ASSOCIAÇÃO NACIONAL DE
PESQUISA E PÓS-GRADUAÇÃO
INTERDISCIPLINAR EM
SOCIAIS E HUMANIDADES

# CIBERSEGURANÇA E TERCEIRA IDADE: ESTRATÉGIAS DE PROTEÇÃO CONTRA GOLPES VIRTUAIS E DESAFIOS DA INCLUSÃO DIGITAL

Paulus Ralf Neves Soares
ralfnevesss@gmail.com

## RESUMO

A crescente digitalização das relações sociais e econômicas tem impactado diretamente a vida da população idosa, que, ao adentrar o ambiente virtual, depara-se com desafios relacionados à segurança e ao uso consciente das tecnologias. A vulnerabilidade desse grupo frente aos golpes virtuais, especialmente aos ataques de *phishing*, revela a necessidade de compreender as barreiras da inclusão digital e de desenvolver estratégias eficazes de cibersegurança voltadas a esse público. Assim, esta pesquisa tem como objetivo analisar as estratégias de proteção digital que podem contribuir para a segurança da terceira idade, considerando as dificuldades no processo de alfabetização tecnológica e a importância da educação digital. Metodologicamente, trata-se de um estudo de abordagem qualitativa, de caráter exploratório e descritivo, fundamentado em revisão bibliográfica e em uma etapa prática que envolve o mapeamento de iniciativas acadêmicas voltadas à inclusão digital de idosos e a aplicação de questionário estruturado com participantes dessas ações. A análise dos dados será conduzida a partir de técnicas qualitativas de categorização e interpretação das respostas, buscando identificar padrões, percepções e fragilidades nas práticas de segurança digital desse público. Espera-se, com esta pesquisa, contribuir para o aprimoramento de políticas e estratégias de cibersegurança

**Palavras-chave:** Idoso, cibersegurança e tecnologia

## ABSTRACT

The increasing digitalization of social and economic relations has directly impacted the lives of the elderly population, who, upon entering the virtual environment, face challenges related to security and the conscious use of technology. The vulnerability of this group to online scams, especially phishing attacks, reveals the need to understand the barriers to digital inclusion and to develop effective cybersecurity strategies aimed at this population. Thus, this research aims to analyze digital protection strategies that can contribute to the security of the elderly, considering the difficulties in the technological literacy process and the importance of digital education. Methodologically, this is a qualitative, exploratory, and descriptive study, based on a literature review and a practical phase involving the mapping of academic initiatives focused on the digital inclusion of the elderly and the application of a structured questionnaire to participants in these actions. Data analysis will be conducted using qualitative techniques for categorizing and interpreting responses, seeking to identify patterns, perceptions, and weaknesses in the digital security practices of this population. This research is expected to contribute to the improvement of cybersecurity policies and strategies.

Keywords: Elderly, cybersecurity, and technology

## INTRODUÇÃO

As Tecnologias da Informação e Comunicação (TICs) perpassam por diferentes setores da sociedade, o acesso generalizado a computadores, smartphones e à internet modificou não apenas a forma como nos comunicamos, mas também como trabalhamos, nos entretemos e nos relacionamos socialmente (Kamimura; Yaegashi; Yaegashi, 2023). Essa revolução digital, embora tenha trazido inúmeros benefícios, também impôs novos desafios, especialmente no campo da segurança da informação, os idosos por exemplo, fazem parte de uma parcela significativa da população que são alvos recorrentes dos diversos tipos de crimes cibernéticos (Silva; Oliveira, 2024).

A era digital, marcada pela crescente interconexão e dependência de sistemas tecnológicos, trouxe consigo um avanço na comunicação, no comércio e nas relações sociais. Contudo essa evolução também pavimentou o caminho para o crescimento exponencial da criminalidade cibernética, um desafio complexo e multifacetado que transcende as barreiras geográficas e exige abordagens integradas para sua compreensão e combate (Da Silva; De Souza; De Oliveira, 2025).

A cibersegurança tornou-se uma área estratégica e essencial no quesito da

segurança da informação e pode ser definida como o conjunto de práticas, tecnologias e processos voltados à proteção de sistemas, redes e dados contra ataques digitais (Pereira, 2022). No Brasil um dos órgãos responsáveis pelos incidentes (indicadores) cibernéticos é o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). Este órgão tem por objetivo coordenar e integrar as ações destinadas a gestão de incidentes computacionais em órgãos ou entidades da Administração Pública Federal (APF), bem como: prevenir, monitorar e mitigar os incidentes de segurança da informação. Além disso, possui papel importante na articulação para o estabelecimento de diretrizes sobre gestão de incidentes computacionais e a criação de políticas públicas e tomada de decisão (CTIR Gov, 2025).

Um outro órgão ligado à área de resposta a incidentes cibernéticos no país, é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Este órgão contempla um grupo de respostas a incidentes de segurança de responsabilidade nacional e é mantido pelo NIC.br, uma entidade civil de direito privado, sem fins lucrativos, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de sistemas autônomos no país. Tem como missão aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à internet no Brasil. Para atingir a sua missão, o órgão desenvolve ainda diversos serviços prestados a comunidade que incluem a conscientização e desenvolvimentos de boas práticas sobre os problemas de segurança, gestão de incidentes e consciência situacional (CERT.br, 2025).

Dentre os diversos tipos de crimes cibernéticos os mais recorrentes englobam fraudes bancárias realizadas em ambientes online, roubo de identidade digital, ataques por meio de ransomware e práticas de cyberstalking. Para a execução dessas atividades ilícitas, os agentes mal-intencionados valem-se de diversas estratégias, entre as quais se destacam o *phishing*[1], o uso de malwares, o sequestro de dados com demanda de resgate (ransomware) e a engenharia social. O *phishing* se configura como uma das ameaças mais frequentes, dada sua capacidade de manipular usuários e obter informações sigilosas por meio de artifícios enganosos (Rodrigues Guzella Dias; Mirella Farina; Florian, 2024). Para mitigar esses riscos, diversas estratégias de cibersegurança que vão desde a conscientização de evitar clicar em links ou abrir anexos de fontes desconhecidas, passando pelo uso de antivírus atualizados, pela utilização de senhas fortes, até a restrição de acesso a dados sensíveis apenas a pessoas autorizadas, têm sido cada vez mais recomendadas (Do Vale *et al.,* 2022).

No entanto, um grupo social específico que se destaca pela sua maior vulnerabilidade frente a essas ameaças são os idosos. Os idosos costumar ser um grupo altamente vulnerável a crime cibernéticos pois apresentam menor familiaridade com as tecnologias digitais, dificuldades cognitivas naturais do envelhecimento e isolamento social, tornando-se alvos preferenciais para golpistas virtuais, desta forma, os crimes cibernéticos contra os idosos podem ter elevadas consequências para as vítimas tanto no aspecto financeiro quanto no aspecto psicológico e social (Serra *et al.*, 2025).

Reconhecendo toda essa realidade, algumas leis foram criadas para proteger toda a população dos crimes no ambiente digital, ainda de acordo com Serra *et al.* (2025), apesar dos avanços na legislação brasileira contra os crimes cibernéticos nas quais foram criadas as Leis n.º 12.737/2012 conhecida como Lei Carolina Dieckmann e a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei n.º 13.709/2018), ainda existe uma grande lacuna no que diz respeito especificamente a proteção da população idosa.

[1] Golpes cibernéticos fraudulentos onde criminosos se passam por bancos, empresas ou órgãos governamentais para roubar informações confidenciais, como senhas, dados bancários e informações pessoais.

Considerando o cenário apresentado, surgiu o seguinte problema de pesquisa: quais são as principais estratégias de cibersegurança que podem ser implementadas para proteger a terceira idade contra golpes digitais, especialmente o *phishing*, e quais os principais desafios enfrentados por esse grupo na inclusão digital e no uso seguro da internet? Problematizando esta questão, surgem as seguintes questões norteadoras: quais são os principais tipos de golpes digitais, especialmente de phishing, que afetam a população idosa? Quais fatores dificultam a inclusão digital e o uso seguro da internet entre pessoas da terceira idade? Quais estratégias de cibersegurança podem ser implementadas para prevenir e reduzir golpes digitais voltados a esse público? De que forma campanhas educativas podem contribuir para a segurança online da terceira idade? Quais são os desafios e limitações enfrentados por instituições na promoção da proteção digital dos idosos?

No intuito de tentar responder aos questionamentos apresentados, parte-se da seguinte hipótese a ser confirmada ao final da pesquisa: de que a implementação de estratégias de cibersegurança adaptadas à terceira idade possam vir a reduzir a incidência de golpes virtuais, embora o acesso limitado à tecnologia e a falta de educação digital continuem sendo desafios significativos a serem enfrentados por esse grupo.

## FUNDAMENTAÇÃO TEÓRICA

O crescimento exponencial da quantidade de usuários que utilizam a internet, bem como a ampliação das diversas atividades realizadas em ambiente digital, fez com que a cibersegurança se tornasse uma área crítica e estratégica para a proteção de dados e para a integridade das operações realizadas no ciberespaço (Ferreira, 2021).

De acordo com o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) a segurança cibernética pode definida como:

> (...) ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (Brasil, 2020, p. 6).

A legislação brasileira tem avançado significativamente no campo da cibersegurança, com o objetivo de garantir a proteção de dados, a privacidade dos usuários e a integridade das redes e sistemas.

O Marco Civil da Internet, Lei n.º 12.965/2014 (Brasil, 2014) é considerado o marco legal da internet no Brasil, estabelecendo princípios e garantias fundamentais. De acordo com o artigo 7º, “o acesso à internet é essencial ao exercício da cidadania”, sendo garantido ao usuário a inviolabilidade da intimidade, da vida privada e da confidencialidade das comunicações. Além disso, a lei prevê que os provedores de serviços devem adotar medidas de segurança compatíveis com os riscos envolvidos, reforçando a importância de políticas técnicas de proteção de dados.

A Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei n.º 13.709/2018) regulamenta como dados pessoais devem ser tratados, obrigando tanto o setor público quanto o privado a adotar medidas de segurança para proteger informações sensíveis. Conforme o artigo 46 da LGPD:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de

> destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (Brasil, 2018).

Uma outra lei em destaque que diz respeito a crimes cibernéticos é a Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, ela tipifica crimes relacionados à invasão de dispositivos eletrônicos, prevendo pena de detenção para quem realizar qualquer invasão de dispositivo informativo, conforme discriminado em seu artigo 2º:

> 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 (Brasil, 2012).

Por fim, a Lei n.º 14.155, de 27 de maio de 2021, alterou dispositivos do Código Penal para agravar penas relacionadas a crimes cometidos por meios eletrônicos, refletindo a crescente preocupação com a segurança no ambiente digital. De acordo com o § 4º-B no artigo 155 do Código Penal, que trata do furto qualificado por meio eletrônico, prevendo reclusão de quatro a oito anos e multa.

> A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo (Brasil, 2021).

Tais alterações visam não apenas punir mais severamente os crimes virtuais, mas também fortalecer o combate às fraudes digitais que afetam cidadãos e instituições. Dessa forma, observa-se que a legislação brasileira busca não apenas punir ações criminosas no meio digital, mas também prevenir danos, orientar boas práticas e promover um ambiente virtual mais seguro e confiável para todos os cidadãos.

No contexto contemporâneo, em que os crimes cibernéticos ocorrem com frequência e impactam tanto organizações quanto usuários finais, torna-se evidente a necessidade de estratégias robustas de segurança da informação. Dentre as diversas ameaças presentes no ambiente digital, os ataques de *phishing* destacam-se como uma das mais recorrentes, evidenciando a urgência de implementar mecanismos eficazes de detecção e prevenção dessas fraudes eletrônicas (De Souza; Tanaka, 2023).

O termo *phishing* vem do inglês “fishing” (pescar), pois os golpistas “lançam iscas” (geralmente por e-mail, mensagens ou sites falsos) tentando “pescar” dados sensíveis (Montagner; Westphal, 2022).

O *phishing* é uma técnica de ataque cibernético utilizado por criminosos para enganar pessoas e levá-las a fornecer informações confidenciais, como senhas, dados bancários ou números de cartão de crédito. Normalmente, essas mensagens se passam por instituições confiáveis como bancos, lojas ou órgãos públicos e contêm links ou anexos maliciosos (Neves, 2022). Ao clicar ou preencher formulários falsos, a vítima entrega suas informações ao criminoso, que pode usá-las para roubo de identidade, fraudes financeiras ou outros crimes. De acordo com a Cisco (2025):

> Phishing é a prática de enviar comunicações fraudulentas que parecem vir de uma fonte legítima e confiável, geralmente por e-mail e mensagens de texto. O objetivo do invasor é roubar dinheiro, obter

acesso a dados confidenciais e informações de login ou instalar malware no dispositivo da vítima. *phishing* é um tipo de ataque cibernético perigoso, prejudicial e cada vez mais comum.

A técnica de ataque cibernético se sofisticou de tal forma que são subdivididas em categorias distintas tais como: *phishing* por E-mail (Email *phishing*), Spear *phishing*, Smishing e Vishing, cada uma com suas respectivas peculiaridades (IBSEC, 2025).

O crescente volume de tentativas de *phishing* no Brasil tem chamado a atenção de instituições especializadas em segurança cibernética, como o CERT.br, que realiza o monitoramento sistemático de páginas falsas associadas a esse tipo de ataque. As estatísticas divulgadas pela entidade evidenciam que os alvos mais frequentes estão agrupados em categorias como Varejo, Financeiro e Governo. Esse cenário evidencia não apenas a sofisticação dos esquemas de engenharia social, mas também a necessidade de estudos aprofundados sobre a eficácia das estratégias de detecção e mitigação de *phishing*, especialmente no contexto brasileiro (Cert.br, 2025).

Apesar da crescente divulgação de alertas sobre golpes digitais, como os relatados, o número de vítimas de *phishing* permanece elevado, o que evidencia uma lacuna entre o acesso à informação e a real compreensão dos riscos. Muitos usuários ainda não reconhecem os sinais comuns de páginas falsas, como erros sutis em URLs, ausência de certificados de segurança ou abordagens de urgência emocional que são técnicas amplamente utilizadas por cibercriminosos (Da Silva, 2023).

Esse cenário revela a necessidade de programas educativos que ultrapassem ações pontuais de conscientização e se consolidem como processos formativos contínuos, interdisciplinares e adaptáveis a diferentes perfis de usuários. Além disso, é essencial que tais programas envolvam não apenas aspectos técnicos, mas também questões sociais, comportamentais e éticas da segurança digital, promovendo a construção de uma cidadania crítica no ciberespaço (Souza Britto; Preuss; Da Cruz, 2023). Um grupo etário que vem sofrendo bastante com ataques cibernéticos são os idosos.

Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE, 2022), no Brasil de acordo com os dados do censo de 2022 o número de pessoas com 65 anos ou mais de idade cresceu 57,4% em 12 anos, diante desse crescimento populacional dos idosos acentua a preocupação com a segurança digital devido as limitações ao usar a tecnologia, incluindo as dificuldades com as interfaces digitais.

A vulnerabilidade dos idosos a ataques de *phishing* está diretamente relacionada a fatores sociais e tecnológicos. Muitos idosos não tiveram contato com tecnologias digitais ao longo da vida e, por isso, apresentam maior dificuldade para reconhecer sinais comuns de fraudes online, como URLs falsificadas, mensagens com erros gramaticais ou solicitações suspeitas de dados pessoais. Além disso, há uma tendência maior de confiar em mensagens que aparentam vir de instituições oficiais, como bancos, serviços públicos ou órgãos previdenciários, o que aumenta significativamente o risco de serem enganados. Essa falta de familiaridade com o ambiente digital, combinada com o uso limitado de ferramentas de proteção, como autenticação em dois fatores ou antivírus atualizados, contribui para tornar essa população um alvo preferencial para criminosos virtuais (Da Silva *et al.*, 2023).

Além das barreiras tecnológicas, fatores emocionais e sociais também tornam os idosos mais suscetíveis ao *phishing*. O isolamento social, comum entre pessoas idosas, pode levá-las a buscar mais interações e, consequentemente, a responder a mensagens ou ligações de origem duvidosa. A confiança excessiva em figuras de autoridade ou o desejo de manter relações interpessoais pode ser explorado por golpistas que se passam por familiares, representantes de instituições ou atendentes de suporte técnico. Esses aspectos tornam a abordagem de *phishing* especialmente eficaz, pois apela não apenas à ignorância técnica, mas também à dimensão afetiva e relacional da vítima. Assim, a vulnerabilidade dos idosos é multifacetada e exige uma

resposta que vá além da tecnologia, abrangendo também educação digital, apoio social e políticas públicas voltadas à proteção dessa população (Serra *et al.*, 2025).

## Contribuições Específicas do Estudo, Etapas de sua Trajetória e Perspectiva Interdisciplinar

O presente estudo oferece contribuições relevantes ao aprofundar a compreensão sobre os desafios da cibersegurança enfrentados pela população idosa no Brasil, articulando avanços tecnológicos, marcos regulatórios, fatores socioculturais e processos educativos. Seu percurso investigativo foi construído em etapas que integram referenciais da Tecnologia da Informação, do Direito Digital, da Psicologia Social, da Gerontologia e da Educação, demonstrando uma perspectiva claramente interdisciplinar.

A primeira etapa da trajetória consistiu no mapeamento do cenário contemporâneo da cibersegurança a partir de documentos oficiais, legislações específicas e análises técnicas. Consideraram-se normas como o Marco Civil da Internet, a Lei Geral de Proteção de Dados pessoais (LGPD), a Lei Carolina Dieckmann e a Lei n.º 14.155/2021, que reforçam a responsabilidade institucional pela proteção de dados e a punição de crimes eletrônicos. Essa base permitiu compreender como o Estado tem estruturado mecanismos de proteção diante da crescente sofisticação dos ataques no ambiente digital.

Em uma segunda etapa, o estudo voltou-se para a caracterização dos ataques de phishing como ameaça central ao cotidiano dos usuários, especialmente dos idosos. Foram analisadas definições técnicas, classificações e tendências de evolução desses ataques, considerando autores como Montagner, Westphal (2022), De Souza e Tanaka (2023), além de dados de instituições especializadas como o CERT.br e a Cisco. Esse levantamento evidenciou que o phishing permanece como uma prática recorrente, sustentada por técnicas de engenharia social, manipulação emocional e replicação de interfaces digitais.

A terceira etapa incorporou análises sociopsicológicas e gerontológicas, aprofundando os fatores que tornam os idosos especialmente vulneráveis às fraudes digitais. Foram considerados aspectos como a limitada familiaridade com tecnologias, dificuldades com interfaces digitais, confiança excessiva em fontes de aparência oficial, isolamento social e uso restrito de mecanismos de proteção. Estudos recentes (Da Silva et al., 2023; Serra et al., 2025) reforçam que a vulnerabilidade dos idosos é multifatorial e envolve tanto barreiras tecnológicas quanto dimensões emocionais e relacionais.

Por fim, o estudo avançou para uma quarta etapa, que aborda a necessidade de programas educativos contínuos, integrando saberes técnicos, pedagógicos e sociais. A partir da perspectiva defendida por Souza Britto, Preuss e Da Cruz (2023), compreende-se que a simples disseminação de alertas não garante a redução de golpes: é preciso promover letramento digital crítico, formação para o uso seguro da tecnologia e ações articuladas entre políticas públicas, instituições financeiras, órgãos de segurança e espaços educativos formais e não formais.

Dessa forma, a principal contribuição deste trabalho reside em evidenciar que a proteção dos idosos contra golpes virtuais exige uma abordagem interdisciplinar, que não se restringe a soluções tecnológicas, mas envolve educação, legislação, psicologia, inclusão social e cuidados gerontológicos. Ao conectar esses campos, o estudo propõe caminhos para práticas preventivas mais eficazes, capazes de promover autonomia digital, reduzir vulnerabilidades e fortalecer a cidadania no ciberespaço.

## Considerações finais

A crescente incidência de golpes virtuais evidencia que a segurança digital deixou de ser apenas um tema técnico para se tornar uma questão social, educacional e cidadã. Os dados apresentados ao longo deste estudo demonstram que, embora o arcabouço jurídico brasileiro tenha avançado significativamente com o Marco Civil da Internet, a LGPD, a Lei Carolina Dieckmann e legislações complementares, tais instrumentos ainda não são suficientes para garantir a proteção integral dos usuários mais vulneráveis, como a população idosa. Os ataques de phishing, especialmente sofisticados e baseados em engenharia social, revelam que a defesa contra crimes cibernéticos ultrapassa a dimensão normativa e demanda estratégias interdisciplinares.

A análise realizada permite concluir que a vulnerabilidade dos idosos decorre de uma combinação de fatores tecnológicos, cognitivos, emocionais e socioculturais. Não basta ampliar mecanismos de segurança ou investir em soluções técnicas: é indispensável promover processos formativos contínuos que desenvolvam competências digitais, senso crítico e autonomia no uso das tecnologias. A educação digital, quando articulada a políticas públicas de inclusão e ao apoio social, torna-se um pilar essencial para fortalecer a resiliência dessa população frente às ameaças do ciberespaço.

Ao integrar perspectivas da Tecnologia da Informação, da Gerontologia, da Psicologia Social e da Educação, este estudo reforça que o enfrentamento aos golpes virtuais exige ações coordenadas entre Estado, instituições financeiras, profissionais da educação e sociedade civil. Proteger os idosos no ambiente digital significa reconhecer sua participação ativa na vida social contemporânea e assegurar que o exercício da cidadania, condicionado cada vez mais ao uso da internet, seja realizado com segurança, dignidade e confiança.

Assim, as reflexões aqui apresentadas contribuem para ampliar o debate sobre cibersegurança e vulnerabilidade digital na terceira idade, além de apontar caminhos para pesquisas futuras e para o desenvolvimento de práticas educativas e políticas de proteção mais eficazes. Garantir um ambiente digital seguro para os idosos é, antes de tudo, garantir um ambiente digital mais seguro para toda a sociedade.

## Referências

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos (Lei Carolina Dieckmann). **Diário Oficial da União**: seção 1, Brasília, DF, p. 1, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 25 maio 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União:** seção 1, Brasília, DF, p. 1, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 maio 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de

Dados Pessoais – LGPD. **Diário Oficial da União:** seção 1, Brasília, DF, p. 1, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 maio 2025.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para agravar penas de crimes cometidos por meio da internet. **Diário Oficial da União:** seção 1, Brasília, DF, p. 1, 28 maio 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 25 maio 2025.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Cartilha de gestão de segurança da informação.** Brasília, DF: GSI/PR, 2020. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/cartilha-de-gestao-de-seguranca-da-informacao/CartilhadeSegurancaInformao.pdf. Acesso em: 30 jun. 2025.

CENTRO DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO - CTIR Gov. **Sobre**. CTIR Gov, 2025. Disponível em: https://www.gov.br/ctir/pt-br/ctirgov. Acesso em: 4 jun. 2025.

CERT.br. Estatísticas de Incidentes Reportados. **NIC.br,** 2024. Disponível em: https://www.cert.br/. Acesso em: 4 jun. 2025.

CISCO. O que é *phishing*? **CISCO**, 2025. Disponível em: https://www.cisco.com/site/us/en/learn/topics/security/what-is-phishing.html?dtid=osscdc000283&linkclickid=srch. Acesso em: 25 maio 2025.

DA SILVA, Alends Venus Oliveira *et al.* proteção e segurança para o idoso no meio da tecnologia da informação. **Revista Contemporânea**, v. 3, n. 12, p. 29922-29938, 2023.

DA SILVA, Rodolfo Maravilha Franco; DE SOUZA Carlos Henrique Medeiros; DE OLIVEIRA Fabio Machado. Engenharia Social e Crimes Virtuais: Uma Análise Bibliométrica da Produção Científica. **InterSciencePlace – International Scientific Journal**, v. 20, n. 4, p. 74-87, 2025.

DE SOUZA, Leonardo Correa; TANAKA, Simone Sawasaki. Estudo sobre ataques de phishing e suas técnicas de defesa. **Revista Terra & Cultura: Cadernos de Ensino e** Pesquisa, v. 39, n. especial, p. 90-95, 2023.

DO VALE, Fabio *et al.* A segurança digital nas pequenas e médias empresas: desafios e possíveis soluções. **Revista Latino-Americana de Estudos Científicos,** v. 3, n. 16, p. 1-9, 2022.

DOS SANTOS, Fernanda Marsaro. Análise de conteúdo: a visão de Laurence Bardin. **Revista Eletrônica de Educação**, v. 6, n. 1, p. 383-387, 2012.

FERREIRA, Sarah Pereira. **Crimes Cibernéticos:** a ineficácia da legislação brasileira. 2021. 31f. Trabalho de Conclusão de Curso (Bacharel em Direito) - Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1709/1/Artigo%20Cientif %c3%adco-%20Sarah%20Pereira%20Ferreira.pdf. Acesso em: 17 jul. 2025.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo: Atlas, 2008.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA – IBGE. **Censo 2022:** número de idosos na população do país cresceu 57,4% em 12 anos. 2023. Disponível em: https://censo2022.ibge.gov.br/noticias-por-estado/38186-censo-2022-numero-de-idosos-na-populacao-do-pais-cresceu-57-4-em-12-anos. Acesso em: 27 maio 2025.

INSTITUTO BRASILEIRO DE CIBERSEGURANÇA – IBSEC. **Ataques de *phishing*:** o que são e como funcionam? 2025. Disponível em: https://ibsec.com.br/ataques-de-phishing-o-que-sao-e-como-funcionam/. Acesso em: 3 jun. 2025.

KAMIMURA, Larissa Nader; YAEGASHI, Solange Franci Raimundo; YAEGASHI, João Gabriel. Sociedade pós-moderna e tecnologias de informação e comunicação: reflexões acerca dos relacionamentos interpessoais na atualidade. **Revista Brasileira de Iniciação Científica**, v. 1, p. e023027–e023027, 13 set. 2023.

MONTAGNER, Antonio S.; WESTPHALL, Carla Merkle. Uma breve análise sobre *phishing*. **Revista ComInG-Communications and Innovations Gazette**, v. 6, n. 1, p. 46-56, 2022.

NEVES, Raquel Alexandra Carvalho. **Vitimação por *phishing*:** um estudo empírico. 2022. Dissertação (Mestrado) - Universidade do Porto, Portugal, 2022.

PEREIRA, Sara Margarida Teófilo. **Cibersegurança:** o Papel da Polícia de Segurança Pública na Prevenção do Cibercrime. 2022. Dissertação (Mestrado) - Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa, 2022.

PICALHO, Antonio Carlos; FADEL, Luciane Maria; GONÇALVES, Alexandre Leopoldo. Expressões de busca e o uso de diferentes operadores avançados de pesquisa em um mecanismo de busca. **Texto Livre**, v. 16, p. e47531, 2023.

PRODANOV, C. C.; FREITAS, E. C. de. **Metodologia do Trabalho Científico**: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. 2. ed. Novo Hamburgo: Universidade Freevale, 2013.

RODRIGUES GUZELLA DIAS, Jhonatan; MIRELLA FARINA, Renata; FLORIAN, Fabiana. Segurança cibernética - estudo das técnicas de ataques cibernéticos (phishing, ransmware, DDOS) de engenharia social e medidas de

prevenção. **Revista Científica Semana Acadêmica**, v. 12, n. 248, p. 1-16, 5 jul. 2024.

SERRA, Francineia Cartaxo da Silva *et al.* A proteção dos idosos contra crimes cibernéticos no Brasil: desafios e soluções jurídicas. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 11, n. 3, p. 2071–2082, 1 mar. 2025.

SILVA, U. P.; OLIVEIRA, M. C. Os crimes cibernéticos e a vulnerabilidade dos idosos. **Revista Eletrônica de Direito**, v. 1, n. 1, p. 34-55, 2024.

SOARES, Márcia Regina Pacheco; GOMES, Heloisa Landim; ISTOE, Rosalee Santos Crespo. Diagnóstico das Atividades Socioculturais no Município de Campos dos Goytacazes/RJ na Percepção de Idosos Participantes. **Revista foco**, v. 16, n. 9, p. e2994, 2023.

SOUZA BRITTO, Melina Carla de; PREUSS, Lislei Teresinha; DA CRUZ, Fabricio Bittencourt. Políticas sociais de inclusão e cidadania digital: O programa de extensão Universidade aberta para a Terceira Idade. **Revista Conexão UEPG**, v. 19, n. 1, p. 1-14, 2023.