# Análise da Vulnerabilidade dos Idosos ao *Phishing*

*Analysis of the Vulnerability of the Elderly to Phishing*

[1]Mariana Nascimento da Silva, [2]Natalia Seguchi Barboza, [3]Sabrina Cabral de Andrade

[1]*Faculdade de Tecnologia Prefeito Hirant Sanazar (Fatec Osasco)*
*mariana.nascimentosilva7@gmail.com*
*https://orcid.org/0009-0009-5228-3990*

[2] *Pontifícia Universidade Católica de São Paulo(PUC-SP)/ Faculdade de Tecnologia Prefeito Hirant Sanazar (Fatec Osasco)*
*natalia.seguchi2001@gmail.com*
*https://orcid.org/0009-0001-8545-7186*

[3]*Faculdade de Tecnologia Prefeito Hirant Sanazar (Fatec Osasco)*
*sabrina.andrade01@fatec.sp.gov*
*https://orcid.org/0009-0000-2189-5139*

*Recebido: 06/08/2025 – Aprovado: 25/09/2025*
*Processo de Avaliação: Double Blind Review*

**Resumo**

**Objetivo:** o *phishing* é uma das práticas criminosas mais comuns na internet, utilizando mensagens, e-mails ou *sites* falsos para capturar dados pessoais e financeiros. Idosos tendem a ser mais vulneráveis devido à menor familiaridade com tecnologias digitais, limitações cognitivas e barreiras de acessibilidade. O objetivo deste estudo é analisar os fatores que tornam a população idosa mais suscetível aos golpes de *phishing* e comparar seu comportamento digital ao de adultos mais jovens.

**Problematização:** Há necessidade de reflexão sobre a importância de atenção aos idosos em relação aos golpes com tecnologia. Portanto a pesquisa busca identificar: quais fatores tornam os idosos mais vulneráveis ao *pishing?*

**Metodologia:** a pesquisa utilizou abordagem quantitativa, por meio de um questionário estruturado em escala Likert aplicado via Google Forms. A amostra foi composta por 217 participantes divididos em dois grupos: adultos de 18 a 59 anos e idosos de 60 anos ou mais. A coleta ocorreu entre novembro de 2024 e março de 2025, permitindo comparar hábitos de segurança digital, percepção de risco e exposição a fraudes entre as faixas etárias.

**Resultados:** Os resultados revelam que idosos verificam menos a autenticidade de e-mails, sendo que apenas 23% sempre checam o remetente. Demonstram menor confiança na identificação de tentativas de *phishing*, menor uso de ferramentas de segurança e reduzida busca por informações sobre prevenção. Embora ambos os grupos reconheçam a crescente sofisticação dos golpes, os idosos apresentam maior dificuldade em diferenciar mensagens legítimas de fraudulentas.

**Contribuições:** a vulnerabilidade dos idosos ao *phishing* resulta da combinação entre dificuldades tecnológicas, limitações cognitivas e baixo letramento digital. O estudo reforça a necessidade de programas de inclusão digital voltados à terceira idade, ações educativas e políticas públicas que fortaleçam a segurança e autonomia desse público no ambiente *on-line*.
**Palavras-chave:** *Phishing*, Idosos, Golpes Virtuais, Segurança Digital, Inclusão Digital

***Abstract***

***Objectives:*** *phishing is one of the most common cybercrimes, using fraudulent emails, messages, or websites to obtain personal and financial information. Older adults tend to be more vulnerable due to limited digital skills, cognitive constraints, and accessibility challenges. This study aims to analyze the factors that increase seniors' susceptibility to phishing attacks and compare their digital security behaviors with those of younger adults.*
***Problem Diagnosis:*** *There is a need for reflection on the importance of paying attention to the elderly in relation to technology-based scams. Therefore, this research seeks to identify: what factors make the elderly more vulnerable to phishing?*
***Methodology/approach:*** *a quantitative approach was adopted using a structured Likert-scale questionnaire applied via Google Forms. The sample included 217 participants divided into two groups: adults aged 18 to 59 and older adults aged 60 or above. Data were collected between November 2024 and March 2025, enabling comparison of security habits, risk perception, and exposure to fraud across age groups.*
***Results:*** *findings show that older adults check email authenticity less frequently, with only 23% always verifying the sender. They report lower confidence in identifying phishing attempts, reduced use of security tools, and less engagement in seeking information about digital threats. Although both groups recognize that phishing scams have become more sophisticated, older adults display greater difficulty distinguishing legitimate from fraudulent messages.*
***Contribution:*** ***t****he increased vulnerability of older adults to phishing is associated with technological limitations, cognitive challenges, and low digital literacy. The study highlights the importance of digital inclusion programs, educational initiatives, and public policies aimed at strengthening the autonomy and online safety of this population.*
***Keywords****: Phishing, Older Adults, Online Scams, Digital Security, Digital Inclusion.*

## 1 Introdução

Recentemente, há enorme discussão sobre a desenfreada elevação de golpes aplicados na internet. Infelizmente, foram desenvolvidas várias modalidades criminosas que podem diferir na forma de ataque ou na vítima escolhida, porém todas possuem uma única meta: roubar recursos financeiros e/ou dados de pessoas que estejam em um momento de desatenção.

No trabalho em questão, o golpe abordado é o *phishing*. Para Kosinski (2024), *phishing* é uma forma de ataque virtual que utiliza e-mails, mensagens de texto, ligações telefônicas ou *sites* falsos para enganar indivíduos e fazer com que revelem informações pessoais, instalem malware ou se tornem vulneráveis a outras ameaças digitais.

Globalmente, a Kaspersky (2023) registrou 286 milhões de bloqueios de *phishing* no período de 12 meses – apresentando um aumento de 617% em comparação com os 12 meses anteriores e uma média de 544 ataques por minuto. O relatório pontua que o Brasil foi um dos países com maior incidência de *phishing*, com 134 milhões de tentativas de ataque.

Diante dos riscos, a presente pesquisa busca identificar se os idosos realmente podem ser considerados como o grupo mais vulnerável ao *phishing*, seja em razão de seu despreparo frente à tecnologia, em sua maioria, ou da diminuição de suas atividades cognitivas devido à idade avançada.

## 2 Referencial Teórico

### 2.1 *Phishing*: a Modalidade de Golpe

Kosinski (2024) ressalta que em um golpe de *phishing* típico, um criminoso virtual se apresenta como uma pessoa ou entidade confiável, como um amigo, um colega, uma figura de autoridade ou um representante de uma empresa conhecida. O golpista envia uma mensagem que leva a vítima a realizar ações como pagar uma fatura, abrir um anexo ou clicar em um link. A "fatura" pode transferir recursos para a conta do golpista. O anexo pode instalar um ransomware no dispositivo da vítima. Já o *link* é capaz de direcioná-la para um *site* que coleta informações sensíveis, como números de cartões de crédito, dados bancários, credenciais de login ou outros dados pessoais.

Conforme Montagner e Westphall (2022), o termo *phishing* faz alusão à palavra em inglês *fishing*, ou seja, pescaria. O ”ph” é derivado de sofisticado, do inglês *sophisticated*, por conta das técnicas sofisticadas que os criminosos usam para se distinguir da atividade mais simples de pescar. Neste cenário, a vítima faria o papel do peixe que morde a isca e o pescador seria o golpista.

Esta modalidade de golpe surgiu por volta de 1995, sendo citada pela primeira vez em 02 de janeiro de 1996. A menção ocorreu em um grupo de notícias chamado AOHell. De acordo com Phishing.org, na época, o *phishing* ocorria por meio do roubo de senhas de usuários e do uso de algoritmos para criar números de cartão de crédito aleatórios.

Com o passar dos anos, o *phishing* se adaptou a diversas inovações, como os sistemas de pagamentos *on-line* em 2001, criptomoedas em 2008, anexos de e-mail contendo malware em 2013 e, mais recentemente, em 2020 houve a circulação de golpes contendo *fake news* relacionadas à pandemia, à quarentena, ao *home office*, dentre outros (Phishing.org).

De acordo com Valente (2021), em 2020 o Brasil ficou em primeiro lugar em tentativas de phishing, com 19,9% dos usuários clicando em links fraudulentos. Portugal ficou em segundo (19,7%), seguido pela França (17,9%) e Tunísia (17,6%). Um levantamento da Kaspersky mostrou que os ataques aumentaram 120% no Brasil entre fevereiro e março de 2020. Os golpistas se faziam passar por empresas conhecidas, como a Amazon.

O WhatsApp foi uma das principais ferramentas usadas para esses golpes, que incluíam promessas de prêmios e mensagens falsas sobre a pandemia, como auxílio emergencial e vacinação. Apesar de uma redução em relação a 2019, quando mais de 30% dos brasileiros tentaram abrir *links* de *phishing*, a situação ainda é preocupante.

Já com relação ao *spam*, ele representou 50% do tráfego de e-mails em 2020, mas houve uma queda de 6,14% em relação ao ano anterior. O Brasil foi responsável por 3,26% do *spam*, enquanto a Rússia liderou com 21,27%. No total, foram enviados 183,4 milhões de anexos maliciosos durante o ano (Valente, 2021).

Uma das maiores especialistas em segurança digital, a Kaspersky registrou 286 milhões de bloqueios de *phishing*, o que equivale a uma média de 544 ataques por minuto. O Brasil liderou o número de tentativas, com 134 milhões, seguido por México (43 milhões) e Peru (31,5 milhões). Quase 43% dos golpes visavam dados financeiros, sendo 28,4% focados em temas bancários.

Conforme a Kaspersky (2023), com a retomada da economia e o aumento do uso da Inteligência Artificial, as tentativas de golpes de *phishing* cresceram 617% e os trojans bancários - plataformas que fingem ser os canais oficiais de instituições financeiras - aumentaram 50% entre junho de 2022 e julho de 2023.

Pessoas de todas as idades, gêneros, etnias e classes sociais estão suscetíveis ao *phishing*. Porém, uma matéria do portal Serasa detalha que os idosos se destacam nesse quesito: "[...] os golpistas também se aproveitam dos idosos por meio de fraudes *on-line* e por e-mail, na tática de *phishing*. Eles enviam mensagens de e-mail falsas, projetadas para parecerem legítimas [...] essas mensagens podem solicitar informações pessoais, senhas, números de cartão de crédito ou, até mesmo, induzir os idosos a clicar em *links* maliciosos que infectam seus dispositivos com malware. Essas fraudes *on-line* visam roubar informações sensíveis e financeiras ou obter acesso a contas e dados pessoais dos idosos." (Brenol, 2023)

Segundo Cardoso (2023), durante a pandemia, o isolamento social levou muitos idosos a procurar mais frequentemente a internet para se comunicar com familiares e amigos, o que os tornou mais suscetíveis a ataques de *phishing*. O uso de mensagens fraudulentas, imitando empresas ou bancos, tornou-se comum, com o objetivo de coletar informações como senhas e números de cartões de crédito.

Um estudo da Febraban (2022) revelou que o isolamento social incentivou muitos idosos a acessar mais a internet para manter contato com familiares, ampliando sua exposição a ameaças cibernéticas, como mensagens falsas em nome de bancos ou empresas, com a intenção de roubar dados confidenciais. Já Almeida (2020) aponta que, durante a quarentena, as tentativas de golpes financeiros, como *phishing*, aumentaram em mais de 80%, impulsionadas pela vulnerabilidade dos idosos, que muitas vezes possuem menos familiaridade com práticas de segurança digital.

## 2.1 Características que Reforçam a Vulnerabilidade dos Idosos

Nos Estados Unidos, cerca de um em cada seis habitantes tem 65 anos ou mais, e essa porcentagem deve crescer. Os adultos mais velhos geralmente ocupam posições de poder e têm economias de aposentadoria acumuladas ao longo de suas vidas – o que os torna alvos atraentes para exploração financeira, segundo Ebner e Pehlivanoglu (2024).

Somado a isso, Cardoso (2023) afirma que a vulnerabilidade dos mais velhos ao *phishing* é acentuada por sua falta de familiaridade com as tecnologias digitais e a internet. Um estudo recente mostra que houve um aumento de 97% nos casos de *phishing* entre 2021 e 2022. Além disso, de acordo com um levantamento realizado pelo Procon de Alagoas, em 2023,

houve um aumento de 140% nas reclamações relacionadas a empréstimos consignados fraudulentos, sendo o *phishing* uma das principais modalidades utilizadas para aplicar golpes.

Quanto às ligações neurais e sua relação com a vulnerabilidade a golpes, um fator importante é a consciência interoceptiva: a capacidade de ler com precisão os sinais do nosso próprio corpo, como um "pressentimento". Essa consciência está correlacionada com uma melhor detecção de mentiras em adultos mais velhos.

De acordo com Ebner e Pehlivanoglu (2024), os idosos explorados financeiramente tinham um tamanho significativamente menor de ínsula – uma região do cérebro fundamental para integrar os sinais corporais com os sinais ambientais – do que os idosos que foram expostos à mesma ameaça, mas a evitaram. A atividade reduzida da ínsula também está relacionada a uma maior dificuldade em captar pistas que fazem alguém parecer menos confiável.

O aumento do uso de dispositivos móveis e internet para realizar transações financeiras coloca desafios para aqueles que não acompanharam as inovações tecnológicas. Segundo Juvenassi (2021), muitos idosos enfrentam dificuldades e preconceitos ao navegar em interfaces digitais complexas e ao lidar com procedimentos de segurança, como múltiplas camadas de autenticação. Isso aumenta o risco de cometer erros, o que os torna alvos preferidos de golpes *on-line.*

As interfaces digitais, muitas vezes, não consideram as necessidades de acessibilidade dos idosos, como o uso de letras pequenas e processos complicados, o que agrava sua vulnerabilidade. Anjos e Gontijo (2015) ressaltam que os problemas como a dificuldade em compreender ícones, funções e comandos, além da navegação desordenada, tornam a interação com dispositivos móveis desafiadora para essa população. Esses obstáculos, somados à falta de familiaridade com as tecnologias, aumentam a suscetibilidade dos idosos a fraudes, já que os criminosos se aproveitam dessas fragilidades para enganá-los. A ausência de uma interface intuitiva e amigável, aliada à falta de destreza dos idosos, contribui significativamente para que sejam mais propensos a cair em golpes.

Essa vulnerabilidade, contudo, não se restringe apenas a idosos com limitações cognitivas mais severas. James, Boyle e Bennett (2014) demonstraram que, mesmo entre idosos sem demência, fatores como menor bem-estar psicológico, baixo suporte social e reduzida literacia financeira e em saúde estão fortemente associados à maior suscetibilidade a golpes. Inclusive, mesmo que sejam leves, sentimentos como a solidão e a vulnerabilidade psicológica estão associadas à vitimização. Mensagens fraudulentas são intencionalmente projetadas para explorar vulnerabilidades psicológicas e necessidades não atendidas, e indivíduos solitários podem estar mais dispostos a interagir com golpistas que oferecem validação emocional e companhia, de acordo com DeLiema (2024). Isso evidencia que a vulnerabilidade resulta de um conjunto de elementos psicológicos, sociais e comportamentais, e não apenas da relação com a tecnologia.

Fraga (2023) sintetiza que programas de inclusão digital são fundamentais para mitigar esses riscos, ensinando idosos a reconhecer fraudes e a navegar de forma mais segura na internet. A educação digital específica para esse grupo etário, incluindo o uso seguro de dispositivos e a identificação de sinais de golpe, é apontada como uma das melhores ferramentas de prevenção.

## 2.2 Medidas de Prevenção e Educação

Para Fuentes (2021), o aumento nos casos de violência contra idosos, seja física, psicológica ou financeira, é reflexo da falta de políticas públicas voltadas para esse grupo. A ausência de programas educativos que ensinem os idosos a reconhecer e evitar esses golpes é um dos principais fatores que contribuem para o aumento de fraudes dessa natureza.

Marichal (2022) enfatiza a importância de proteger os dados pessoais, apontando algumas práticas fundamentais: fazer *backups* regulares dos dados, especialmente os guardados na nuvem, criar senhas complexas utilizando uma mistura de caracteres especiais, letras maiúsculas, minúsculas e números, evitando palavras comuns ou informações pessoais, e ativar a autenticação de dois fatores sempre que possível.

Além disso, é aconselhável saber identificar o *phishing* e, de acordo com o Cloudflare (n.d), ele pode ser identificado por vários sinais:

- Primeiramente, ele pode falhar nas verificações de segurança como SPF, DKIM ou DMARC, o que indica que sua origem não é confiável;
- O endereço de e-mail do remetente costuma ser semelhante, mas não idêntico ao de uma empresa legítima, como pequenas variações no domínio;
- A saudação geralmente é genérica, sem mencionar o nome da pessoa, e o e-mail costuma criar uma sensação de urgência exagerada para que a vítima tome uma ação rápida, como clicar em um *link* ou fornecer informações;
- Erros gramaticais ou de ortografia no corpo da mensagem são comuns em tentativas de *phishing*, e os *links* no e-mail podem redirecionar para *sites* maliciosos, em vez de levar ao *site* oficial da empresa.

Embora os jovens já tenham se inserido no ambiente *on-line*, muitos idosos tiveram que se adaptar rapidamente durante o auge da Covid-19, sem ter acesso à alfabetização digital, que é o primeiro contato com o uso dessas tecnologias.

Menezes, Couto e Santos (2019) afirmam que a alfabetização digital é o primeiro contato com o universo digital, enquanto o letramento digital vai além, envolvendo a compreensão e o uso eficiente dos dispositivos. A falta de acesso a essas tecnologias pode aumentar a vulnerabilidade dos idosos, afetando sua saúde e interação social. Estudos mostram que o uso de Tecnologias de Informação e Comunicação (TICs) está cada vez mais presente entre os idosos, especialmente para comunicação e acesso à internet.

A inclusão digital traz benefícios psicológicos e sociais, como a redução da solidão e a promoção da independência. Durante a pandemia, o uso de dispositivos digitais ajudou os idosos a mantê-los ativos, participando de atividades físicas e culturais *on-line*, além de melhorar o bem-estar e a saúde mental. Portanto, investir no letramento digital de idosos os torna aptos a compreender as facetas por trás das redes e, assim, pode reduzir sua suscetibilidade a golpes que utilizam a internet como meio.

Complementando essa análise, estudo recente publicado na Frontiers in Public Health aplicou a Teoria da Atividade Rotineira ao contexto *on-line*, destacando que a vulnerabilidade ocorre em dois estágios: a exposição e a vitimização. Chen et al. (2025) identificaram que aspectos como a frequência de uso de redes sociais, a quantidade de aplicativos instalados e,

sobretudo, a presença de familiares jovens atuando como “guardiões sociais” podem reduzir significativamente a probabilidade de vitimização. Esse achado reforça a importância de políticas e ações que envolvam não apenas os idosos, mas também suas redes de apoio no combate a fraudes digitais.

Um estudo da Universidade da Flórida mostrou que pessoas mais velhas correm maior risco de cair em golpes de e-mail (phishing). Esse tipo de fraude, que engana usuários para revelar dados pessoais, tem crescido muito: só entre 2020 e 2021, idosos nos EUA perderam 1,7 bilhão de dólares em golpes, um aumento de 74%.

Na pesquisa, 182 pessoas entre 18 e 90 anos fizeram dois testes: um com e-mails falsos enviados durante 30 dias e outro em laboratório, onde tinham que avaliar se mensagens pareciam seguras ou suspeitas. Os resultados mostraram que quanto maior a idade, menor a capacidade de diferenciar e-mails falsos de verdadeiros.

O risco foi ainda maior em idosos com memória mais fraca ou que tinham o gene APOE4, ligado ao Alzheimer. Os testes de laboratório se mostraram bons para prever quem tem mais chance de cair em golpes.

O estudo foi feito em parceria com universidades e institutos dos EUA e Canadá, mas teve como limitação a falta de diversidade dos participantes (a maioria era branca e da Flórida).

Segundo os pesquisadores, é urgente criar estratégias de proteção, já que muitos idosos usam aplicativos e serviços *on-line*, mas têm menos experiência digital e mais dificuldade para se recuperar de prejuízos.

## 3 Metodologia

A metodologia utilizada para a pesquisa foi a realização de uma pesquisa de campo, por meio de um questionário contendo perguntas da escala Likert sobre o contato prévio dos entrevistados com golpes da modalidade *phishing*. A pesquisa foi desenvolvida a partir da ferramenta *Google Forms* e divulgada por meio das redes sociais dos integrantes que, assim, obtiveram respostas de uma amostra não probabilística e por conveniência.

O mesmo questionário foi aplicado a dois públicos distintos: o primeiro abrange pessoas entre 18 e 59 anos, enquanto o segundo contém pessoas com 60 anos ou mais. O foco da pesquisa consiste em coletar respostas de variadas faixas etárias para sustentar a hipótese de que o grupo mais propenso a se tornar vítima de *phishing* é a terceira idade. Devido ao caráter estatístico do tema escolhido, foi empregado o método quantitativo.

Algumas das perguntas contidas no questionário estão relacionadas a trabalhos acadêmicos previamente publicados, incluindo Alves (2024), Brenol (2023), Valente (2001), Wojahn (2022) e Wust (2023).

A pesquisa, somando os dois questionários, resultou em 217 respondentes, que estão contidos dentro de um universo de 160 milhões de pessoas, número correspondente à quantidade de brasileiros com idade igual ou acima de 18 anos (IBGE, 2022). As respostas foram obtidas entre 08 de novembro de 2024 e 13 de março de 2025, ou seja, durante um período de 125 dias.

No início de cada questionário foi incluído um Termo de Consentimento Livre e Esclarecido (TCLE), como forma de garantir aos entrevistados que os dados coletados serão

tratados com total sigilo e utilizados exclusivamente para fins acadêmicos, além de apontar o objetivo do projeto.

## 4 Resultados e Discussões

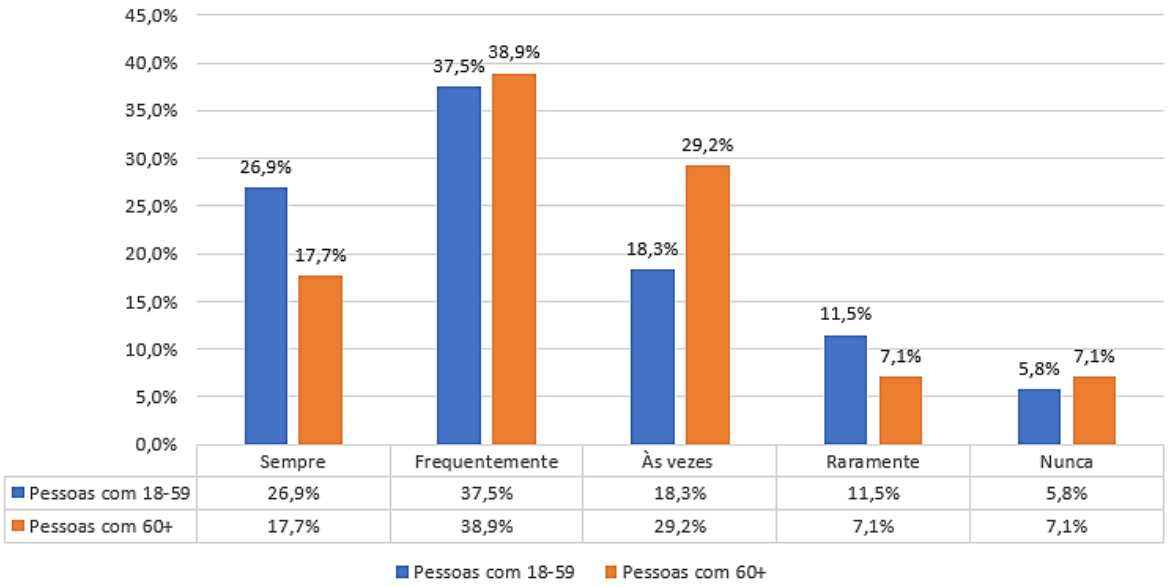
A seguir estão explicitados os resultados obtidos com a pesquisa, em que os dados brutos são convertidos em análises e comparações entre os dois públicos entrevistados.

Na Figura 1, observou-se que a maioria dos respondentes até 59 anos já foi exposta a tentativas de obtenção de informações pessoais ou financeiras de maneira suspeita. 37,5% dos participantes afirmaram receber essas mensagens frequentemente, enquanto 26,9% relataram que isso ocorre sempre.

No grupo de respondentes com 60 anos ou mais, os resultados revelam uma realidade semelhante à observada no público mais jovem. A maior parte dos participantes (38,9%) relatou receber frequentemente e-mails ou mensagens solicitando informações pessoais ou financeiras de maneira suspeita. Além disso, 29,2% afirmaram que recebem essas abordagens às vezes, e 17,7% declararam que isso acontece sempre. Esses resultados sugerem que, embora ambos os grupos estejam vulneráveis, há uma maior recorrência de tentativas de contato com o grupo mais jovem, ao passo que o público idoso continua significativamente exposto, confirmando a afirmação de Cardoso (2023).

**Figura 1**

*Você já recebeu algum e-mail ou mensagem solicitando informações pessoais ou financeiras de maneira suspeita?*




| | Sempre | Frequentemente | Às vezes | Raramente | Nunca |
|---|---|---|---|---|---|
| Pessoas com 18-59 | 26,9% | 37,5% | 18,3% | 11,5% | 5,8% |
| Pessoas com 60+ | 17,7% | 38,9% | 29,2% | 7,1% | 7,1% |

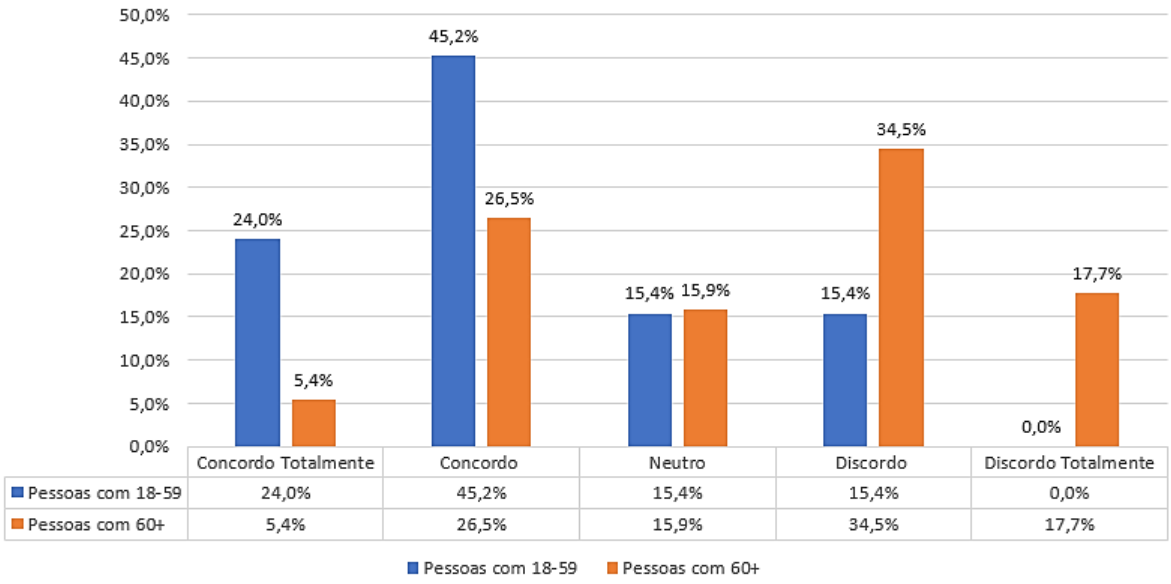
Fonte: Dados da pesquisa

Observa-se que a maioria dos respondentes mais jovens (45,2%) concorda que se sente confiante para identificar golpes de *phishing*, enquanto 24% concordam totalmente. Esses dados (Figura 2) evidenciam a importância de reforçar ações educativas, uma vez que o excesso de confiança pode aumentar o risco de exposição.

Entre os idosos, a maior parte discorda (34,5%), enquanto 26,5% concordam e 15,9% se mantêm neutros. Avalia-se que, no geral, eles têm consciência de sua falta de preparo frente a um golpe dessa modalidade, possuindo dificuldade de identificá-lo.

**Figura 2**

*Você se sente confiante em sua capacidade de identificar um golpe de phishing? (Batista e Gouveia, 2023)*



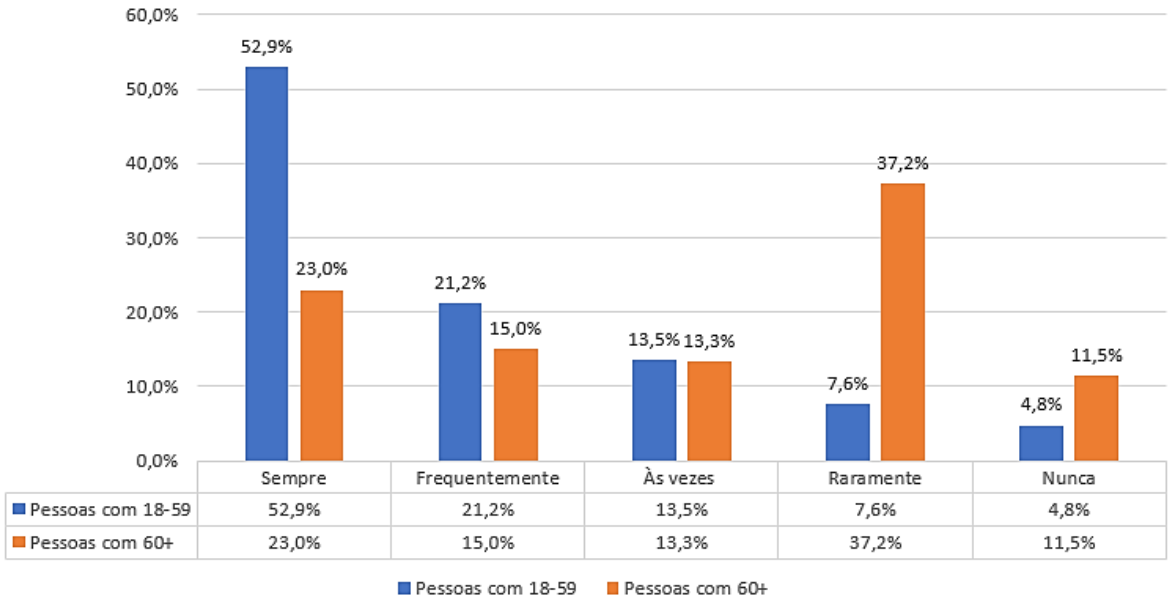

Fonte: Dados da pesquisa

Na Figura 3, dentre os respondentes entre 18 e 59 anos, mais da metade (52,9%) sempre faz essa verificação. Outros 21,2% afirmam verificar frequentemente, enquanto 13,5% fazem isso somente às vezes.

Sobre a frequência com que os participantes 60+ verificam o remetente de um e-mail antes de abrir anexos ou clicar em *links*, percebe-se que a maioria raramente (37,2%) ou às vezes (13,3%) realiza essa verificação. Apenas 23% sempre verificam, enquanto 15% fazem isso frequentemente. Há ainda 11,5% que nunca checam o remetente. De certa forma, os resultados trazidos são alarmantes, visto que uma enorme parcela respondeu que nunca, raramente e às vezes verifica o remetente dos e-mails que recebe. Isso caracteriza o grupo como "presa fácil" para os golpistas.

**Figura 3**

*Com que frequência você verifica o remetente de um e-mail antes de abrir anexos ou clicar em links? (Alves, 2024)*

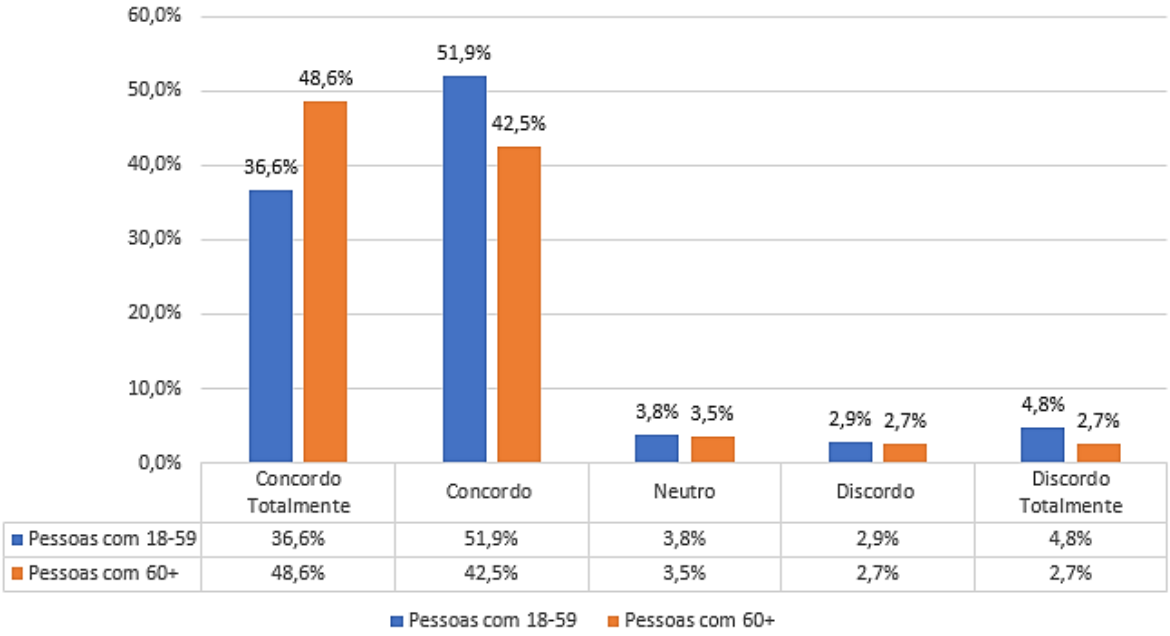



Fonte: Dados da pesquisa

A maioria dos participantes, tanto do grupo entre 18 e 59 anos quanto dos 60+, acredita que a terceira idade é mais vulnerável a golpes de *phishing*. Entre os idosos, 48,6% concordam totalmente com essa afirmação e 42,5% concordam. No grupo mais jovem, 36,6% concordam totalmente e 51,9% concordam (Figura 4). Esses dados refletem uma percepção coletiva clara sobre a fragilidade da população idosa frente a crimes cibernéticos, corroborando estudos como o de Brenol (2023), que apontam os idosos como alvos preferenciais de golpistas. A baixa porcentagem de discordância ou neutralidade mostra que há uma conscientização generalizada do risco, mesmo entre os próprios idosos.

**Figura 4**

*Você acredita que a terceira idade é mais vulnerável a golpes de phishing do que outras faixas etárias? (Brenol, 2023)*



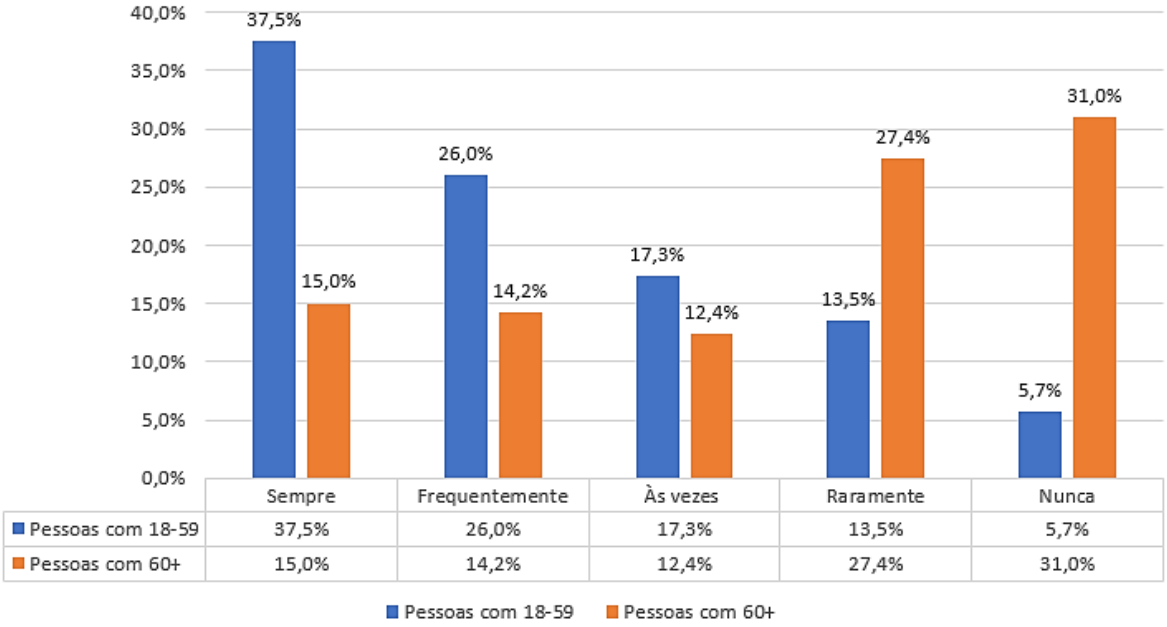

| | Concordo Totalmente | Concordo | Neutro | Discordo | Discordo Totalmente |
|---|---|---|---|---|---|
| Pessoas com 18-59 | 36,6% | 51,9% | 3,8% | 2,9% | 4,8% |
| Pessoas com 60+ | 48,6% | 42,5% | 3,5% | 2,7% | 2,7% |

Fonte: Dados da pesquisa

A análise da Figura 5 demonstra uma disparidade relevante entre faixas etárias quanto ao uso de softwares de segurança digital. Entre os participantes de 18 a 59 anos, 37,5% afirmam sempre utilizar esse tipo de proteção, enquanto apenas 15% dos idosos compartilham da mesma prática. A diferença se intensifica nas categorias raramente e nunca: 27,4% e 31% dos idosos, respectivamente, assumem pouca ou nenhuma utilização de antivírus ou ferramentas similares. Esses dados evidenciam uma lacuna preocupante na proteção digital da terceira idade, reforçando a necessidade de campanhas de educação voltadas à segurança *on-line*, como propõem Wojahn et al. (2022) e Fraga (2023), destacando que a inclusão digital é uma medida essencial para a prevenção de fraudes.

**Figura 5**

*Você costuma usar softwares de segurança, como antivírus, para se proteger contra fraudes online?*

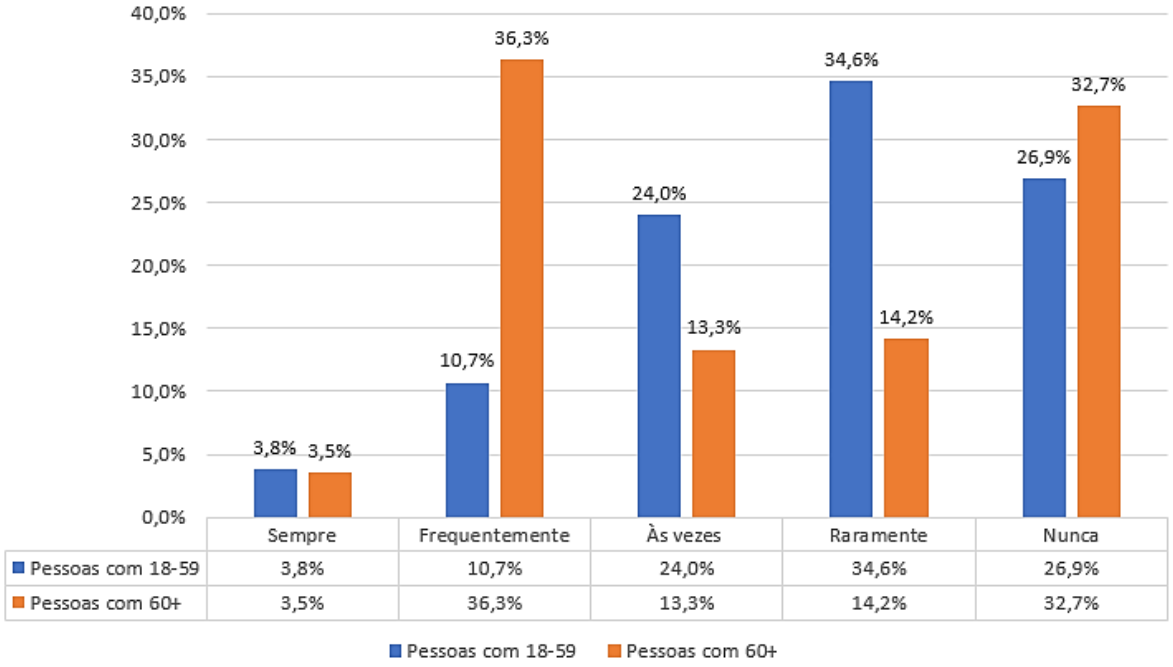



Fonte: Dados da pesquisa

Os dados da Figura 6 demonstram que a maior parte dos idosos não percebeu ter suas informações comprometidas por golpes de *phishing*, com 32,7% respondendo nunca e 14,2% raramente. Ainda assim, 36,3% relataram já terem sido vítimas frequentemente. Já entre os jovens, o maior percentual aparece na resposta raramente (34,6%), seguido de, às vezes, (24%). Isso sugere que ambos os grupos já passaram por situações de risco, embora os idosos tendam a ter menos consciência sobre o ocorrido, o que pode refletir falhas na identificação do golpe ou no reconhecimento do impacto da fraude. Valente (2021) já apontava o Brasil como um dos países com maior número de vítimas de *phishing*, o que torna os dados da pesquisa ainda mais preocupantes.

**Figura 6**

*Você já teve suas informações pessoais comprometidas em algum golpe de phishing? (Valente, 2021)*

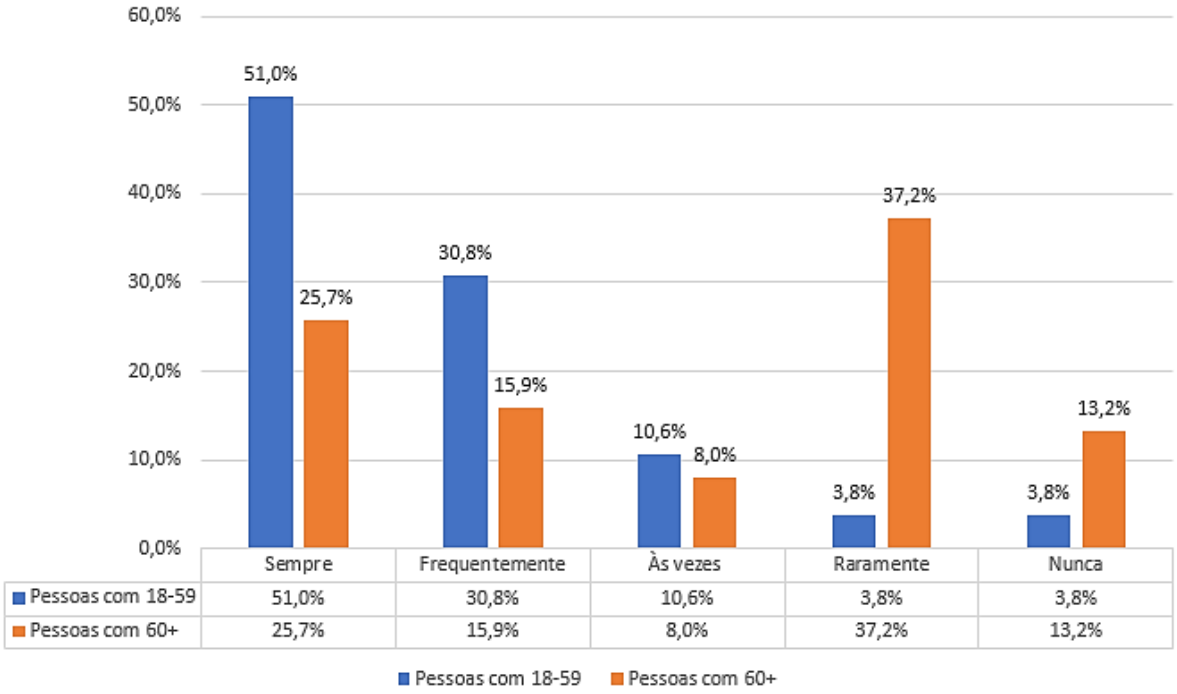



Fonte: Dados da pesquisa

A diferença entre os dois grupos é marcante: 51% dos respondentes entre 18 e 59 anos afirmam sempre questionar a legitimidade de e-mails urgentes, contra apenas 25,7% dos idosos. Ainda, 37,2% dos idosos raramente ou nunca adotam essa postura, demonstrando um baixo nível de criticidade diante de possíveis fraudes. A falta de verificação prévia é um fator de risco destacado por Cloudflare (n.d), que indica que e-mails de *phishing* costumam criar sensação de urgência para induzir a ações precipitadas. Portanto, a Figura 7 reforça a urgência em trabalhar a conscientização digital com o público idoso, promovendo hábitos simples, mas eficazes, de checagem.

**Figura 7**

*Você costuma questionar a legitimidade de e-mails ou mensagens que solicitam ações urgentes, como atualizar informações pessoais?*

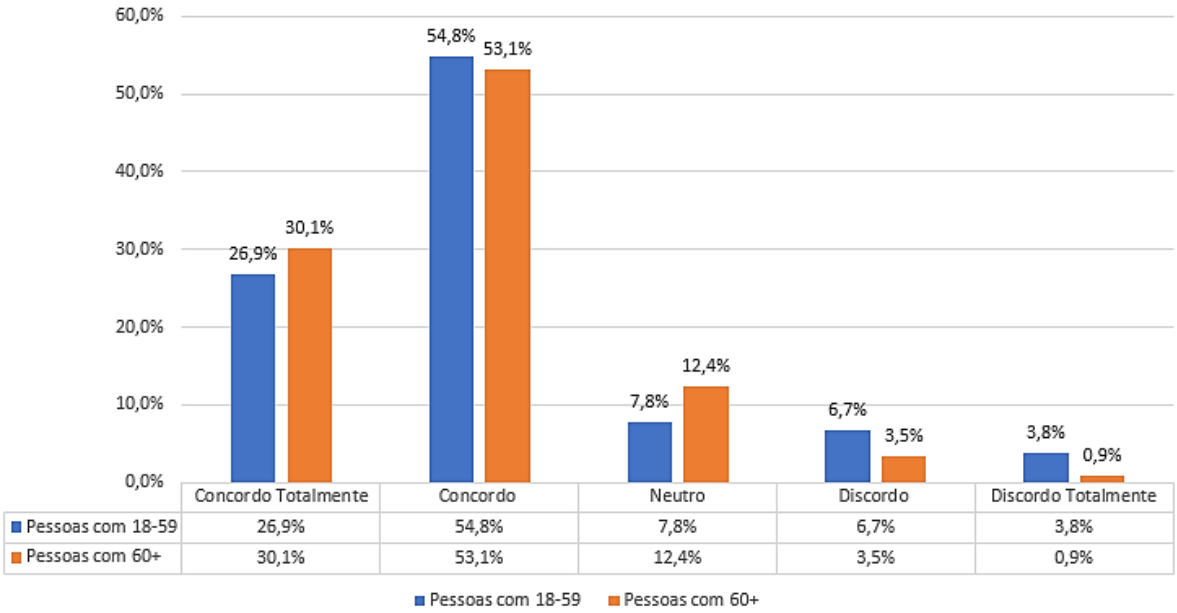



Fonte: Dados da pesquisa

Na Figura 8, ambos os grupos reconhecem que os golpes estão se tornando mais sofisticados e difíceis de identificar. No grupo jovem, 81,7% concordam com essa afirmação (concordo totalmente + concordo), enquanto entre os idosos esse índice é ainda maior: 83,2%. Esse dado aponta para um desafio comum entre todas as faixas etárias e reforça as observações de Wojahn et al. (2022), que destacam a evolução dos golpes como fator preocupante mesmo entre os usuários mais experientes. A crescente complexidade das fraudes exige que a prevenção digital não se limite a ensinar o básico, mas acompanhe a sofisticação dos ataques.

**Figura 8**

*Você considera que os golpes de phishing estão ficando mais difíceis de detectar com o tempo?*

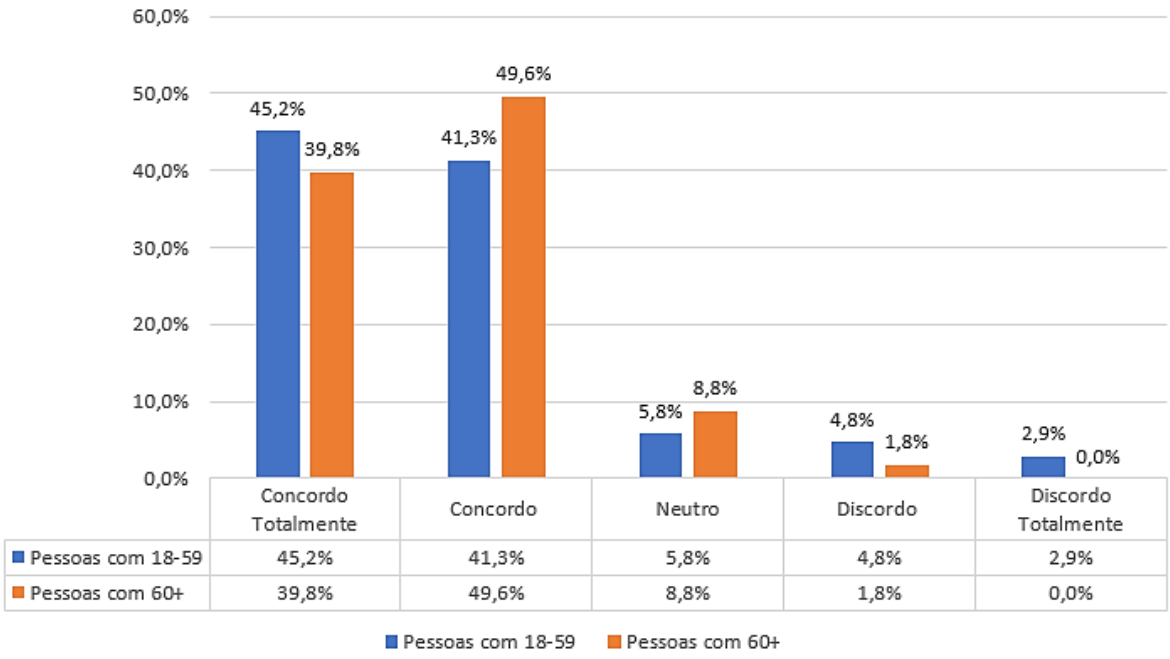



Fonte: Dados da pesquisa

A pesquisa revela uma ampla concordância sobre a necessidade de treinamentos direcionados à terceira idade. Entre os respondentes de 18 a 59 anos, 45,2% concordam totalmente e 41,3% concordam. O grupo 60+ reforça essa percepção, com 39,8% concordando totalmente e 49,6% concordando. Essa convergência entre faixas etárias na Figura 9 demonstra uma percepção clara da vulnerabilidade digital dos idosos, e vai ao encontro do que propõe Cardoso (2023), ao destacar que o preparo específico é essencial para combater fraudes virtuais. O dado reforça a importância de políticas públicas voltadas à educação digital inclusiva.

**Figura 9**

*Você acha que pessoas mais velhas deveriam receber treinamento específico para reconhecer golpes de phishing e proteger seus dados pessoais on-line? (Cardoso, 2023)*

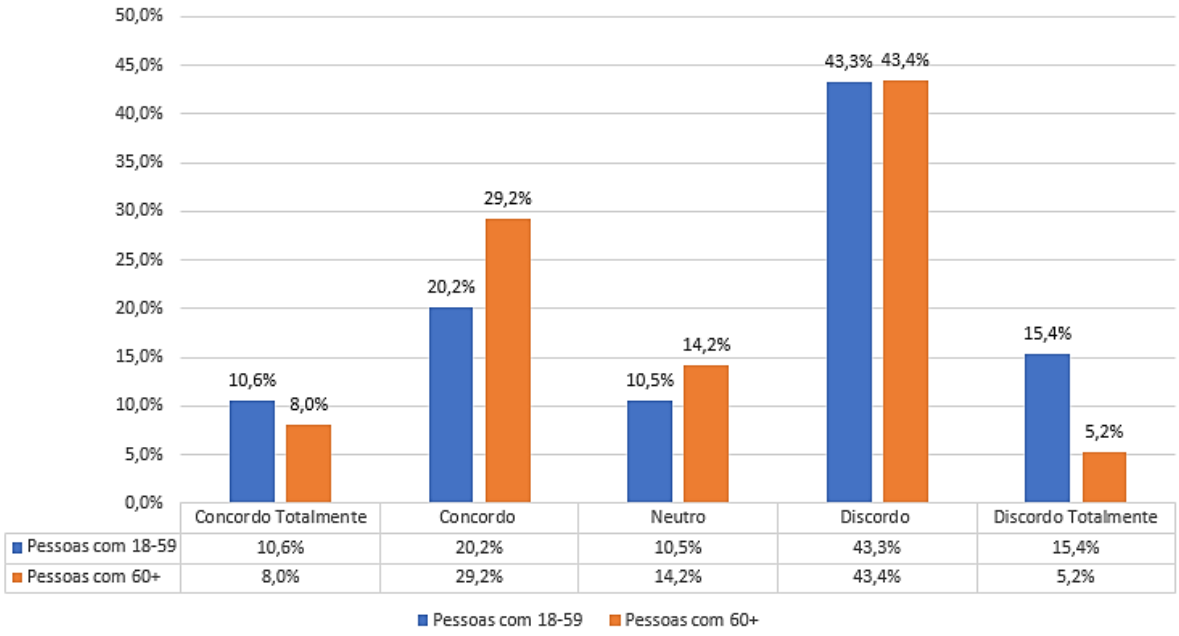



Fonte: Dados da pesquisa

A Figura 10 mostra a percepção de diferentes faixas etárias sobre a eficácia da educação e conscientização digital na proteção contra golpes *on-line*. Entre as pessoas de 18 a 59 anos, nota-se que 20,2% concordam e 10,6% concordam totalmente, indicando que aproximadamente 30,8% acreditam que a educação digital é eficaz. Já entre os idosos (60+), a concordância total é menor (8,0%) e a concordância simples é maior (29,2%), totalizando 37,2%. No entanto, o maior destaque está na alta taxa de discordância em ambos os grupos: 43,3% entre os mais jovens e 43,4% entre os idosos, sugerindo um forte ceticismo quanto à eficácia da conscientização digital isoladamente. Esse resultado indica que, apesar dos esforços educativos, muitas pessoas ainda não se sentem plenamente protegidas contra os golpes *on-line*, especialmente os de *phishing*.

**Figura 10**

*Você sente que a educação e conscientização digital é suficiente para proteger as pessoas contra os golpes online? (Wojahn et al., 2022)*




Fonte: Dados da pesquisa

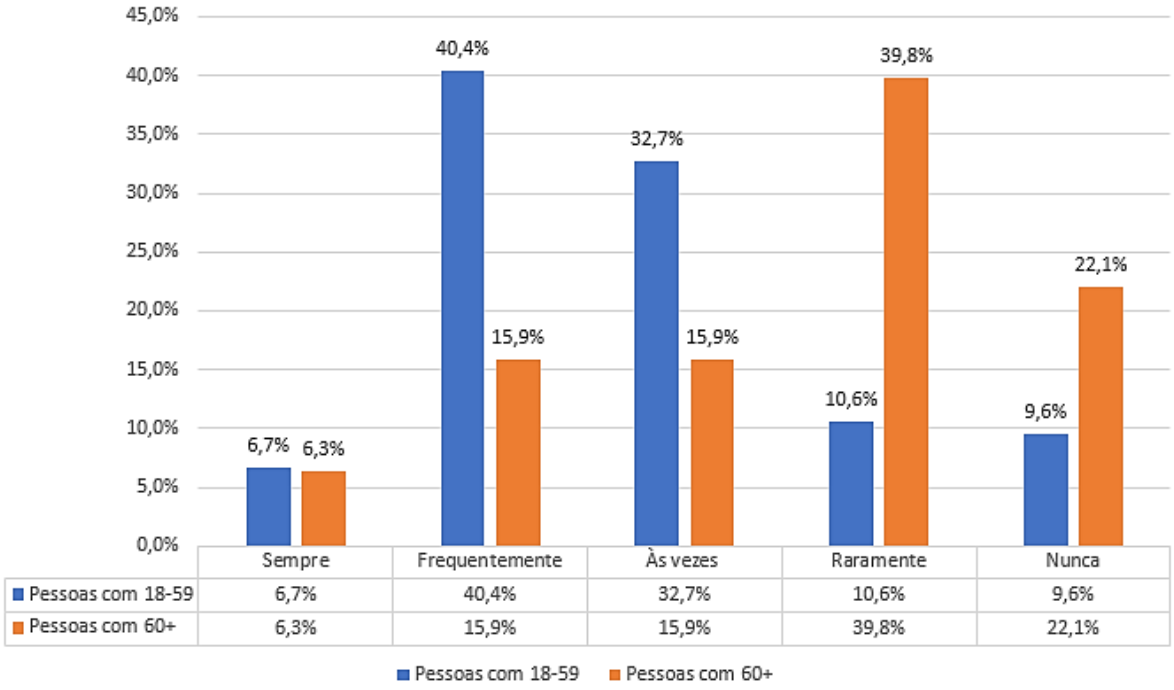
Pode-se analisar que no grupo com 18 a 59 anos, os indivíduos frequentemente se informam sobre os golpes de *phishing* (40,4%), 6,7% sempre se informam, 32,7% às vezes, 10,6% raramente e 9,6 nunca se informam.

Quanto ao grupo 60+, percebe-se a queda de pessoas informadas sobre os golpes financeiros, sendo que 39,8% raramente busca informação sobre o assunto e 22,1% nunca se informaram sobre. Apenas 15,9% se informam às vezes e frequentemente.

Com isso, a Figura 11 aponta que os mais jovens tendem a pesquisar mais informações sobre golpes de *phishing* e formas de prevenção, enquanto os idosos, em grande parte, se informam pouco ou quase nunca. Isso pode indicar uma maior vulnerabilidade dos mais velhos a esse tipo de golpe, ressaltando a importância de campanhas educativas voltadas para esse público.

**Figura 11**

*Você costuma se informar sobre golpes de phishing e formas de preveni-los?*




Fonte: Dados da pesquisa.

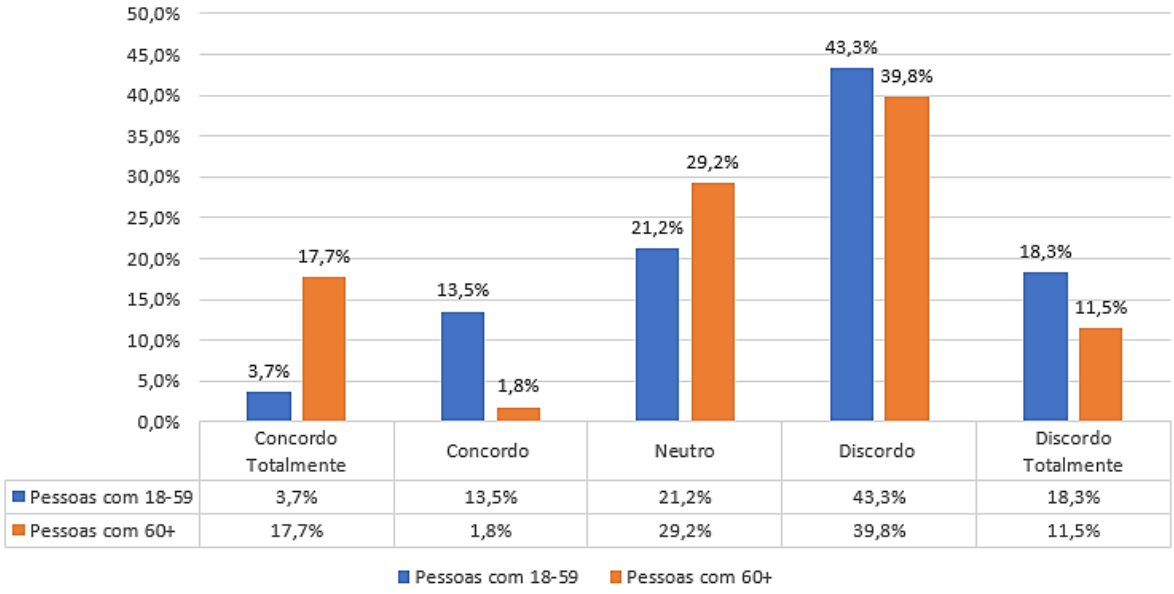
Nota-se que dentre as pessoas de 18 a 59 anos, a maioria dos entrevistados desconfia das medidas de segurança de bancos e *e-commerce*. 43,3% discordam e 18,3% discordam totalmente. Uma parte se mantém neutra com 21,2%, enquanto 13,5% concordam com a medidas de segurança e uma pequena parte (3,7%) concordam totalmente.

Replicando o pensamento dos jovens, os idosos também desconfiam da segurança trazida por bancos e e-commerces, havendo uma discordância de 39,8% e uma discordância total de 11,5%. 29,2% se mantiveram neutros, enquanto 1,8% concordam e 17,7% concordam totalmente.

Sintetizando, a Figura 12 evidencia um alto nível de desconfiança da população em relação às medidas de segurança adotadas por bancos e plataformas de *e-commerce*, demonstrando que os mais jovens são mais céticos do que os mais velhos.

**Figura 12**

*Você confia nas medidas de segurança oferecidas por bancos e plataformas de e-commerce para proteger seus dados? (Wust, 2023)*




Fonte: Dados da pesquisa

## 5 Considerações Finais

A presente pesquisa permitiu compreender que o golpe de *phishing* representa uma ameaça significativa para pessoas de todas as idades, mas afeta de forma mais acentuada a população idosa. A análise dos dados coletados revelou que os idosos, em sua maioria, apresentam menor preparo para lidar com ameaças digitais, seja por falta de familiaridade com as tecnologias, dificuldades cognitivas ou interfaces pouco acessíveis.

Os resultados do questionário evidenciaram que grande parte dos idosos não verifica remetentes de e-mails suspeitos, não utiliza com frequência softwares de proteção e, muitas vezes, não se sente segura ou preparada para identificar tentativas de fraude. Essa realidade contrasta com o público mais jovem, que tende a buscar mais informações sobre segurança digital, embora também esteja exposto a riscos.

Diante disso, fica clara a necessidade de ações preventivas voltadas especificamente para a terceira idade. Investimentos em programas de inclusão e letramento digital, bem como o fortalecimento de políticas públicas educativas, são medidas fundamentais para reduzir a vulnerabilidade desse grupo.

Os achados de James et al. (2014) e de Chen et al. (2025) reforçam esse entendimento ao apontar que a prevenção deve atuar em três frentes: fortalecimento cognitivo e psicológico por meio de programas de literacia digital e financeira; engajamento da família e da comunidade como guardiões sociais; e políticas públicas que estimulem práticas mais seguras no ambiente *on-line*. A integração dessas medidas amplia a capacidade de proteção dos idosos, favorecendo tanto sua autonomia quanto a sua participação segura no mundo digital.

Conclui-se que a conscientização digital, aliada à construção de ambientes virtuais mais acessíveis e seguros, pode contribuir significativamente para a proteção dos idosos contra golpes como o *phishing*, promovendo sua autonomia, segurança e inclusão no meio digital.

**Referências**


Almeida, M.(2020). Golpes financeiros contra idosos crescem 60% na pandemia. Como evitar. *Exame*, 02 set. 2020. https://exame.com/invest/minhas-financas/golpes-financeiros-contra-idosos-crescem-60-na-pandemia/

Alves, L. de M. (2024). *Engenharia social: estudo de ataques e métodos de prevenção* (Trabalho de Conclusão de Curso, Bacharelado em Ciência da Computação, Pontifícia Universidade Católica de Goiás). Pontifícia Universidade Católica de Goiás. https://repositorio.pucgoias.edu.br/jspui/handle/123456789/7976

Anjos, T. P. dos, & GONTIJO, L. A. (2015). Recomendações de usabilidade e acessibilidade para interface de telefone celular visando o público idoso. *Production*, v. 25, n. 4, p. 791-811, out./dez. http://dx.doi.org/10.1590/0103-6513.091312

Batista, R. F., & GOUVEIA, J. S. (2023). Crimes cibernéticos financeiros: a evolução do phishing através da vulnerabilidade do público digital. *Revista Juris Sertão/Juris Sertão Journal,* v. 1, n. 1, jul./dez. ISSN 3547-4755. https://jurissertao.com.br/index.php/home/article/view/17

Brenol, M. (2023). Golpes contra idosos cresce no Brasil. *Serasa*, 11 jul. https://www.serasa.com.br/premium/blog/golpes-contra-idosos/

Campêlo, M. A. (2024). Engenharia social: como aspectos psicológicos podem se relacionar com golpes e fraudes. Gov.br. *Portal do Investidor*, 25 jun. https://www.gov.br/investidor/pt-br/penso-logo-invisto/engenharia-social-como-aspectos-psicologicos-podem-se-relacionar-com-golpes-e-fraudes-1

Cardoso, M.A.F. (2023). O estelionato virtual praticado contra o idoso e os reflexos jurídico-penais. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, v. 9, n. 5, p. 3385–3398. DOI: 10.51891/rease.v9i5.10125 https://periodicorease.pro.br/rease/article/view/10125

Chen, Y., He, J., Zhang, Y., & Zhou, W. (2025). Examining older adults' vulnerability to online health scams: insights from routine activity theory. *Frontiers in Public Health*, v. 13.

Cloudflare. (n.d).*Como evitar phishing.* https://www.cloudflare.com/pt-br/learning/email-security/how-to-prevent-phishing/

DeLiema, M. (2024). *Safeguarding retirement in the age of scams*. TIAA Institute. https://www.tiaa.org/content/dam/tiaa/institute/pdf/insights-report/2025-01/safeguarding-retirement-in-the-age-of-scams_ti_deliema.pdf

Ebner, N. C., & Pehlivanoglu, D. (2024). Are older adults more vulnerable to scams? What psychologists have learned about who's most susceptible, and when. *UF News.* https://news.ufl.edu/2024/06/older-adults-vulnerable-to-scams/

FEBRABAN. (2022). Com pandemia, idosos brasileiros acessam mais a internet e redes sociais, mas ainda têm dificuldades com tecnologia. https://febrabantech.febraban.org.br/temas/educacao/com-pandemia-idosos-brasileiros-acessam-mais-a-internet-e-redes-sociais-mas-ainda-tem-dificuldades-com-tecnologia

Fraga, J. (2023). Inclusão digital é chave para prevenir golpes virtuais contra idosos, apontam especialistas. Folha de Pernambuco. https://www.folhape.com.br/noticias/inclusao-digital-e-chave-para-prevenir-golpes-virtuais-contra-idosos/304659/

Fuentes, P. (2021). Aumento de casos de violência contra idosos demonstra falta de políticas públicas. Jornal da USP. https://jornal.usp.br/atualidades/aumento-de-casos-de-violencia-contra-idosos-demonstra-a-falta-de-politicas-publicas/4

IBGE. Censo 2022. https://cidades.ibge.gov.br/brasil/pesquisa/10102/122229

James, B.D., Boyle, P. A.; Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect*, v. 26, n. 2, p. 107-122. DOI: 10.1080/08946566.2013.821809.

Juvenassi, A. J. B. (2021). Idosos enfrentam mais dificuldades e preconceito no uso das tecnologias digitais. Universidade Federal de Santa Maria. *Agência Hora.* https://www.ufsm.br/midias/experimental/agencia-da-hora/2021/09/01/idosos-enfrentam-mais-dificuldades-e-preconceito-no-uso-das-tecnologias-digitais

Kaspersky. (2023). Com retomada econômica e IA, phishing cresce mais de 5 vezes no Brasil. https://www.kaspersky.com.br/blog/panorama-de-ciberameacas-2023/21631/

Kaspersky. (2023). *Nova epidemia: phishing cresce mais de 5 vezes no Brasil com retomada das atividades econômicas e apoio da IA*. https://www.kaspersky.com.br/about/press-releases/nova-epidemia-phishing-cresce-mais-de-5-vezes-no-brasil-com-retomada-das-atividades-economicas-e-apoio-da-ia .

Kosinski, M. (2024). O que é phishing? *IBM*. https://www.ibm.com/br-pt/topics/phishing

Marichal, P. L. de. (2022). Phishing na era da informação: relevância da proteção de dados pessoais (Trabalho de Conclusão de Curso, Bacharelado em Biblioteconomia, Universidade Federal do Rio Grande do Sul). Universidade Federal do Rio Grande do Sul. https://lume.ufrgs.br/handle/10183/258868

Montagner, A. S., Westphall, C. M. (2022). Uma breve análise sobre phishing. Revista ComInG. *Communications and Innovations Gazette*, v. 6, n. 1, p. 46–56. DOI: 10.5902/2448190471731. https://periodicos.ufsm.br/coming/article/view/71731

Phishing.ORG. (n.d.). History of phishing. https://www.phishing.org/history-of-phishing

Supera. (2021). A importância do letramento digital para idosos institucionalizados. https://metodosupera.com.br/a-importancia-do-letramento-digital-para-idosos-institucionalizados/

Valente, J. (2021). Brasil é o país com maior número de vítimas de *phishing* na internet. *Agência Brasil*. https://agenciabrasil.ebc.com.br/geral/noticia/2021-03/brasil-e-o-pais-com-maior-numero-de-vitimas-de-phishing-na-internet .

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. (2022). The social vulnerability of the elderly against scams in the digital scope. *Research, Society and Development*, 11(11), e452111133652. https://doi.org/10.33448/rsd-v11i11.33652

Wust, E. F. M. (2023). Fraudes e golpes bancários no Brasil: tipologia e iniciativas das instituições financeiras (Trabalho de Conclusão de Curso, Bacharelado em Administração, Fundação Universidade Federal de Mato Grosso do Sul). Fundação Universidade Federal de Mato Grosso do Sul. https://repositorio.ufms.br/handle/123456789/8105