do assunto, podemos analisar que para que houvesse uma movimentação do judiciário sobre o assunto, precisou que alguém com influência tivesse que sofrer um ataque.

Além disso, a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, introduziu alterações no código penal, tipificando condutas relacionadas à invasão de dispositivos informáticos para obtenção de dados sem autorização, sendo que a lei geral de proteção de dados pessoais (LGPD), Lei nº 13.709, de 14/08/2018, aprimorou a privacidade digital e implementou no combate aos cibercriminosos.

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Vigência Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Vigência Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.²⁰

Em 2018 tivemos a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14/08/2018, que aprimorou a privacidade digital e implementou no combate aos cibercriminosos, com cada vez mais a introdução de procedimentos digitais, os dados ficam cada vez mais nas redes possibilitando os ataques de cibercriminosos em banco de dados com milhões de registro de dados pessoais altamente sensíveis.

Os crimes mais comuns ainda são os furtos por meios eletrônicos pois, são mais lucrativos para os cibercriminosos como, furto de material intelectual, dinheiro

em contas bancárias, até mesmo cripto moedas em que nesses casos é impossível rastrear qualquer informação, se qualificando no art. 155, § 4º-B do Código Penal.

Seguindo sobre dispositivos legais acerca dos crimes cibernéticos no Brasil a doutrina é unânime no assunto de crimes cibernéticos, no que se refere-se ao meio operante para se julgar como cibercrime na caracterização do crime em si, para que este seja apontado como crime virtual é necessário que tenha sido praticado por meio ou contra sistemas de informática. Nesse sentido conceitua Cassanti:

Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital. (Cassanti, p.6, 2014).

Portanto, não é suficiente ter uma compreensão teórica dos mecanismos técnicos dos ataques cibernéticos, é necessário abordar mais de perto os aspectos psicológicos e sociais do comportamento criminoso que se utiliza dos princípios da engenharia social.

3. CONSIDERAÇÕES FINAIS

O artigo científico foi desenvolvido através de análises de doutrinas, legislações, julgados, artigos científicos, sendo assim, com a finalidade de mostrar como, o que são e quais os métodos empregados pelos engenheiros sociais. Assim sendo com o objetivo de obter grau na disciplina, Trabalho de Conclusão de Curso em Direito.

portanto o objetivo proposto no trabalho foi atingido, a pesquisa colaborou para a compreensão dos diferentes tipos de ataques de engenharia social e a demonstração prática de como um ataque desse tipo é realizado.

O trabalho possibilitou demonstrar práticas que podem ajudar os usuários e empresas a não cair em golpes nesse formato. As questões de segurança tornaram-

se muito importantes. Apesar disso, muitas organizações esqueceram que seus próprios recursos humanos estão no centro da maioria das violações de cibersegurança.

Entre as práticas de ataque está a engenharia social, que encontrou um grande terreno para ser explorado, dentre eles, Phishing, Pretexting, Baiting e a inteligência artificial. Sendo técnicas muito comuns usadas em ataques virtuais, explorando os diversos sentimentos humanos, sem a necessidade apenas de técnicas de hacking.

Não se trata somente de proteger nossos equipamentos eletrônicos com programas de antivírus, as pessoas devem saber como o cibercriminoso se comporta, pois, um simples convite em uma rede social pode comprometer a segurança, ao demonstrar que um usuário mesmo sem conhecimento profundo de programação pode causar grandes prejuízos para pessoas e até mesmo, grandes empresas e sites governamentais.

O sistema de segurança não está relacionado apenas à tecnologia em si, mas também aos processos por trás dela. Por mais avançada que seja a tecnologia, ela não servirá de nada se os fatores humanos não forem levados em consideração, treinados e preparados para enfrentar tais possíveis cenários.

É preciso conscientizar as pessoas de que elas podem estar sendo observadas e que podem acabar se tornando um potencial alvo de engenharia social, assim podendo ser ponto chave para o criminoso, se prejudicando e tendo experiências negativas no meio digital.

4. REFERÊNCIAS

ALLEN, Malcolm. Social Engineering: **A Means to Violate a Computer System**. SANS Institute InfoSec Reading Room. [S.l.], 13 f., Jun. dec. 2006. Disponível em: <http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violatecomputer-system_529>. Acesso em: 02 jun. 2024.

BRASIL. **Lei nº 11.384, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da república, [2018], Disponível em:

https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 de nov. de 2024.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, 30 nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/ato2011-2014/2012/lei/l12737.htm. Acesso em 08. nov. 2024.

BRASIL, 2021. **Lei nº 14.155, DE 27 DE MAIO DE 2021.** Brasília, 27 de maio de 2021; 200º da Independência e 133º da República. Disponível em: http://www.planalto.gov.br/ccivil_03/ato2019-2022/2021/lei/L14155.htm. Acesso em: 23. out. de 2024.

BASTOS, C.A. **Segurança da Informação vs. Engenharia Social:** Como se proteger para não ser mais uma vítima. Artigo apresentado à Banca examinadora do Centro Universitário do Distrito Federal - UDF, como requisito parcial para obtenção do grau de bacharel em Sistemas de Informação – Brasília, 2010.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais.** 1ª ed. Rio de Janeiro: Brasport, 2014., p.6.

LIMA, Daniela. Um em cada quatro brasileiros perdeu dinheiro em golpes digitais nos últimos 12 meses, diz pesquisa. **G1.** 30/09/2024. Disponível em: <https://g1.globo.com/politica/blog/daniela-lima/post/2024/09/30/um-em-cada-quatro-brasileiros-perdeu-dinheiro-em-golpes-digitais-nos-ultimos-12-meses-diz-pesquisa.ghtml>. Acesso em: 03/11/2024.

GONÇALVES, G. V.C; OGAWA, K.R.L; LIMA, M.A. **Engenharia Social e a Segurança da Informação.** Artigo apresentado como requisito para conclusão do curso de Bacharelado em Sistemas de Informação pelo Centro Universitário do Planalto Central Aparecido dos Santos – Uniceplac. Gama-DF 06/2022.

LUCAS Agrela. Vazamento de dados de "220 milhões de brasileiros" não aconteceu da noite para o dia. **Exame.** 2021. Disponível em: <https://exame.com/tecnologia/vazamento-de-dados-de-220-milhoes-de-brasileiros-nao-aconteceu-da-noite-para-o-dia/> . acesso em 14 mar 2024.

MARCELO, Antonio; PEREIRA, Marcos. **A Arte de Hackear Pessoas.** Rio de Janeiro: Brasport, 2005., p.3.

MARCIANO, J.L.M; LIMA, M. L. **O enfoque social da segurança de informação.** 2006., p.14.

PINHEIRO, Patrícia Peck. **Direito digital.** 4ª ed. São Paulo: Saraiva, 2010., p.36.

PIPKIN, Donald L. Halting the hacker: **a practical guide to computer security.** 2nd ed. Upper Saddle River: Pearson Education, 2003.

QUINTINHO Sociedade de Advogados. A nova lei Carolina Dieckmann. **Jusbrasil**. 2012. Disponível em: <https://www.jusbrasil.com.br/artigos/a-nova-lei-carolina-dieckmann/121823244> . Acesso em 12 mar 2024.

SOUZA, F.B. **usuário, o elo mais fraco da segurança da informação**. UniALFA Faculdade de Umuarama. v. 3 n. 03 (2022): Revista Scientia Alpha. 2022. Acesso em: 02 JUN. 2024.

SEGINFO. **Conheça o SET: Social-Engineer Toolkit**. 22 set.2010. Disponível em:<<https://seginfo.com.br/2010/09/22/conheca-o-set-social-engineer-toolkit-2/#:~:text=O%20Social%20Engineering%20Toolkit%20%C3%A9,ataques%20relacionados> >. Acesso em 5 set.2024.

MITNICK, Kevin D.; SIMOM, William L. A arte de enganar. Pearson Education, São Paulo: 2003.