Ferramenta Educacional para Avaliação e Melhoria do Nível de Conscientização em Segurança da Informação

Fernanda Lemos Fialho[1], Fernando A. Aires Lins[1], Jeisa P. O. Domingues[1]

[1]Departamento de Computação - Universidade Federal Rural de Pernambuco (UFRPE)
52.171-900 – Recife – PE – Brazil

{fernanda.lfialho, fernandoaires, jeisa.domingues}@ufrpe.br

Abstract. *The advancements in communication technology also enhanced the means to steal sensitive data through cyber scams. In this context, this paper describes the website De Olho na Isca, designed to raise awareness and identify the level of knowledge the general Brazilian public has on Social engineering-related attacks through various digital scenarios. The results obtained through the answers of 70 participants positively highlight a broad knowledge by the users on the addressed areas. However, the study also shows topics that should be more widespread and enlightened to the population in general, like the social media fake account scam scenario.*

Resumo. *Através do avanço da tecnologia na comunicação, também foram aprimoradas as maneiras para roubar dados sensíveis por meio de golpes cibernéticos. Neste contexto, este artigo descreve o De Olho na Isca, um website desenvolvido para conscientizar e avaliar o nível de conhecimento da população brasileira em relação a ataques envolvendo Engenharia Social nos mais diversos cenários digitais. Os resultados obtidos a partir das respostas de 70 participantes destacam positivamente um bom conhecimento dos usuários acerca do tema. Porém, o estudo também demonstra pontos que devem ser melhor esclarecidos para a população, como o cenário de golpes via contas falsas em redes sociais.*

1. Introdução

A técnica de enganação através da Engenharia Social existe há décadas, como relatado pelo famoso hacker Kevin Mitnick em seu livro "A Arte de Enganar" [Mitnick e Simon 2003]. Mitnick mostra que a Engenharia Social e o *phishing* trazem diversos prejuízos à sociedade. De acordo com os autores do livro citado, o engenheiro social é aquele indivíduo que, por meio de influência e persuasão, consegue convencer alguém a realizar alguma tarefa que normalmente não faria, com o objetivo de adquirir informações úteis daquela pessoa. Transportando para o cenário atual do Brasil, onde grande parte da população possui acesso a smartphones e à Internet, diariamente diversos dados importantes são armazenados nesses dispositivos. Para um criminoso, o menor esforço que ele vai ter para conseguir acesso a informações bancárias, por exemplo, é convencer o próprio alvo a entregar esses dados [Mitnick e Simon 2003]. Somado a isso, a tecnologia também avançou de forma a facilitar o lado do golpista, que agora também conta com a possibilidade de utilização da Inteligência Artificial [Folhapress 2024].

Ainda neste cenário, as notícias sobre os prejuízos causados pelas fraudes digitais revelam a necessidade da população se atentar aos indícios de que podem estar sendo alvo dos engenheiros sociais. Conforme o relatório "Panorama de Ameaças para a América Latina 2024" da Kaspersky [Kaspersky 2024], empresa especializada em desenvolver softwares para a Segurança da Informação, foram registradas 3,9 milhões de tentativas de ataques cibernéticos nos dispositivos móveis na América Latina entre

agosto de 2023 e julho de 2024. Especificamente no Brasil, 1,8 milhão de ameaças de ataques.

É importante que todo cidadão saiba se defender contra a Engenharia Social, pois é um tipo de ataque que, combinado com outros golpes cibernéticos, podem levar a danos financeiros e roubo de dados. Em outro estudo, realizado pelo Instituto DataSenado [Instituto DataSenado 2024], os golpes digitais em 2024 atingiram mais de 40,85 milhões de pessoas por meio de crimes cibernéticos como fraude na Internet ou invasão de contas bancárias. Outro levantamento em relação a golpes cibernéticos no Brasil em 2024, realizado pelo Datafolha [Miato e Nicoceli 2024] em parceria com o Fórum Brasileiro de Segurança Pública, mostra que ocorreram muitas tentativas de golpe via ligação telefônica ou aplicativos de mensagem.

Existem diferentes vetores de ataques dentro da Engenharia Social, e estes ataques podem ocorrer não apenas via e-mail, mas também através das redes sociais, SMS, ligação e sites falsos [Cert.br et al. 2022]. Ao se procurar por exemplos práticos, ou seja, testes ou simulações desses ataques na Internet, existem duas situações: ou aparecem as propagandas das empresas que atuam nessa área, como a KnowBe4, Cofense e a Proofpoint, ou aparecem alguns sites demonstrando e simulando situações suspeitas, através de um *quiz*, para que o usuário identifique se é uma tentativa de ataque ou não. No primeiro cenário, realizar os testes gratuitos disponibilizados pelas empresas não é tão simples para um usuário comum, pois o objetivo das empresas é oferecer serviço para outras organizações, e dessa forma, acabam barrando quem não possui contas institucionais para se cadastrar. No segundo cenário, apesar de ser bem mais viável para um usuário comum acessar esse conteúdo educacional, e de ser oferecida uma explicação didática, quando se completa o *quiz,* é apresentada na tela apenas a pontuação recebida, sem recomendações de uma curadoria de materiais educativos para o usuário se informar mais. Além disso, nas soluções encontradas, o foco é principalmente em *phishing* via e-mail. Outro ponto de atenção é que algumas soluções possuem o aspecto de desatualizadas, com simulações sendo feitas utilizando telas antigas de websites.

Diante desse contexto de lacuna de ferramentas em português que ajudem a população a identificar ataques digitais, o propósito deste trabalho é propor uma alternativa de solução educacional em relação à Engenharia Social no contexto da Segurança Computacional, abrangendo cenários mais diversos, atuais e próximos da realidade média da população brasileira. A análise do nível de conhecimento por parte dos usuários será feita a partir da coleta de dados obtidos na ferramenta desenvolvida. Além disso, serão disponibilizados na ferramenta proposta materiais de apoio devidamente validados, como forma de incentivo ao estudo do tema. Dessa forma, é possível tanto contribuir para a conscientização da população em si como na avaliação do comportamento dos usuários diante das situações de possível golpe.

O restante deste trabalho está estruturado da seguinte maneira: a Seção 2 apresenta os conceitos básicos necessários para a compreensão do estudo. A Seção 3 descreve a metodologia utilizada para criação da ferramenta e para análise das respostas submetidas. A Seção 4 aborda a avaliação dos resultados obtidos. A Seção 5 apresenta e discute trabalhos relacionados. Por fim, na Seção 6 são apresentadas as conclusões e os trabalhos futuros.

2. Conceitos Básicos

Inicialmente, entende-se por Segurança da Informação uma série de medidas que podem ser tomadas para garantir que as informações estejam disponíveis, íntegras, confiáveis e autênticas [CGSI et al. 2022]. Em uma sociedade que utiliza tecnologias diariamente, seja para aprendizado, trabalho, socialização ou outras situações, entender esse conceito e aprender a se proteger e manter a privacidade dos dados é de extrema importância [Ahmad et al. 2022]. Existem várias formas de quebrar esta segurança através de golpes digitais [Gupta et al. 2016], e, para o atacante, a forma mais fácil de realizar o crime é explorando o lado humano e persuadindo a vítima a fornecer as informações desejadas [Wang 2021]. Esse tipo de técnica é conhecida como Engenharia Social.

O Engenheiro Social possui inúmeros métodos para conseguir burlar a segurança. Estes métodos compreendem atitudes mais simples, como enviar mensagens para diversas pessoas esperando alguém morder a isca do golpe, que pode ser um *link* malicioso que vai capturar os dados do usuário [Cert.br et al. 2022], até golpes mais sofisticados utilizando Inteligência Artificial, visando convencer a vítima a, por exemplo, realizar uma transferência bancária para ajudar um "familiar" [Machado 2024].

Para identificar se essas situações são autênticas ou não, é possível tomar algumas medidas de prevenção, como verificar se o tom da mensagem recebida é urgente, pois é uma estratégia de manipulação dos atacantes e que faz a vítima agir rapidamente [Wang 2021]. Outro ponto de atenção que deve ser observado são os criminosos golpistas que criam contas em redes sociais, com anúncios falsos e enganam os outros usuários da plataforma a realizar pagamentos de produtos que não existem [G1 2024]. Uma das formas de se prevenir desse tipo de situação é realizando diversas verificações sobre a conta que está vendendo os produtos, os anúncios dos produtos em si, como é feita a forma de pagamento, pesquisando se é uma conta oficial da marca do produto, entre outras verificações [Cert.br et al. 2022].

3. Construção da Ferramenta "De Olho na Isca"

É importante saber se defender de golpes digitais que utilizam a técnica da Engenharia Social. Nesse contexto, uma das opções para transmissão desse conhecimento é através de *gamificação*. Este trabalho propõe um *quiz* para verificar o nível de conhecimento acerca do tema, e, ao mesmo tempo, conscientizar e transmitir mais informações que ajudem os usuários a se defender de possíveis ataques. Essa opção é interessante porque é facilmente acessível pelo público, não envolve muito tempo e esforço do usuário, e é uma técnica simples e eficaz de abordar um assunto sem ser massante e cansativo para quem está interagindo com o conteúdo [Nuci et al. 2021].

O público-alvo deste trabalho é justamente a população geral, que não necessariamente trabalha com tecnologia, e que não possui tanta familiaridade com os conceitos da Segurança da Informação. Outro ponto positivo nesse formato de exibição de conteúdo é que o usuário aprende a partir de exemplos – os cenários das perguntas. Ao finalizar o *quiz*, o usuário recebe uma pontuação referente à quantidade de acertos. Esse método avaliativo também mostra-se útil para o usuário entender quais temas ele pode melhorar seu conhecimento [Couto et al. 2023].

3.1. Visão Geral do Projeto do Quiz

Para a disponibilização do *quiz,* optou-se pela criação de um website, o De Olho na Isca. Tendo em vista a proposta de fácil acessibilidade do *quiz*, um website que rode tanto nos dispositivos móveis quanto nos computadores se mostrou como a escolha mais conveniente. Dessa forma, também é possível gerar uma facilidade de uso e consulta maior com os visitantes, que terão a oportunidade de ler e visualizar as dicas à vontade sempre que quiserem. O website foi desenvolvido pela ferramenta Framer em sua versão gratuita [Framer 2013], e é composto por duas páginas: "Página Inicial e Teste" e "Conteúdos para aprender mais".

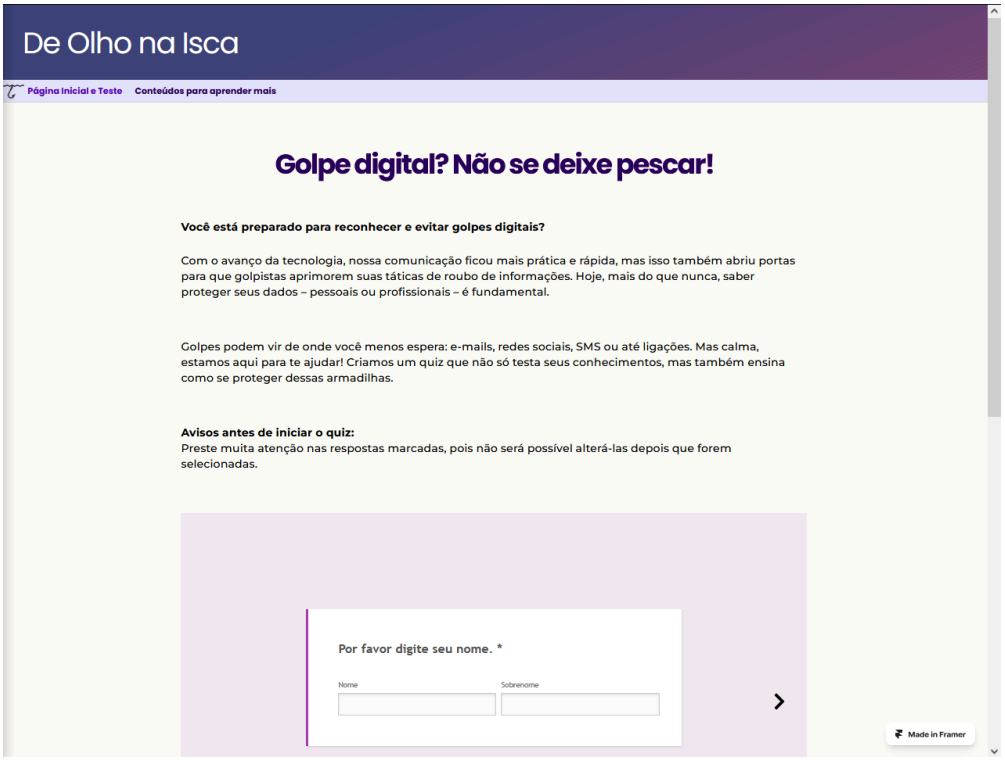

Figura 1. Topo da Página inicial do website De Olho na Isca

A Página Inicial é composta por três partes: primeiramente um breve resumo sobre a importância do estudo em desenvolvimento e do *quiz*, depois o *quiz* em si para o usuário responder, e por fim a divulgação das notícias jornalísticas sobre o tema de golpes digitais que inspiraram algumas das perguntas. Na Figura 1 é possível observar o topo da Página Inicial, que mostra o resumo do estudo desenvolvido, e uma parte da primeira tela do quiz. O usuário pode utilizar a barra de rolagem para ver o restante da Página, como os links para as notícias jornalísticas que estão abaixo do quiz. Já a Página de Conteúdos oferece três opções de fontes para o leitor adquirir mais conhecimento sobre o tema: o conteúdo "Cartilhas de Segurança para Internet", o "Internet Segura" e o "Cidadão na Rede". A escolha de exibir essas fontes deu-se por serem conteúdos bem produzidos, de simples entendimento e gerenciados pelo Comitê Gestor da Internet no Brasil (CGI.br). Na Figura 2, é possível observar o topo da página de Conteúdos para aprender mais, que mostra primeiramente o material das Cartilhas de Segurança para Internet. O usuário pode visualizar o restante dos conteúdos indicados utilizando a barra de rolagem.

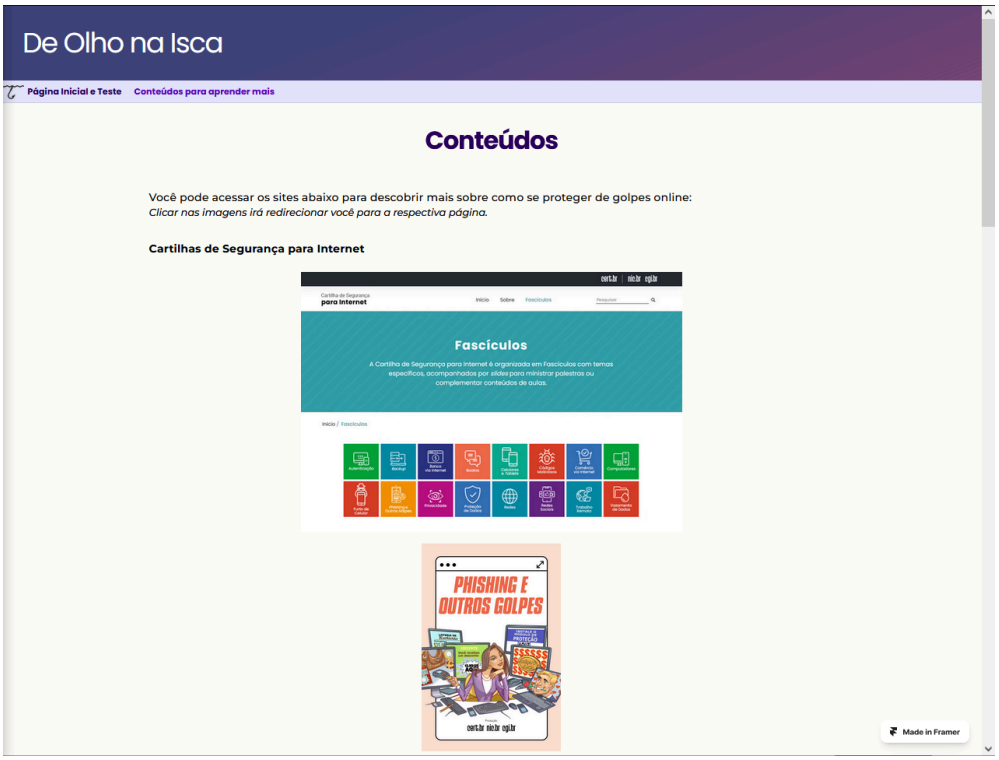

Figura 2. Topo da Página de Conteúdos

O material "Cartilhas de Segurança para Internet" é um conjunto de fascículos com linguagens simples, com dicas de diversas ações a serem tomadas não só para evitar golpes cibernéticos, mas boas práticas e boas maneiras para lidar com proteção de dados, privacidade, redes sociais, entre outros temas. Já o material "Internet Segura" [Cert.br 2017], por outro lado, tem um foco mais amplo em cuidados na Internet em si, e os guias são desenvolvidos com foco em públicos específicos (por exemplo: guia voltado para crianças, adolescentes, voltado para os pais, para pessoas acima de 60 anos, etc.). Também possui diversos jogos, o que o torna um conteúdo bem diverso. Por fim, o material "Cidadão na Rede" [Cert.br et al. 2020] é composto por vídeos curtos, explicando diversos temas que ajudam o usuário a se proteger de diversas situações digitais, com várias dicas para identificar fraudes e como agir, como denunciar.

3.2. Estrutura do *Quiz*

Em relação ao *quiz* em si, foi desenvolvido através da ferramenta CrowdSignal em sua versão gratuita. Ele inicia perguntando o nome e sobrenome do usuário, em seguida apresenta uma mensagem de aviso para o usuário prestar atenção nas respostas selecionadas. Por fim, as perguntas são iniciadas.

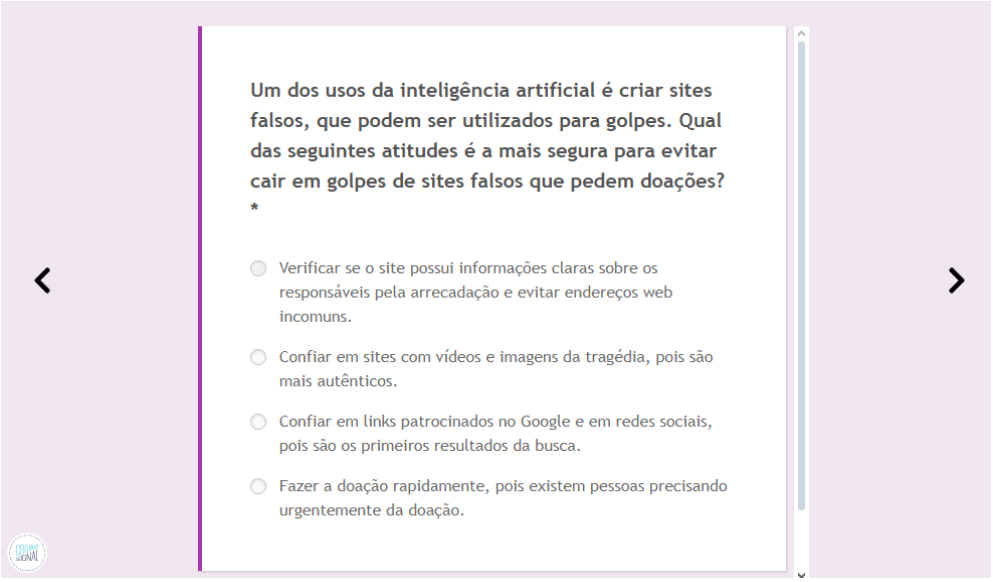

Figura 3. Exemplo da visualização das perguntas no *quiz*

O *quiz* apresenta dez perguntas no total, separadas em páginas individuais. Após cada pergunta, a página seguinte indica qual era a resposta correta e a sua explicação. Exemplos de uma página de pergunta e de uma página com a resposta correta e explicação são ilustrados, respectivamente, na Figura 3 e na Figura 4. A ferramenta foi estruturada desta forma para que, mesmo se o usuário apenas responder o *quiz* e não olhar o resto dos conteúdos no website, ele terá a oportunidade de aprender informações úteis para se manter protegido.

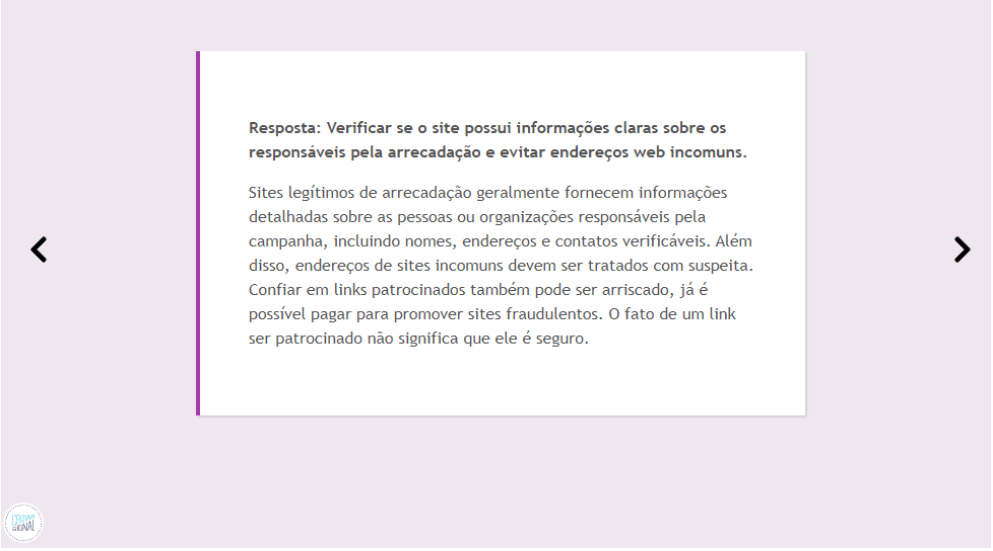

Figura 4. Exemplo de resposta correta e explicação após cada pergunta

Todas as perguntas são de múltipla escolha, com 4 opções diferentes que o usuário deve escolher apenas uma para continuar. A forma com que as perguntas são apresentadas também se altera no *quiz*, por exemplo, as perguntas 2 e 9 pedem para o usuário responder à opção mais arriscada ao invés da opção que evita o golpe, e as perguntas 3 e 5 pedem para o usuário conferir se as imagens são reais ou golpes; nesses

casos, o usuário possui apenas duas escolhas para marcar. Além disso, em relação aos temas que elas abrangem, podemos classificá-los em 6 categorias para o usuário ser testado nos mais diversos cenários, que estão detalhados na Tabela 1. Dessa forma também, espera-se que ao analisar os resultados obtidos, identifiquemos se existe uma lacuna maior de conhecimento em alguma área, mostrando a necessidade de maior conscientização para aquela área específica.

Tabela 1. Categorias das perguntas do quiz De Olho na Isca

Pergunta	Categorias dos golpes abordados
Pergunta 1, 2 e 9	Golpes realizados por redes sociais, como o Instagram ou o Facebook;
Pergunta 3	Golpe de *phishing* através de e-mail falso.
Pergunta 4	Golpe de site falso, com uso de Inteligência Artificial.
Pergunta 5 e 7	Golpes através de SMS falsos.
Pergunta 6 e 8	Golpes de Engenharia Social por ligação, destaque para a pergunta 8 envolvendo o uso de Inteligência Artificial.
Pergunta 10	Conhecimentos gerais em relação aos golpes digitais.

As perguntas foram construídas com base nas pesquisas e notícias divulgadas, principalmente durante 2024 [Folhapress 2024], [G1 2024], [Machado 2024]. Tanto as perguntas quanto as opções de resposta são cenários próximos à realidade de uma pessoa com acesso a um celular e Internet. Em comparação com outros testes de *phishing* tradicionais, por exemplo, que pedem para o usuário identificar visualmente coisas que indiquem um golpe de *phishing* [Google 2019], a ferramenta desenvolvida neste estudo opta por perguntar o que um usuário faria diante do cenário descrito, e depois explica qual seria a melhor resposta.

4. Avaliação dos Resultados Obtidos

Após a divulgação do website De Olho na Isca, foram coletadas e analisadas 70 submissões completas de respostas do *quiz no período de Janeiro/2025 até Fevereiro/2025*. A divulgação foi feita através de uma abordagem direta, onde o link do website foi enviado para pessoas conhecidas que não tinham um conhecimento aprofundado na área da Tecnologia da Informação. De modo geral, os resultados obtidos foram extremamente positivos, devido ao fato de 6 das 10 perguntas possuírem taxas de acerto acima de 90%. Este fato mostra que o nível de conscientização das pessoas que responderam o teste, considerando o escopo teórico da ferramenta, está em um bom nível. Na Figura 5 é possível observar de forma geral a porcentagem aproximada de taxa de acertos em cada resposta. Todas as perguntas, alternativas e as explicações para cada resposta correta estão disponíveis no Documento GoogleDocs a seguir: https://docs.google.com/document/d/1s02H03Jr3CHGklySXrkA2uz-jlSJfzMLOKeh_cCs9Mw/edit?usp=sharing. Neste mesmo documento também estão disponíveis todos os

dados coletados referentes às respostas dos usuários, com exceção dos dados pessoais de nome e sobrenome.

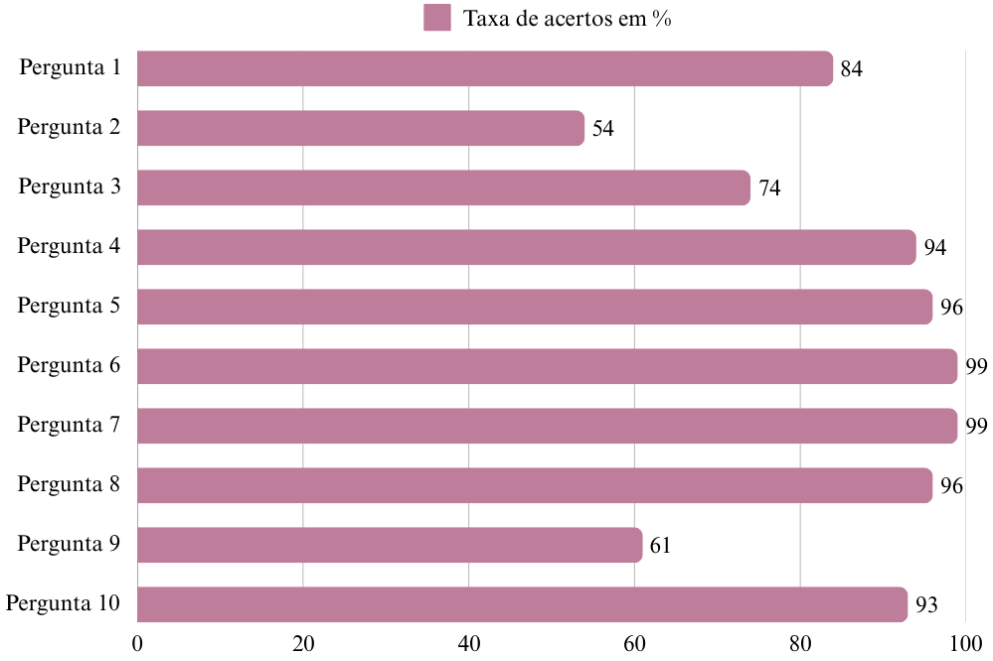

Figura 5. Taxa de acertos em cada pergunta do quiz De Olho na Isca

As perguntas mais bem respondidas foram a Pergunta 6, sobre a melhor atitude em um cenário de golpe através de ligação telefônica; e a Pergunta 7, para escolher a opção que ajuda a evitar o golpe do SMS falso. Ambas as perguntas obtiveram aproximadamente 99% de acerto, com apenas uma resposta errada cada. Isso demonstra alto conhecimento por parte dos usuários que responderam o teste em relação a golpes mais antigos, hipótese que pode estar ligada ao conhecimento acerca de como evitar essas situações estar mais difundido na sociedade. Outro dado que ilustra essa hipótese é visto na Pergunta 5, também em relação ao tipo de golpe via SMS, na qual apenas 3 pessoas responderam incorretamente. Nesta pergunta, o usuário precisa interpretar uma imagem de SMS recebido informando empréstimo e compra aprovada, e identificar se as mensagens se referem a tentativas de golpe ou se são válidas (reais). A baixa taxa de erros pode ser uma demonstração de que os usuários estão alerta para SMS suspeitos.

As perguntas que refletem maiores divergências em suas respostas são as Perguntas 1, 2, 3 e 9, que são as perguntas com taxas de acerto abaixo de 90%. Percebe-se que quando o tema é ataques através de redes sociais, existe uma dificuldade para entender qual a melhor atitude que evite o golpe. Baseado nestes dados, podem-se estimar duas hipóteses: a técnica da Engenharia Social para essa área é melhor aplicada, causando certas dificuldades para a possível vítima perceber se tratar de uma fraude, ou os usuários não possuem bom conhecimento nesta área, revelando a necessidade de conscientização e divulgação do assunto. Na Figura 6 é possível observar o conflito por parte dos usuários para responder corretamente uma pergunta relacionada a este tema de golpes através das redes sociais. Vale ressaltar que a Pergunta 2 foi categorizada como golpe por rede social porque o objetivo do golpe que está sendo simulado é atingir a rede social WhatsApp, e as alternativas para essa pergunta também são relacionadas a atitudes que o usuário deve tomar no WhatsApp para evitar o golpe.

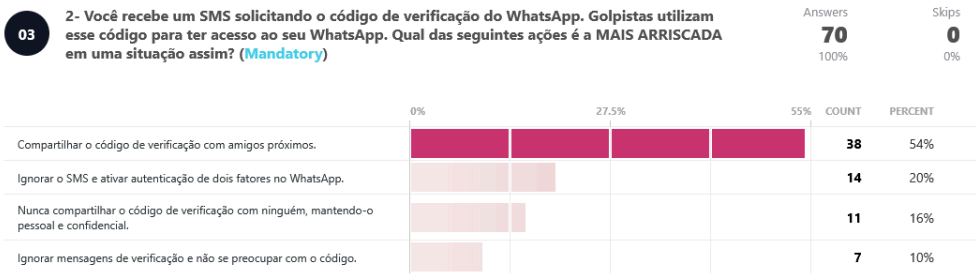

Figura 6. Pergunta referente a golpes pela rede social WhatsApp

A Pergunta 3, por outro lado, pede para o usuário interpretar uma imagem de um e-mail recebido informando que um novo login na conta Google foi realizado, e identificar se o e-mail é válido (real) ou uma tentativa de golpe. Segundo os princípios da Segurança da Informação, o esperado para essa pergunta é que, na dúvida, o usuário marque "Golpe", pois seria a atitude mais segura ao interagir com um conteúdo nos meios digitais. Surpreendentemente, a taxa de acerto para essa pergunta foi consideravelmente boa. Na Figura 7 os dados obtidos para a Pergunta 3.

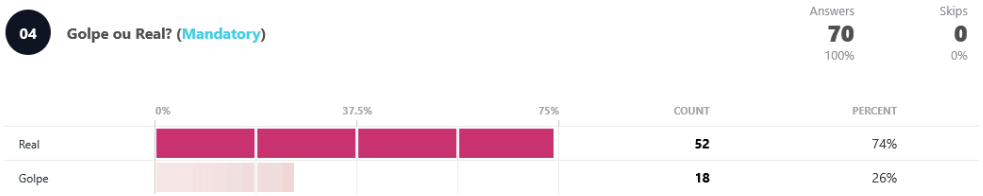

Figura 7. Pergunta referente a golpe de e-mail falso

Em relação às Perguntas 4, 8 e 10, as taxas de acerto foram respectivamente: 94% - Apenas 4 respostas erradas; 96% - Apenas 3 respostas erradas; 93% - Apenas 5 respostas erradas. De forma geral, os usuários que responderam o teste não tiveram dificuldades com os temas de ataques utilizando Inteligência Artificial, nem em relação a conhecimentos gerais sobre golpes digitais. Supõe-se que, devido à quantidade de alertas através das notícias divulgando o uso de Inteligência Artificial para esse tipo de fraude, houve uma atenção maior dos usuários na hora de responder às perguntas.

Baseado em todos os dados coletados, os resultados se mostraram positivos, pois evidenciam um bom conhecimento dos usuários que responderam o teste no entendimento do tema. Estes usuários, de modo geral, conseguem identificar os ataques, e usualmente sabem quais atitudes tomar para evitar cair nestes golpes.

5. Trabalhos Relacionados

Com frequência, as ferramentas no contexto de avaliação em relação à Segurança da Informação são desenvolvidas por empresas, e muitas vezes os resultados não são divulgados, o conteúdo em si abordado é desatualizado ou é focado para poucos tipos de cenários de golpes. Na Tabela 2 observa-se a análise e comparação feita em 4 diferentes sites.

De acordo com as soluções disponíveis analisadas, percebe-se uma limitação nos cenários simulados, onde geralmente os mesmos focam em tentativas de golpe por e-mail ou sites falsos. Com exceção do teste do Google, é presente a barreira linguística

pelo fato dos testes serem desenvolvidos todos em inglês. Os testes apresentam explicações para as respostas, com exceção da ferramenta do PhishingBox, contudo, nota-se a ausência de indicação de materiais educativos após a realização do teste.

Tabela 2. Comparação entre testes de phishing online

Soluções encontradas	Link para realizar o teste	Explica as respostas?	Indica material educativo?	Idioma
Google	https://phishingquiz.withgoogle.com	Sim	Não	Português
OpenDNS	https://www.opendns.com/phishing-quiz/	Sim	Não	Inglês
SonicWall	https://www.sonicwall.com/phishing-iq-test	Sim	Não	Inglês
PhishingBox	https://www.phishingbox.com/phishing-iq-test/	Não	Não	Inglês

Comparando os outros trabalhos apresentados na Tabela 2, o De Olho na Isca possui seu conteúdo em Português, ponto presente apenas na ferramenta do Google. Essa opção de idioma facilita a acessibilidade por parte do usuário, principalmente para um público-alvo voltado para o Brasil. O De Olho na Isca também possui a presença de materiais educativos sobre o tema de golpes online, que é uma característica ausente nas demais ferramentas, e é importante por conta da necessidade de conscientização e divulgação das informações para proteção das pessoas. Os materiais educativos são fornecidos pelo governo brasileiro por meio do Comitê Gestor da Internet no Brasil, e são materiais que recebem atualizações frequentes. Por fim, o De Olho na Isca também aborda em suas perguntas os cenários de golpe por redes sociais e chamadas falsas com uso de Inteligência Artificial, golpes que não estão presentes nas soluções analisadas, e fornece explicações breves para cada resposta correta, para que o usuário aprenda enquanto realiza o teste. Apenas a ferramenta do Google também apresenta golpes de SMS, as demais ferramentas abordam principalmente *phishing* por e-mail ou golpes de sites falsos.

Em contrapartida, foi encontrado o *Quiz60+* [Santana e Amorim 2024] voltado para o público idoso. O *quiz* é baseado em notícias de golpes virtuais que mais atingem essa parcela da população, abrangendo o tema de contas falsas em redes sociais, por exemplo. Foi desenvolvido em formato de aplicativo *mobile* Android, diferentemente do De Olho na Isca, que foi disponibilizado via website com suporte para desktop e dispositivo móvel. Em comparação com o *Quiz60+*, para seleção do público-alvo do De Olho na Isca desconsiderou-se a faixa etária dos usuários, ao invés disso foi considerado a relação dos usuários com tecnologias e os conceitos de Segurança da Informação. Por fim, observa-se no De Olho na Isca a preocupação com a divulgação de conteúdos educativos sobre o tema da Segurança Digital.

6. Conclusões e Trabalhos Futuros

A importância da conscientização em Segurança da Informação, nos dias atuais, é evidente. Contudo, apesar de já existirem ferramentas e *quiz* sobre *phishing* na internet, em particular alguns exemplos não abrangem o cenário atual da população brasileira, não são fáceis e acessíveis para o público interagir, e não é feito um trabalho de

incentivo à divulgação de materiais de apoio sobre o tema. Identificou-se como importante que a ferramenta desenvolvida abrangesse diversos cenários de golpes digitais, como golpes através de SMS, ligação telefônica, redes sociais, e-mail e golpes utilizando Inteligência Artificial. Estes cenários estão alinhados com os golpes de Engenharia Social que vêm sendo comumente abordados no Brasil.

O *quiz* desenvolvido mostra que existe um bom conhecimento geral das pessoas que responderam o teste sobre essas técnicas da Engenharia Social, pois referente às perguntas sobre golpes de SMS e de ligação telefônica, a taxa de acerto foi de 99%, com apenas 1 resposta errada em ambas as perguntas. Em contraponto, nas perguntas referentes a golpes através de redes sociais, percebe-se a necessidade de mais divulgação acerca de como os golpes funcionam, quais as estratégias de Engenharia Social que são aplicadas e como se prevenir.

Como limitações da pesquisa, pode-se considerar a limitação do próprio CrowdSignal, ferramenta utilizada para desenvolver o *quiz*, pois a sua versão gratuita não permite grandes customizações, o que pode afetar a visualização na hora do usuário responder ao teste. Além disso, embora se objetivou ter um escopo maior com a escolha de perguntas de diferentes temas dentro da Segurança da Informação, é fato que existem outros tópicos e ataques relevantes que não puderam ser avaliados, e isto limita o alcance dos resultados obtidos.

Como continuidade da pesquisa, planeja-se expandir e aprimorar o *quiz*, adicionando uma parte com um questionário relacionado ao usuário em si, solicitando informações como faixa etária e escolaridade, por exemplo. Desta forma, poderão ser feitas perguntas mais direcionadas, avaliando melhor o público-alvo considerando diferentes níveis de conhecimento inicial. No questionário para o usuário, também pretende-se solicitar que ele indique o grau de conhecimento que ele possui na área de Segurança da Informação. Esse dado poderá apresentar outra perspectiva em relação às respostas. Outro ponto a ser aprimorado é a criação de perguntas que auxiliem a identificar as áreas em que os usuários possuem mais dificuldade. Por exemplo, no contexto das perguntas relacionadas a golpes através das redes sociais, pode-se perguntar para o usuário quais perguntas ele identificou como mais difíceis e por quê. Isso permitirá uma análise mais aprofundada das dificuldades enfrentadas.

Referências

Ahmad, N., Laplante, P. A., DeFranco, J. F. and Kassab, M. (2022). A Cybersecurity Educated Community. IEEE Transactions on Emerging Topics in Computing, 10:1456-1463.

Cert.br, NIC.br, e CGI.br. (2020). Cidadão na Rede. Disponível em: https://cidadaonarede.nic.br/pt/. Acesso em: 06 mar. 2025.

Cert.br, NIC.br, e CGI.br. (2022). Fascículos. Disponível em: https://cartilha.cert.br/fasciculos/. Acesso em: 28 fev. 2025.

Cert.br, NIC.br, e CGI.br. (2017). Internet Segura. Disponível em: https://internetsegura.br/. Acesso em: 06 mar. 2025.

CGSI, DSI, e AssESI. (2022). Cartilha de gestão de segurança da informação. Disponível em: https://www.gov.br/gsi/pt-br/ssic/cartilha-de-gestao-de-seguranca-da-informacao/CartilhadeSegurancaInformao.pdf. Acesso em: 22 fev. 2025.

Couto, T. F., Santos, C. M., Travaglia, G., Pereira, H. I. e Mallmann, J. S. (2023). Quiz como ferramenta de avaliação. Anais Do II Congresso Brasileiro On-Line de Ensino, Pesquisa E Extensão. https://doi.org/10.51189/ii-ensipex/13607

Folhapress. (2024). Criminosos usam inteligência artificial para aplicar cinco novos golpes; veja como se proteger. Disponível em: https://portalcorreio.com.br/criminosos-usam-inteligencia-artificial-para-aplicar-cinco-novos-golpes-veja-como-se-proteger/. Acesso em: 19 fev. 2025.

Framer. (2013). Framer. Disponível em: https://www.framer.com. Acesso em 06 mar. 2025.

G1. (2024). Operação busca prender 15 suspeitos de aplicar golpes digitais com prejuízo de R$ 1 milhão a vítimas em SP. Disponível em: https://g1.globo.com/sp/ribeirao-preto-franca/noticia/2024/11/18/operacao-busca-prender-15-suspeitos-de-aplicar-golpes-digitais-com-prejuizo-de-r-1-milhao-a-vitimas-em-sp.ghtml. Acesso em: 15 fev. 2025.

Google. (2019). Teste sobre phishing. Disponível em: https://phishingquiz.withgoogle.com. Acesso em: 8 fev. 2025.

Gupta, S., Singhal, A., Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. 2016 International Conference on Computing, Communication and Automation (ICCCA), 537-540.

Instituto de Pesquisa DataSenado. (2024). Panorama Político 2024: Apostas esportivas, golpes digitais e endividamento. Disponível em: https://www12.senado.leg.br/institucional/datasenado/materias/relatorios-de-pesquisa/golpes-digitais-atingem-24-dos-brasileiros-aponta-21a-edicao-da-pesquisa-panorama-politico. Acesso em: 15 fev. 2025.

Kaspersky Team. (2024). Ataques contra celular crescem 70% e atingem número histórico na América Latina. Disponível em: https://www.kaspersky.com.br/blog/panorama-ameacas-latam-2024/22888/. Acesso em: 14 fev. 2025.

Machado, S. (2024). 'Eram meu rosto e minha voz, mas era golpe': como criminosos 'clonam pessoas' com inteligência artificial. Disponível em: https://www.bbc.com/portuguese/articles/cd1jv45dq3go. Acesso em: 15 fev. 2025.

Miato, B. e Nicoceli, A. (2024). Datafolha: Brasil tem quase 4.700 tentativas de 'golpe do 0800' por hora. Disponível em: https://g1.globo.com/economia/noticia/2024/08/13/datafolha-brasil-tem-quase-4700-tentativas-de-golpe-do-0800-por-hora.ghtml. Acesso em: 19 fev. 2025.

Mitnick, K. D. e Simon, W. L. (2003), A Arte de Enganar, Trad. São Paulo: Pearson Education do Brasil.

Nuci, K.P., Tahir, R., Wang, A. I. e Imran, A. S. (2021). Game-Based Digital Quiz as a Tool for Improving Students' Engagement and Learning in Online Lectures. IEEE Access, 9:91220-91234.

Santana, M. C. e Amorim, S. S. (2024). Quiz60+: Um Jogo Educativo para Segurança Digital dos Usuários Idosos. Anais do Seminário SJEEC Jogos Eletrônicos, Educação e Comunicação. https://doi.org/10.5281/zenodo.11270846

Wang, Z., Zhu, H., and Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. IEEE Access, 9:11895–11910