ENGENHARIA SOCIAL NA ERA DIGITAL: MITIGANDO RISCOS PARA OS IDOSOS

Fabiano Pontes Pereira da Silva
Mestre em Ciência da Computação pela UFPE. Neuropsicopedagogia em formação. Professor pesquisador na Faculdade de Tecnologia – Fatec Senai MT; docente no Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso – IFMT.
DOI: http://lattes.cnpq.br/6710550167962984.
E-mail: fabiano.silva@fatecsenaimt.ind.br.

Nauam Belo Oliveira
Graduado em Análise e Desenvolvimento de Sistemas pela FATEC-SENAI MT; Pós-Graduando em Cibersegurança e Governança em Tecnologia da Informação; Atualmente na Superintendência de Arquivo Público – SEPLAG.
E-mail: nauam.oliveira@mt.estudante.senai.br.

Resumo: O presente trabalho teve como finalidade apresentar o contexto da engenharia social, assim como seus efeitos em pessoas com conhecimentos modestos em tecnologia. Engenharia Social é a capacidade de conseguir acesso a informações confidenciais e dados sigilosos por meio de técnicas de persuasão, trabalhando a partir da manipulação psicológica. Tais ataques, sejam técnicos ou sociais, estão cada vez mais presentes na era moderna. Pesquisas apontam que houve um grande aumento de acesso às redes por parte dos idosos e de crianças, considerados por muitos alvos preferidos dos criminosos digitais, uma vez que eles são os mais suscetíveis a serem afetados por ameaças cibernéticas. Dessa forma, o objetivo deste trabalho é apresentar medidas eficazes, a fim de que casos recorrentes de golpes, furtos e até clonagem de dados pessoais diminuam com o avançar do tempo, e, junto desses fatos, enfatizar a suma importância que possui para a população em geral ajudando sobre como proceder em situações de ataque cibernético. Para tanto, foi utilizado como método para coleta de dados a pesquisa via questionário online. A análise de dados revelou a necessidade de maior atenção aos idosos e criar estratégias que promovam momentos de conscientização do acesso à internet e segurança na rede, visto que é de grande importância manter esse público alerta a qualquer tentativa de golpe. O resultado

deste trabalho apresenta por meio do estudo realizado a melhor interação da população em geral com o mundo digital através das boas práticas na internet.
Palavras-chave: Engenharia Social. Idosos. Segurança. Dados Pessoais.

Abstract: *The present work aims to present the context of social engineering as well as its effects on people with modest knowledge in technology. Social Engineering is the ability to gain access to confidential information and sensitive data through persuasion techniques, working from psychological manipulation, such attacks, whether technical or social, are increasingly present. in the modern era we live in. In the current world, research has shown that there has been a large increase in access to networks by the elderly and kids, considered by many to be the preferred targets of digital criminals, since they are the most susceptible to being affected by cyber threats. In this way, the objective of this work is effective measures so that recurring cases of scams, thefts and even cloning of personal data decrease over time and together with these facts, emphasize the paramount importance it has for the general population, helping in how to proceed in cyber attack situations. For this purpose, the research via online questionnaire was used as a method for data collection. Data analysis revealed the need to pay more attention to the elderly and create strategies that promote moments of awareness of Internet access and network security, since it is of great importance to keep this public alert to any attempted coup. The result of this work presents, through the study carried out, a better interaction between the general population and the digital world through good practices on the Internet.*
Keywords: *Social Engineering. Seniors. Security. Personal Data.*

INTRODUÇÃO

A internet é sem dúvidas a invenção tecnológica mais avançada e que mais trouxe benefícios à nossa sociedade, entretanto, é necessário estarmos atentos às armadilhas que nela existem e para isso não há outra forma a não ser conhecer medidas eficazes, a fim de encarar situações de riscos às quais os usuários estão expostos.

Com isso, a Engenharia Social ganha grande destaque, uma vez que perpassa por uma técnica empregada de criminosos virtuais, a fim de induzir usuários desavisados a enviarem dados confidenciais. Dessa forma, seus computadores são infectados através de malwares ou também com links para sites enganosos.

O termo "*phishing*" tem origem na palavra em inglês "*fishing*" (pesca), devido à semelhança entre as táticas utilizadas pelos criminosos cibernéticos e a prática de pescar. Além disso, esse crime é o preferido hodiernamente entre vários outros existentes devido a sua fácil manipulação psicológica, visto que os criminosos tentam obter informações confidenciais, como senhas, números de cartão de crédito, informações bancárias ou outros dados pessoais, fingindo ser uma entidade confiável.

Em 1194 a.C. na guerra de Troia, um cavalo de madeira foi deixado junto aos muros de Troia pelos Gregos, supostamente como um presente. Os troianos levaram o cavalo para dentro de seus muros, acreditando que o suposto presente era uma rendição dos gregos. Diante disso compreende-se que os crimes citados anteriormente perpassam por algum presente ou dádiva que traz prejuízo para quem recebeu, ao contrário do que era esperado.

1. DESENVOLVIMENTO

Indubitavelmente, envelhecer é parte do desenvolvimento humano e acontece de forma natural, sendo influenciado por fatores genéticos. Dessa forma, por se tratar de um processo de perdas e maior exposição a doenças, o envelhecimento pode trazer vulnerabilidades, sejam elas sociais, emocionais ou físicas (Irigaray *et al*., 2016).

É de fundamental importância falar sobre o porquê de o idoso ser mais suscetível para se aplicar golpes, uma vez que a falta de conhecimento sobre certas ferramentas que poderiam e podem evitar golpes bancários faz com que os cibercriminosos se aproveitem da

fragilidade desse grupo, e consequentemente conseguem roubar dados pessoais com mais facilidades.

Nesse contexto, segundo o site Folha Universal (2023), o levantamento conduzido pela Confederação Nacional de Dirigentes Lojistas (CNDL) e pelo Serviço de Proteção ao Crédito (SPC Brasil), em parceria com a Offer Wise Pesquisas, revela um notável aumento no acesso à internet entre os brasileiros com mais de 60 anos, com isso criminosos adotaram o espaço virtual devido à sua maior eficiência: seus ganhos de produtividade estão entre as grandes histórias de sucesso da internet (Cohen, 2003).

De acordo com Kevin Mitnick (2003, p. 22) , famoso *hacker* já falecido em 16 de julho de 2023, em seu livro *A Arte de Enganar*, "a Engenharia Social é o uso da manipulação, engano e influência sobre um indivíduo pertencente a uma organização, para que este aceite a um determinado pedido". Esse pedido poderá consistir na divulgação de determinada informação ou o desempenho de determinada tarefa que beneficia o atacante. Dessa forma hacker, ou simplesmente denominado por "engenheiro social" perpassa por uma pessoa com algum tipo de autoridade para requisitar essa informação confidencial, tendo como objetivo final adentrar sistemas.

Nesse contexto, num passado próximo, os ataques a computadores e a outros dispositivos informáticos de rede tinham como finalidade atingir o maior número de sistemas possível e causar o máximo de dano, uma vez que tais ataques não eram, no entanto, movidos por qualquer objetivo específico. Ademais, com a evolução do comércio eletrônico e da própria *World Wide Web*, tem-se observado uma alteração de paradigma, visto que os ataques estão se tornando mais complexos e direcionados. Em suma, um "engenheiro social" basicamente recorre ao telefone ou à internet para enganar as pessoas, levando-as a ceder informação confidencial. Além disso, ao recorrer a essas técnicas, os "engenheiros sociais" aproveitam-se da tendência humana para confiar nas pessoas, levando a que o princípio básico utilizado pela engenharia social seja o de que os humanos são o elo mais fraco dos mecanismos de segurança.

2. METODOLOGIA

Esta pesquisa trata-se do estudo dos danos e do alcance da engenharia social na sociedade brasileira, assim como o conhecimento da cibersegurança e suas boas práticas. Ademais, visa estudar a relação dos crimes cometidos, muitas vezes despercebidos e, também, das atitudes dos usuários em detrimento de algumas situações de risco. A coleta de dados foi realizada por meio de questionário disponibilizado virtualmente. Perguntas como idade, gênero e escolaridade abrem o formulário, a fim de identificar o público respondente. Em seguida o formulário é dividido em duas partes: perguntas gerais e específicas.

Nesse contexto, perguntas gerais perpassam pela frequência na utilização da internet, quais aplicativos são mais acessados pelos internautas para comunicação e se tais oferecem riscos para sociedade. Ademais, em perguntas específicas está presente o nível de conhecimento da população em relação ao tema engenharia social, quais vítimas são mais propícias a serem enganadas, o envio de e-mail e SMS falsos, cliques de forma curiosa ou enganosa em anexos aleatórios contidos nos sites navegados, quais danos que esses cliques podem causar e para finalizar se alguma vítima já sofreu sequestro de dados virtuais, uma vez que os atacantes fingem ser tal pessoa.

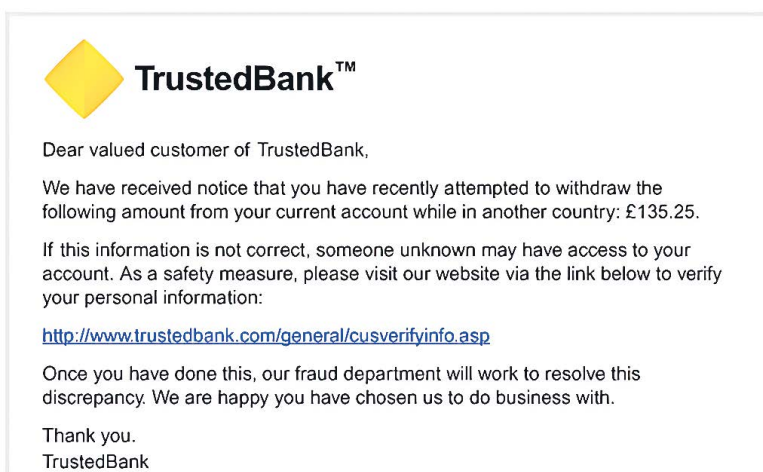
Dessa forma, o objetivo com tal questionário perpassa por avaliar o conhecimento e conscientização que a população atual tem sobre a engenharia social. Concebe-se que o questionário é a técnica de investigação composta por um conjunto de questões que são submetidas a pessoas com o propósito de obter informações sobre conhecimentos, sentimentos, valores, interesses e expectativas. Nesse contexto, construir um questionário consiste basicamente em traduzir objetivos da pesquisa em questões específicas, uma vez que as respostas a essas questões é que irão proporcionar os dados requeridos para descrever as características da população pesquisada ou testar as hipóteses que foram construídas durante o

planejamento da pesquisa. Outrossim, foram utilizadas pesquisas quantitativa e qualitativa.

Destaca-se que é de fundamental importância apresentar quais os principais ataques realizados pelos cibercriminosos, a fim de ludibriar a terceira idade.

Segundo a Microsoft, *phishing* é uma forma de obtenção de dados sigilosos por meio de sites falsos ou clonados. Além disso, o caminho para a aplicação desse método é por um e-mail, no qual o atacante descreve uma situação emergencial, geralmente, para atingir o emocional da vítima e estimular a sua curiosidade. Nesse contexto, ao clicar no link a vítima será direcionada a um site mal-intencionado onde algumas informações secretas poderão ser coletadas. Ademais, outra forma é enviar um malware pelo e-mail e a vítima será infectada ao clicar. Para exemplificar essa fraude, toma-se, por exemplo, a Figura 1, que corresponde a uma mensagem de um banco solicitando informações pessoais, no qual com apenas um clique o atacante tem acesso às informações desejadas.

Figura 1 – Phishing – Roubo de informações

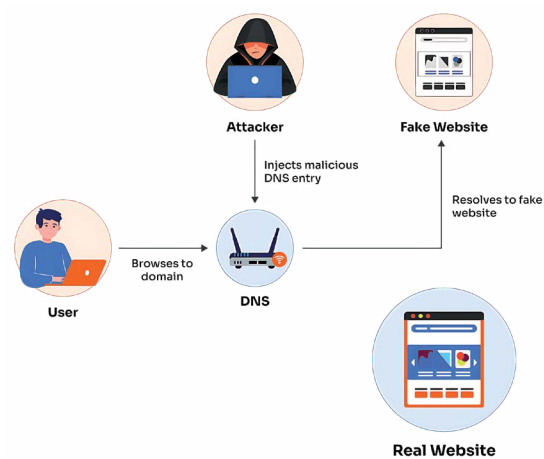


Fonte: The Open University, 2023

Na sequência, o *pharming* é uma técnica muito utilizada que altera o *Domain Name Server* (DNS) da vítima ou o arquivo *hosts* da máquina e quando a pessoa entrar em um site específico será direcionada automaticamente a um site clonado pelo golpista, visto que este será idêntico ao original. Nesse caso, a vítima, com conhecimentos modestos, dificilmente perceberá que ao digitar suas credenciais as informações serão imediatamente repassadas ao *hacker*. Esse tipo de ataque é muito sofisticado. O DNS é o servidor que resolve o nome dos sites, de uma linguagem do usuário em "www.teste.com" para um endereço IP, por exemplo, 200.255.255.27, o qual o servidor web reconhecerá como uma requisição válida.

Nesse contexto, quando esse tradutor de endereços é adulterado, faz com que o endereço de exemplo acima passe a traduzir para um destino malicioso, como exemplo 200.254.125.27. Ademais, a vítima será direcionada sem perceber para o site clonado, no qual até mesmo a URL estará ainda original, mas somente o endereço IP do site que estará falsificado. Portanto, a segunda frente do ataque consistirá no *phishing*, no qual o fraudador criará uma página falsa, idêntica à original, e conseguirá em seguida as credenciais da vítima quando ela inserir e enviar no site clonado.

Figura 2 – *Pharming* – Envenenamento de DNS



Fonte: Valimail, 2023

Continuando, os *pop-ups*, técnica utilizada por muitos websites para anunciar seus produtos e serviços, em estilo propaganda, em uma pequena janela externa ligada ao site. Dessa forma, os *hackers* utilizam tal método para conseguir um clique despercebido da vítima, e quando isso ocorrer ela fará automaticamente o *download* de um *malware* ou será direcionada a uma página falsa, cuja intenção será a coleta de informações sigilosas.

3. DISCUSSÃO E RESULTADOS

Esta pesquisa enfatizou que uma boa parte dos participantes sustenta o seu nível de informação em apenas conhecimento básico sobre a engenharia social ou ouviram falar na mídia alguma coisa sobre esse importante tema, e a maior parte dos respondentes dizem sequer conhecer. Nesse contexto, os participantes possuem um grau adequado de conhecimento sobre todas as fraudes questionadas, e consciência de sua importância, afirmando ser um assunto sério a ser discutido. Ademais, quanto aos tipos de fraudes conhecidas, os participantes, revelam ter recebido a maioria dos ataques perguntados.

O resultado desta pesquisa trouxe à tona alguns problemas antigos, como o alto grau de e-mails falsos recebidos, apesar de que poucos tenham sido atingidos financeiramente. A antiga prática dos trotes telefônicos com assuntos de prêmios, sequestros, em que a grande maioria afirma ter recebido uma ligação falsa. Apesar de grande parte ter consciência dos riscos, há uma vasta prática de envios de SMS com links de sorteios falsos, prêmios, vislumbrando o engano e curiosidade do usuário. Apesar disso também poucos foram efetivamente atingidos pelo roubo de informações e clone de documentos.

O golpe do WhatsApp também tem grande impacto. Enfim a perda de dados ou prejuízo financeiro sofrido pela engenharia social em alguma vertente corresponde a 36% dos participantes, que afirmaram terem sido atingidos. É notório que os ataques que

atiçam a curiosidade dos usuários para que cliquem em notícias e imagens têm uma eficácia surpreendente, além de links ocultos onde os usuários devem clicar em um link para prosseguir na página ou para visualizar tal conteúdo.

Em suma, deduz-se pela pesquisa que os danos causados pela engenharia social são reais e preocupantes, por isso o usuário deve sempre se atentar e suspeitar de quaisquer e-mails ou notícias em redes sociais que aparentam suspeitas, e sempre manter seu sistema de antivírus atualizado.

Não há dúvidas de que a atitude do participante é a forma mais simples de se prevenir a um ataque de engenharia social, desde evitar compartilhar informações pessoais a até sempre garantir veracidade de toda informação pesquisada.

A seguir, uma linha do tempo em conjunto com sua explicação será apresentada, a fim de compartilhar o máximo de conhecimento. Em seguida, os principais princípios e motivos que permeiam a engenharia social.

Portanto, destacam-se as boas práticas, cujo objetivo é mencionar práticas conscientes, em conjunto com pequenas atitudes rotineiras em uma atividade muito atual, o pagamento via Pix, a fim de preservar as informações no mundo virtual. Alguns exemplos serão discutidos abaixo.

Pagamento via PIX, método muito atual por se tratar de uma forma mais prática e rápida de efetuar uma compra. Pessoas estão aderindo a esse novo formato de pagamento, incluindo as pessoas idosas. Porém pessoas idosas ou que não detêm conhecimentos básicos da tecnologia podem acabar sendo vítimas de aproveitadores ou criminosos.

Para se proteger, primeiro é preciso pensar se você realmente precisa compartilhar suas informações com todos. Ademais, cuidado com as pessoas ou perfis falsos que se fazem passar por contatos oficiais e que se oferecem para ajudá-lo e pedir seus dados pessoais. Lembre-se de que redes sociais são baseadas em conexões com pessoas que você não conhece bem e que podem vir a ser contatos

valiosos no futuro. Nesse contexto, destacam-se algumas práticas rotineiras de fundamental importância:

- Garanta que as informações que você está vendo no perfil de alguém sejam realmente verdadeiras.
- Cuidado com mensagens que possuem links, pois eles podem conter algum *malware*, ao serem clicados, seu dispositivo pode ficar vulnerável a futuras invasões.
- Caso haja problemas com seu banco, empresa de cartão de crédito, entre outros, você deve ser extremamente cuidadoso com quem entra em contato. Procure sempre um canal de comunicação confiável. Certifique-se de que o perfil dessas empresas são os canais oficiais.
- Nunca envie dados pessoais por e-mail: seus dados são valiosos, dessa forma, caso receba um e-mail solicitando suas informações pessoais, não responda. Os bancos e outras empresas nunca lhe pedirão que envie dados pessoais, como seu CPF, endereço ou dados de login por e-mail.
- Reforce a segurança de suas redes sociais, como a autenticação de dois fatores.
- Não clique em links ou responda a e-mails que solicitem seu nome de usuário e senha. Essas informações podem ser utilizadas para obter acesso à sua conta.

CONSIDERAÇÕES FINAIS

A partir de todas as bibliografias estudadas para o desenvolvimento deste trabalho, foi possível concluir que a falta de conhecimento necessário referente à engenharia social, em específico para os idosos, gera impactos negativos em um mundo tão digital, assim é de fundamental importância mitigar tais riscos. Nesse contexto, os objetivos alcançados neste estudo perpassam pela contextualização e conscientização de tal tema através de pesquisas qualitativas.

Dessa forma, podemos responder à seguinte pergunta: Como podemos alertar pessoas idosas, que possuem baixo conhecimento tecnológico, sobre os impactos negativos provenientes da vulnerabilidade no ambiente virtual? Através de projetos que visem à formação continuada das pessoas, uma vez que podem desencadear competências e habilidades para garantir uma melhor segurança de todos no ambiente digital e, assim, efetivar boas práticas no uso da internet com segurança.

Além disso, baseado nas pesquisas qualitativas e quantitativas realizadas pode-se afirmar que o grupo da terceira idade é um dos focos preferidos dos cibercriminosos, assim, ensinar e conscientizar os idosos a ter bons hábitos nas redes digitais é de suma importância. A divulgação de medidas eficazes é o principal objetivo, pois quanto mais a população em geral detiver esses conhecimentos, mais segura ela estará para combater essas ameaças cibernéticas.

De modo geral, todos que participaram deste estudo demonstraram interesse na temática do trabalho e em contribuir com suas informações, proporcionando a eles um maior conhecimento do assunto e atualizado sobre os principais riscos que a internet proporciona para aqueles que não possuem nenhuma instrução eficaz. Ainda, foi possível notar com o auxílio das pesquisas que, em conjunto com os idosos, as crianças também são os alvos preferidos dos atacantes, uma vez que aproveitam da ingenuidade deles, que muitas vezes tomam alguma decisão sem o apoio necessário dos responsáveis.

Em suma, o efeito social esperado será de uma sociedade capaz de enfrentar os crimes cibernéticos, através do conhecimento adquirido em estudos como este e de trabalhos futuros que serão realizados, uma vez que se recomenda que sejam feitos estudos longitudinais que avaliem de maneira prospectiva os riscos da engenharia social na era digital.

REFERÊNCIAS

BRASIL REGISTROU mais de 234 milhões de acessos móveis em 2020. GOV.BR. Disponível em: https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/05/brasil-registrou-mais-de-234-milhoes-de-acessos-moveis-em-2020. Acesso em: 20 maio 2024.

BURKART, Daniele Vincenzi Villares. Proteção de dados e o estudo da LGPD. 2021. Disponível em: https://repositorio.unesp.br/items/d3f31333-1765-4c9b-998e-036640aee715 Acesso em: 27 maio 2024.

CERT.BR. **Cartilha de Segurança para Internet**. Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://www.cgi.br/media/docs/publicacoes/1/cartilha-seguranca-internet.pdf Acesso em: 21 abr. 2024.

CNDL. **Número de idosos que acessam a internet cresce de 68% para 97%, aponta pesquisa CNDL/SPC Brasil.** CNDL. 2021. Disponível em: https://site.cndl.org.br/numero-de-idosos-que-acessam-a-internet-cresce-de-68-para-97-aponta-pesquisa-cndlspc-brasil/ Acesso em: 05 maio 2024.

ENGENHARIA SOCIAL: o que é, tipos de ataque, técnicas e como se proteger. Disponível em: https://blogbr.clear.sale/engenharia-social-o-que-e-e-como-se proteger#:~:text=Ou%20seja%2C%20a%20engenharia%20social,a%20partir%20da%20manipula%C3%A7%C3%A3o%20psicol%C3%B3gica. Acesso em: 17 abr. 2024.

FARIA, Thiago Stefanini. **Técnica phishing**: simples, mas eficaz. 2017. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/773 Acesso em: 28 maio 2024.

GERALDES, Ana Vaz. Phishing. Revista da Faculdade de Direito da Universidade de Lisboa, v. 54, p. 87-102, 2013. Disponível em: https://repositorio.ul.pt/handle/10451/59340 Acesso em: 26 maio 2024.

GUEDES, M. S.; PINTO, R. A. N.; FILHO, R. A. B.; NASCIMENTO, P. H.; REIS, D. L.; CEDRAN, P. C.; COSTA, A. P. Crimes e golpes virtuais: desafios enfrentados pelos idosos na era tecnológica. **Observatório de la Economía Latinoamericana**, *[S. l.]*, v. 21, n. 9, p. 14026–14040, 2023. DOI: 10.55905/oelv21n9-190. Disponível em: https://ojs.observatoriolatinoamericano.com/ojs/index.php/olel/article/view/129 3. Acesso em: 20 mar. 2024.

MITNICK, Kevin D. SIMON, William L. **A Arte de Enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. Tradução: Kátia Aparecida Roque. São Paulo: Pearson Education, 2003.

LISKA, Allan; TIMOTHY, Gallo. **Ransomware**: defendendo-se da extorsão digital. Novatec Editora, 2019. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=gf6ZDwAAQBAJ&oi=fnd&pg=PT4&dq=Ransomware:+defendendo-se+da+extors%C3%A3o+digital.+Novatec+Editora,+2019.+Liska,+Allan,+and+Timothy+Gallo.+&ots=SGZiEKgg4J&sig=b0-ySQT2_ukQby0bl6dnOv1Ji00#v=onepage&q=Ransomware%3A%20defendendo-se%20da%20extors%C3%A3o%20digital.%20Novatec%20Editora%2C%202019.%20Liska%2C%20Allan%2C%20and%20Timothy%20Gallo.&f=false. Acesso em: 10 mar. 2024.

O ENVELHECIMENTO na atualidade: aspectos cronológicos, biológicos, psicológicos e sociais. Disponível em: https://www.scielo.br/j/estpsi/a/LTdthHbLvZPLZk8MtMNmZyb/abstract/?lang=pt. Acesso em: 28 maio 2024.

PEREIRA, Cleber Guedes. **Phishing**: Conceitos e ações preventivas aplicadas à empresa. Brasília, 2012. 56 p. Trabalho de Conclusão de Curso (Redes de Computadores) – Centro Universitário de Brasília, Brasília, 2012. Disponível em: https://blog.grupogen.com.br/juridico/postagens/dicas/ataques-e-crimes-ciberneticos/ Acesso em: 23 maio 2024.

PLANALTO. **Lei nº 10.741, de** 1º **de outubro de 2003**. Planalto: Presidência da República Casa Civil Subchefia para Assuntos Jurídicos. 2003. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2003/L10.741compilado.htm. Acesso em: 23 maio 2024.

PLANALTO. **Lei nº 12.737, de 30 de novembro de 2012**. Lei Carolina Dieckmann. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em: 25 maio 2024.

PLANALTO. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral da proteção de dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 maio 2024.

PROTEJA-SE CONTRA phishing Disponível em: https://support.microsoft.com/pt-br/windows/proteja-se-contra-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44**.** Acesso em: 11 maio 2024.

SANTOS, Daniel Pitanga dos. **A Engenharia Social no Brasil e seus riscos**. 2016. Disponível em: http://riut.utfpr.edu.br/jspui/bitstream/1/19455/1/CT_GETIC_V_2015_05.pdf. Acesso em: 20 jan. 2024.

SANTOS, Yuri Rafael de Lima. A engenharia social nas redes sociais online. Mato Grosso: Universidade do Estado de Mato Grosso, 2014. Disponível em: https://www.academia.edu/39700176/A_ENGENHARIA_SOCIAL_NAS_REDES_SOCIAIS_ONLINE20190626_9659_zawg2a. Acesso em: 05 fev. 2024.

SCARPIONI, Agesandro, et al. Desenvolvimento de ambiente virtual para treinamento de idosos para evitar golpes pela Internet. Revista ESPACIOS, v. 37, n. 9, a*ño 2016*. Disponível em: https://www.revistaespacios.com/a16v37n09/16370913.html. Acesso em: 01 maio 2024.

SILVA, Pedro Henrique da. Cibersegurança no novo mundo digital: como alertar os idosos sobre os riscos cibernéticos descendente do phishing na utilização dos smartphones. Disponível em: https://repositorio.ufersa.edu.br/handle/prefix/8860. Acesso em: 01 maio 2024.

WOJAHN, A. S.; MICHAEL, C. da P.; VEIGA, D. J. S. da; LENZ, R.; SILVA, S. G. da; ROSSETTO, T. P.; SANTOS, M. L. dos. The social vulnerability of the elderly against scams in the digital scope. Research, Society and Development, *[S. l.]*, v. 11, n. 11, p. e452111133652, 2022. DOI: 10.33448/rsd-v11i11.33652. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/33652. Acesso em: 20 mar. 2024.