ANAIS DO SEMINÁRIO DE BOAS PRÁTICAS DE ENSINO E APRENDIZAGEM (SBPEA) DA EEL-USP
VIII SBPEA – 03 DE DEZEMBRO DE 2025

Simulação de Phishing como Estratégia Pedagógica para Conscientização em Cibersegurança: Experiência em Ambiente Educacional.

Victor Soares de Miranda
Instituto Federal do Pará *(codecipher7743@gmail.com)*

Luana Rabelo dos Santos
Instituto Federal do Pará *(luanasants290@gmail.com)*

Jacqueline Cristina Teixeira do Rosário
Instituto Federal do Pará *(jacqueteixeira25@gmail.com)*

Resumo

Este estudo investiga vulnerabilidades humanas em segurança da informação através de simulação controlada de ataque de *phishing* em ambiente educacional. O objetivo foi mensurar a taxa de sucesso de campanha simulada no Instituto Federal do Pará (IFPA), Campus Vigia, fornecendo dados para programas de conscientização em cibersegurança. A metodologia envolveu cenário controlado utilizando *QR Code* direcionando para página de *feedback* falsa sobre oficina de robótica educacional sustentável, com monitoramento durante 30 minutos. Os resultados demonstraram captura de 8 credenciais nos primeiros 5 minutos e identificação de mais de 60 endereços IP, evidenciando vulnerabilidade significativa a técnicas de engenharia social. A análise revelou taxa de interação de 34% e conversão de 18%, confirmando que vulnerabilidades humanas representam vetor crítico de ataque. O estudo reforça a importância da educação em segurança digital, onde docentes, discentes e servidores necessitam desenvolver competências para identificação de ameaças cibernéticas. Conclui-se que a conscientização em cibersegurança constitui elemento crítico na proteção institucional. Como desdobramento, estão planejadas ações educativas incluindo palestras, oficinas e

minicursos para capacitar toda a comunidade acadêmica em identificação e prevenção de ameaças digitais.

Palavras-chave: Phishing, Engenharia Social, Cibersegurança, Educação em Segurança Digital, Vulnerabilidades Humanas.

Abstract

This study investigates human vulnerabilities in information security through a controlled phishing attack simulation in an educational environment. The objective was to measure the success rate of a simulated campaign at the Federal Institute of Pará (IFPA), Vigia Campus, providing data for cybersecurity awareness programs. The methodology involved a controlled scenario using a QR Code directing to a fake feedback page about a sustainable educational robotics workshop, with 30-minute monitoring. Results demonstrated capture of 8 credentials in the first 5 minutes and identification of over 60 IP addresses, evidencing significant vulnerability to social engineering techniques. Analysis revealed 34% interaction rate and 18% conversion, confirming that human vulnerabilities represent a critical attack vector. The study reinforces the importance of digital security education, where faculty, students, and staff need to develop competencies for identifying cyber threats. It is concluded that cybersecurity awareness constitutes a critical element in institutional protection. As a follow-up, educational actions are planned including lectures, workshops, and short courses to train the entire academic community in identifying and preventing digital threats.

Keywords: Phishing, Social Engineering, Cybersecurity, Digital Security Education, Human Vulnerabilities.

Resumen

Este estudio investiga las vulnerabilidades humanas en seguridad de la información a través de una simulación controlada de ataque de phishing en ambiente educativo. El objetivo fue medir la tasa de éxito de una campaña simulada en el Instituto Federal de Pará (IFPA), Campus Vigia, proporcionando datos para programas de concienciación en ciberseguridad. La metodología involucró un escenario controlado utilizando código QR dirigiendo a una página de retroalimentación falsa sobre un taller

de robótica educativa sustentable, con monitoreo durante 30 minutos. Los resultados demostraron la captura de 8 credenciales en los primeros 5 minutos e identificación de más de 60 direcciones IP, evidenciando vulnerabilidad significativa a técnicas de ingeniería social. El análisis reveló tasa de interacción de 34% y conversión de 18%, confirmando que las vulnerabilidades humanas representan vector crítico de ataque. El estudio refuerza la importancia de la educación en seguridad digital, donde docentes, discentes y servidores necesitan desarrollar competencias para identificación de amenazas cibernéticas. Se concluye que la concienciación en ciberseguridad constituye elemento crítico en la protección institucional. Como continuación, se planean acciones educativas incluyendo charlas, talleres y minicursos para capacitar a toda la comunidad académica en identificación y prevención de amenazas digitales.

Palabras clave: Phishing, Ingeniería Social, Ciberseguridad, Educación en Seguridad Digital, Vulnerabilidades Humanas.

1. INTRODUÇÃO

A transformação digital acelerada nas últimas décadas trouxe benefícios significativos para instituições educacionais, ampliando possibilidades de ensino-aprendizagem, mas também expandiu a superfície de ataque para ameaças cibernéticas. Neste contexto, a segurança da informação tornou-se preocupação estratégica fundamental para a continuidade das atividades educacionais e proteção de dados institucionais e pessoais da comunidade acadêmica.

Embora investimentos massivos sejam direcionados para soluções tecnológicas de cibersegurança, como *firewalls*, sistemas de detecção de intrusão e criptografia, o elemento humano permanece como o elo mais vulnerável na cadeia de proteção, conforme demonstrado por Schneier (2015) ao estabelecer que segurança é um processo contínuo que depende fundamentalmente do comportamento humano, não apenas de produtos tecnológicos.

O *phishing* representa uma das técnicas de ataque mais prevalentes no cenário atual de ameaças cibernéticas, explorando vulnerabilidades psicológicas e comportamentais dos usuários (MITNICK; SIMON, 2002). Diferentemente de ataques técnicos, o *phishing* manipula fatores humanos como confiança, urgência, autoridade e medo, princípios documentados por Cialdini (2021) em sua obra sobre persuasão e influência.

De acordo com a Verizon (2024), que analisou 30.458 incidentes de segurança e 10.626 violações confirmadas de dados, aproximadamente 68% das violações envolvem elemento humano, seja por meio de *phishing*, uso de credenciais roubadas ou erro humano. Este dado evidencia que as vulnerabilidades comportamentais representam vetor de ataque mais significativo que falhas puramente técnicas em sistemas computacionais.

No contexto educacional, essa vulnerabilidade se torna ainda mais crítica, considerando a diversidade de perfis de usuários (docentes, discentes, técnicos administrativos) com diferentes níveis de familiaridade tecnológica e a natureza colaborativa e aberta característica de ambientes de ensino, que podem facilitar a exploração de técnicas de engenharia social.

Este estudo teve como objetivo avaliar a vulnerabilidade de usuários em instituição educacional através da simulação de campanha de *phishing* combinada com técnicas de engenharia social, fornecendo informações para desenvolvimento de estratégias pedagógicas de conscientização em cibersegurança. A pesquisa buscou quantificar a taxa de sucesso do ataque, o tempo médio de resposta das vítimas e o alcance da campanha em termos de dispositivos comprometidos.

Os resultados obtidos fornecem dados importantes para compreensão da dimensão do risco humano em segurança da informação e fundamentam a necessidade de programas de conscientização e treinamento em cibersegurança, conforme recomendado por Krombholz *et al*. (2015) em sua análise de ataques avançados de engenharia social.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Conceitos de Segurança da Informação e Cibersegurança

A segurança da informação é definida como conjunto de práticas, processos e tecnologias destinados a proteger informações contra acesso não autorizado, uso indevido, divulgação, destruição ou modificação. Neste sentido, Whitman e Mattord (2021) estabelecem que os pilares fundamentais da segurança da informação são determinados pela tríade CID, composta por Confidencialidade (garantia de que informações sejam acessíveis apenas a pessoas autorizadas), Integridade (assegurar que dados não sejam alterados de forma não autorizada) e Disponibilidade (garantir que informações e recursos estejam acessíveis quando necessário).

A cibersegurança, por sua vez, representa subconjunto especializado da segurança da informação, focado especificamente na proteção de sistemas computacionais, redes e dados digitais contra ameaças cibernéticas. De acordo com Anderson (2020) que destaca que com a crescente digitalização de processos organizacionais e a expansão da conectividade, a cibersegurança tornou-se componente essencial de estratégia empresarial, isso inclui também instituições de ensino, exigindo implementação de camadas múltiplas de defesa que combinem controles técnicos, administrativos e físicos para mitigar riscos de forma efetiva.

Schneier (2015) argumenta que a segurança não pode ser tratada como produto que se adquire e instala, mas sim como processo contínuo que requer vigilância constante, atualização de controles e adaptação a novas ameaças. O autor enfatiza que investimentos exclusivos em tecnologia, ignorando o fator humano, resultam em falsa sensação de segurança, uma vez que atacantes exploram sistematicamente vulnerabilidades comportamentais para contornar barreiras tecnológicas sofisticadas.

No contexto educacional, a segurança da informação adquire dimensão adicional, uma vez que instituições de ensino são responsáveis não apenas pela proteção de seus próprios sistemas, mas também pela formação de cidadãos digitalmente conscientes. A educação em cibersegurança torna-se, portanto, componente essencial do processo formativo contemporâneo.

2.2 Phishing e Engenharia Social

O termo *phishing* deriva da palavra inglesa "*fishing*" (pescaria) e representa técnica de ataque cibernético baseada em engano e manipulação psicológica. As autores Mitnick e Simon (2002) definem engenharia social como a arte de explorar a tendência natural humana de confiar, estabelecendo que é consideravelmente mais fácil manipular pessoas a revelarem informações confidenciais do que explorar vulnerabilidades técnicas em sistemas bem configurados. Os autores documentam casos reais onde atacantes obtiveram acesso a sistemas críticos simplesmente solicitando credenciais por telefone, fazendo-se passar por técnicos de suporte.

Krombholz *et al.* (2015) apresentam taxonomia detalhada de ataques de engenharia social, classificando o *phishing* em diversas variantes. Segundo eles, o *spear phishing* representa forma direcionada do ataque, onde o criminoso personaliza a mensagem para vítima específica ou grupo reduzido, utilizando informações coletadas previamente sobre o alvo através de redes sociais ou vazamentos de dados. O *whaling* foca especificamente em executivos de alto escalão e tomadores de

decisão organizacionais, frequentemente simulando comunicações de parceiros de negócios ou autoridades regulatórias. O *vishing* utiliza chamadas telefônicas como vetor de ataque, enquanto o *smishing* emprega mensagens SMS para distribuir links maliciosos.

Cialdini (2021) identifica seis princípios fundamentais de persuasão que são sistematicamente explorados em ataques de engenharia social, sendo eles:

- O princípio da reciprocidade, que explora a tendência humana de retribuir favores, mesmo quando não solicitados;
- O princípio da autoridade aproveita a inclinação natural em obedecer figuras percebidas como autoridades legítimas, razão pela qual atacantes frequentemente se fazem passar por executivos, agentes governamentais ou especialistas técnicos;
- O princípio da escassez cria senso de urgência através da sugestão de oportunidade limitada no tempo ou quantidade;
- O princípio da prova social utiliza comportamento de outros como validação, sugerindo que "todos estão fazendo" determinada ação, e
- Os princípios de simpatia e compromisso/coerência completam o arsenal de técnicas de manipulação psicológica.

2.3 Panorama Atual de Ameaças

O relatório da Verizon (2024) fornece análise abrangente do panorama de ameaças contemporâneas, baseada em dados de 30.458 incidentes de segurança globais. O relatório confirma que 68% das violações de dados envolvem elemento humano, seja através de engenharia social, erro humano, uso indevido de privilégios ou uso de credenciais roubadas. Esta estatística comprova a premissa fundamental de que vulnerabilidades humanas representam vetor de ataque mais significativo que falhas puramente técnicas.

Dados bem relevantes ainda do relatório da Verizon (2024) indicam que o *phishing* continua sendo método inicial de comprometimento em parcela substancial dos incidentes. A janela temporal de resposta dos usuários é criticamente curta, apresentando desafio significativo para controles de detecção e resposta, pois o dano pode estar consumado antes que qualquer alerta seja processado. O relatório também documenta evolução na sofisticação dos ataques.

Segundo a Verizon (2024), campanhas de *phishing* contemporâneas empregam técnicas avançadas de falsificação de domínios, certificados SSL válidos para páginas maliciosas, e exploração de eventos atuais ou contextos específicos das vítimas para aumentar credibilidade. Durante a pandemia de COVID-19, observou-se crescimento exponencial em tentativas de *phishing* relacionadas a temas de saúde pública, demonstrando capacidade de atacantes de adaptarem rapidamente suas táticas a contextos emergentes (VERIZON, 2024).

2.4 Importância da Conscientização em Segurança

A literatura em cibersegurança reconhece amplamente que tecnologia sozinha não é suficiente para proteção adequada contra ameaças modernas. Autores como Schneier (2015) estabelece que o fator humano representa tanto a maior vulnerabilidade quanto a linha de defesa mais importante em qualquer sistema de segurança. Programas de conscientização em segurança da informação são fundamentais para desenvolver cultura organizacional onde todos os colaboradores compreendem seu papel na proteção de ativos digitais.

Mitnick e Simon (2002) argumentam que educação e treinamento de usuários devem ser prioridade estratégica, equiparando-se em importância aos investimentos em ferramentas tecnológicas. Os autores demonstram através de casos práticos que organizações com programas robustos de conscientização apresentam taxas significativamente menores de comprometimento, pois usuários treinados são capazes de identificar sinais de tentativas de engenharia social e seguir protocolos apropriados de reporte e verificação.

Krombholz *et al.* (2015) recomendam que treinamentos efetivos devem ir além de apresentações teóricas, incorporando simulações práticas de *phishing*, exercícios interativos e feedback personalizado. A repetição periódica é essencial, pois o conhecimento em segurança tende a degradar-se ao longo do tempo sem reforço regular. Métricas de efetividade, como taxa de cliques em simulações controladas e tempo médio de reporte de mensagens suspeitas, permitem avaliar o progresso organizacional e identificar áreas que necessitam atenção adicional.

3. MÉTODO

3.1 Caracterização da Pesquisa

Esta pesquisa caracteriza-se como estudo de caso experimental em ambiente controlado, com abordagem quantitativa para análise dos dados coletados. Segundo Prodanov e Freitas (2013), a abordagem quantitativa parte do princípio de que qualquer aspecto pode ser mensurado, transformando opiniões e informações em valores numéricos para possibilitar sua classificação e análise. Essa perspectiva exige o emprego de diferentes recursos e técnicas estatísticas, como percentuais, medidas de tendência central e de dispersão, além de correlações e análises de regressão.

O objetivo foi avaliar a vulnerabilidade de usuários a ataques de *phishing* e técnicas de engenharia social, mensurando taxas de sucesso, velocidade de comprometimento e alcance da campanha simulada. O estudo foi conduzido com aprovação prévia da administração da organização participante e seguiu rigorosos princípios éticos, garantindo que nenhum dado sensível fosse efetivamente comprometido, conforme recomendações de Mitnick e Simon (2002) para condução de testes de segurança éticos.

3.2 Ambiente de Teste

O ambiente de teste foi estabelecido no Instituto Federal do Pará (IFPA) – Campus Vigia, com aproximadamente 200 usuários ativos entre corpo docente, administrativo e discente. A escolha por ambiente educacional justifica-se pela diversidade de perfis de usuários e níveis variados de familiaridade com tecnologia, proporcionando amostra representativa para avaliação de vulnerabilidades humanas, conforme metodologia sugerida por Krombholz *et al*. (2015) para estudos de engenharia social em contextos organizacionais.

A infraestrutura técnica foi preparada com antecedência, incluindo servidor *web* isolado hospedando a página de *feedback* falsificada, sistema de captura e registro de credenciais, mecanismos de *logging* para rastreamento de endereços IP e *timestamps* (marcações temporais que registram quando um evento específico ocorreu), e ferramentas de análise para processamento dos dados coletados. Certificado SSL (*Secure Sockets Layer*), que é um protocolo de segurança que cria uma conexão criptografada entre um servidor web e um navegador, válido foi implementado para conferir maior credibilidade à página falsa, replicando técnicas documentadas por Anderson (2020) como práticas comuns em ataques sofisticados de *phishing*.

3.3 Planejamento da Campanha

A campanha de *phishing* foi cuidadosamente planejada para simular cenário realista de ataque, aplicando princípios de engenharia social documentados por Cialdini (2021) e Mitnick e Simon (2002). O cenário escolhido foi uma página de *feedback* sobre uma oficina de Robótica Educacional Sustentável realizada no IFPA, campus da cidade de Vigia-PA. Este contexto foi especificamente selecionado por sua relevância institucional e pela naturalidade da solicitação de *feedback* após eventos educacionais.

O vetor de distribuição escolhido foi um *QR Code*, amplamente utilizado em ambientes educacionais para facilitar acesso rápido a formulários e recursos digitais. *QR Codes* foram distribuídos fisicamente no campus através de cartazes e materiais impressos, simulando comunicação legítima do departamento organizador da oficina. Esta abordagem explora a familiaridade crescente com tecnologia de *QR Code* e a confiança geralmente depositada em comunicações físicas institucionais.

O design da página de *phishing* replicou fielmente uma interface de formulário de *feedback*, incluindo logotipo oficial do instituto, esquema de cores institucionais, perguntas típicas de avaliação de eventos e solicitação de login para "garantir autenticidade das respostas e possibilitar certificado de participação". Essa justificativa para coleta de credenciais foi elaborada para explorar o princípio de reciprocidade (oferta de certificado) combinado com autoridade institucional. O nível de sofisticação representa fidelidade às técnicas realmente empregadas por atacantes em cenários reais, conforme documentado na Verizon (2024).

3.4 Execução do Experimento

A execução da campanha ocorreu durante horário comercial regular, momento de maior atividade dos usuários no campus. Esta escolha temporal fundamenta-se em dados do *2024 Data Breach Investigations Report* (DBIR), que é um relatório técnico anual publicado pela Verizon Enterprise Solutions, o qual indicam maior taxa de sucesso de ataques de *phishing* durante períodos de alta carga de trabalho, quando usuários estão sob pressão e menos propensos a verificações cuidadosas (VERIZON, 2024).

Os *QR Codes* foram distribuídos estrategicamente em locais de alta circulação no campus, incluindo murais de avisos, corredores principais e áreas de convivência. O monitoramento iniciou-se imediatamente após a distribuição dos materiais, com registro automático de todos os acessos à página

falsificada, incluindo *timestamp* preciso, endereço IP de origem, *user-agent* do navegador , que é uma identificação que o navegador ou aplicativo envia a um servidor sempre que um usuário acessa um site, e, quando aplicável, credenciais inseridas.

A operação teve duração total de 30 minutos, período considerado suficiente para avaliação da resposta inicial dos usuários e identificação de padrões de comportamento. Este intervalo temporal também representa janela crítica em ataques reais, onde respostas rápidas de vítimas aumentam significativamente o sucesso do ataque antes que mecanismos de defesa sejam ativados ou alertas de segurança sejam disseminados.

3.5 Coleta e Análise de Dados

Os dados foram coletados automaticamente através de sistema de *logging* implementado no servidor web. As métricas principais incluíram número total de acessos únicos à página de *phishing*, quantidade de credenciais capturadas, distribuição temporal dos acessos, diversidade de endereços IP registrados e taxa de conversão entre visualizações da página e submissão de credenciais. Análise complementar examinou distribuição por departamentos organizacionais e padrões de horário de maior vulnerabilidade.

Imediatamente após conclusão do período de teste, todos os usuários que interagiram com a campanha foram contatados individualmente, recebendo explicação detalhada sobre natureza experimental do teste, *feedback* personalizado sobre vulnerabilidades identificadas e orientações específicas para reconhecimento de tentativas futuras de *phishing*. Esta abordagem de *debriefing* imediato segue recomendações de Mitnick e Simon (2002) para maximizar valor educacional de simulações de segurança.

Nenhuma credencial real foi armazenada de forma persistente, e todos os dados coletados foram tratados com confidencialidade absoluta, seguindo princípios éticos estabelecidos por Schneier (2015) para pesquisa em segurança da informação.

4. RESULTADOS E DISCUSSÃO

4.1 Resultados Gerais da Campanha

A campanha de *phishing* demonstrou níveis alarmantes de eficácia, evidenciando vulnerabilidade significativa dos usuários a técnicas de engenharia social. Dos aproximadamente 200 potenciais

participantes no campus, a página de *phishing* registrou 68 acessos únicos ao longo dos 30 minutos de operação, representando taxa de interação de 34%. Este percentual é substancialmente superior à taxa típica de 10 a 15% observada em campanhas de *phishing* genéricas, mas alinha-se com expectativas para ataques personalizados e contextualizados, conforme documentado por Krombholz *et al*. (2015) e reforçando a necessidade de integração de práticas educativas de segurança digital na formação da comunidade acadêmica.

A análise de endereços IP revelou mais de 60 dispositivos distintos acessando a página falsificada durante o período experimental, confirmando alcance amplo da campanha através de diferentes segmentos da organização. Está métrica válida a observação de Mitnick e Simon (2002) de que vulnerabilidade humana não está concentrada em perfil específico de usuários, mas distribui-se amplamente pela população organizacional, reforçando necessidade de programas de conscientização abrangentes que alcancem todos os níveis hierárquicos e funcionais.

Das 68 visualizações da página de *phishing*, 12 usuários procederam com inserção e submissão de suas credenciais, resultando em taxa de conversão de aproximadamente 18%. Esta proporção indica que além da vulnerabilidade à escaneamento inicial do *QR Code*, parcela substancial dos usuários também está suscetível a revelar informações confidenciais quando confrontada com página de login convincente contextualizada em cenário familiar. Estes números são consistentes com dados apresentados na Verizon (2024), que indica elevada propensão de usuários a comprometerem credenciais em situações que aparentam legitimidade institucional.

4.2 Velocidade de Comprometimento

Um dos resultados mais preocupantes relaciona-se à velocidade com que usuários responderam ao ataque. Nos primeiros 5 minutos após distribuição dos *QR Codes*, 8 usuários já haviam submetido suas credenciais na página falsificada. Esta rapidez na resposta demonstra eficácia da combinação entre familiaridade do contexto (*feedback* de oficina educacional) e conveniência do método de acesso (*QR Code*), conforme previsto pela teoria de persuasão de Cialdini (2021). Em cenário real de ataque, esta janela temporal de 5 minutos seria suficiente para atacante estabelecer acesso inicial aos sistemas, potencialmente iniciando movimento lateral na rede antes que qualquer medida de contenção pudesse ser acionada.

A distribuição temporal dos acessos revelou pico concentrado nos primeiros 15 minutos, com 75% dos escaneamentos do *QR Code* ocorrendo neste intervalo. Este padrão sugere que usuários tendem

a responder imediatamente quando encontram material institucional aparentemente legítimo em locais familiares do campus, validando a observação de Schneier (2015) de que contexto familiar reduz vigilância e compromete julgamento crítico. Após os 15 minutos iniciais, a taxa de novos acessos diminuiu significativamente, possivelmente devido a comunicações informais entre colegas sobre natureza suspeita do formulário, demonstrando que redes sociais internas podem funcionar como mecanismo de defesa coletiva não-intencional.

4.3 Validação dos Princípios de Engenharia Social

Os resultados confirmam empiricamente a eficácia dos princípios psicológicos de persuasão documentados por Cialdini (2021) e aplicados em contexto de engenharia social por Mitnick e Simon (2002). O princípio de reciprocidade, materializado através da oferta de certificado de participação em troca do login, demonstrou capacidade notável de motivar usuários a fornecerem credenciais. A análise qualitativa pós-experimento revelou que diversos participantes consideraram a solicitação de login razoável justamente pela promessa de um benefício real (certificado).

O princípio de autoridade foi reforçado através de múltiplos elementos: a presença física de materiais impressos no campus, o uso de identidade visual institucional, e o contexto de evento educacional real que havia ocorrido recentemente. Entrevistas com participantes indicaram que a combinação destes elementos conferiu legitimidade imediata à solicitação, validando a análise de Krombholz *et al.* (2015) sobre importância de contextualização detalhada em ataques bem-sucedidos de *phishing*.

A familiaridade com práticas institucionais de coleta de *feedback* através de formulários digitais foi explorada para criar senso de normalidade, demonstrando como experiência prévia pode paradoxalmente aumentar vulnerabilidade ao estabelecer padrões de resposta automática. O uso de *QR Code*, tecnologia amplamente adotada em ambientes educacionais especialmente após a pandemia de COVID-19, contribuiu significativamente para redução de suspeita inicial.

4.4 Implicações para Segurança em Ambientes Educacionais

Os resultados obtidos evidenciam que vulnerabilidades humanas representam risco crítico para segurança de instituições educacionais, frequentemente superando vulnerabilidades técnicas em termos de probabilidade de exploração e potencial de impacto, conforme argumentado por Schneier (2015). A taxa de comprometimento de 18% dos usuários que acessaram a página de *phishing*

demonstra que investimentos exclusivos em soluções tecnológicas, negligenciando dimensão humana da segurança, deixam organizações substancialmente expostas a ataques de engenharia social.

Anderson (2020) estabelece que sistemas de segurança efetivos devem incorporar múltiplas camadas de defesa, incluindo controles técnicos, administrativos e educacionais. Os dados do presente estudo confirmam esta necessidade, pois mesmo em ambiente com infraestrutura tecnológica adequada (*firewall*, antivírus, filtros de rede), o fator humano permaneceu como vetor de comprometimento viável.

A distribuição ampla de acessos através de mais de 60 dispositivos indica que superfície de ataque humano é extensa e heterogênea, tornando abordagens de conscientização segmentadas insuficientes. No ambiente educacional, isso demanda programas de educação em segurança digital que abranjam toda a comunidade acadêmica, desde estudantes iniciantes até gestores e docentes

A captura de 8 credenciais em apenas 5 minutos demonstra que janela de oportunidade para atacantes é extremamente curta, exigindo capacidade de detecção e resposta igualmente rápida. Este resultado sublinha importância de implementação de controles compensatórios, como autenticação multifator, que podem minimizar o impacto de credenciais comprometidas mesmo após resposta inicial bem-sucedida de usuário a tentativa de *phishing*.

O uso de *QR Code* como vetor adiciona camada de complexidade à detecção de ameaças, uma vez que filtros tradicionais de *e-mail* e *links* maliciosos não são efetivos contra distribuição física de códigos. Este achado destaca necessidade de conscientização que abranja múltiplos vetores de ataque, não se limitando a ameaças digitais tradicionais. A formação em segurança digital deve, portanto, incorporar conhecimento sobre tecnologias emergentes e seus riscos associados, preparando a comunidade educacional para identificar ameaças em constante evolução.

4.5 Limitações e Trabalhos Futuros

Reconhece-se que este estudo possui limitações inerentes a sua metodologia e escopo. O ambiente educacional selecionado pode não ser perfeitamente representativo de contextos corporativos, particularmente organizações com cultura de segurança mais madura ou setores altamente regulados. A amostra de aproximadamente 200 usuários, embora adequada para demonstração de vulnerabilidades, é relativamente pequena para generalização estatística ampla. A duração limitada

da campanha (30 minutos) captura apenas fase inicial de potencial ataque, não explorando comportamento de longo prazo ou efeitos de comunicações de alerta subsequentes.

O uso de *QR Code* como vetor específico pode apresentar resultados diferentes em organizações com menor familiaridade com esta tecnologia. Estudos futuros poderiam comparar eficácia de diferentes vetores *(e-mail,* SMS*, QR Code, links* em redes sociais) no mesmo ambiente organizacional para identificar vulnerabilidades relativas.

Como desdobramento desta pesquisa e visando mitigar as vulnerabilidades identificadas, estão planejadas ações educativas sistematizadas junto à comunidade acadêmica do IFPA - Campus Vigia. Serão desenvolvidos palestras, oficinas e minicursos sobre segurança da informação e cibersegurança, abordando técnicas de identificação de phishing, boas práticas de proteção de credenciais e conscientização sobre engenharia social.

Estas iniciativas pedagógicas buscarão transformar os dados obtidos neste estudo em conhecimento aplicável, contribuindo para formação de uma cultura de segurança digital institucional e preparando toda a comunidade acadêmica – docentes, discentes e servidores – para atuar como primeira linha de defesa contra ameaças cibernéticas

5. CONSIDERAÇÕES FINAIS

Este estudo demonstrou, através de simulação controlada em ambiente educacional, vulnerabilidade significativa de docentes, discentes e servidores a ataques de *phishing* via *QR Code* e técnicas de engenharia social, confirmando a necessidade crítica de educação em segurança digital nas instituições de ensino. A captura de 8 credenciais em apenas 5 minutos de operação e identificação de mais de 60 endereços IP ao longo de 30 minutos evidenciam que fator humano representa vetor de ataque crítico que não pode ser negligenciado em estratégias de cibersegurança, validando argumentos centrais de Schneier (2015) e Mitnick e Simon (2002) sobre predominância das vulnerabilidades humanas sobre falhas puramente técnicas.

O uso de *QR Code* como vetor de ataque revelou-se particularmente eficaz, explorando a crescente familiaridade e confiança depositada nesta tecnologia em ambientes educacionais. A contextualização do ataque em cenário real e relevante, neste caso, o *feedback* sobre oficina de Robótica Educacional Sustentável no IFPA – Campus Vigia, demonstrou como atacantes podem explorar eventos legítimos e confiança institucional para aumentar taxa de sucesso de campanhas maliciosas.

Os resultados reforçam o consenso crescente na comunidade de segurança da informação de que proteção efetiva requer abordagem abrangente, combinando controles técnicos robustos com programas educacionais permanentes de conscientização e formação em segurança digital para docentes, discentes e servidores. A taxa de interação de 34% e taxa de conversão de 18% demonstram eficácia dos princípios psicológicos de persuasão documentados por Cialdini (2021), particularmente reciprocidade e autoridade, quando aplicados em contexto de engenharia social bem elaborado.

A velocidade observada no comprometimento, particularmente nos primeiros 5 minutos da campanha, reforça a urgência de programas educacionais preventivos em segurança digital. Instituições educacionais devem implementar abordagem integrada que priorize estratégias pedagógicas de conscientização permanente em cibersegurança, complementadas por controles técnicos como monitoramento contínuo, alertas automatizados e autenticação multifator, conforme recomendado por Anderson (2020).

A pesquisa também evidencia importância de simulações regulares e controladas de *phishing* como ferramenta educacional e avaliativa, seguindo diretrizes estabelecidas por Krombholz *et al.* (2015). Estas simulações permitem identificar áreas de maior vulnerabilidade, mensurar efetividade de iniciativas de treinamento e manter conscientização de usuários constantes através de exposição prática a técnicas de ataque diversificadas, incluindo ferramentas emergentes como o *QR Code*. Quando conduzidas eticamente, com *debriefing* adequado e foco em aprendizado em vez de punição, estas simulações representam investimento valioso em resiliência organizacional.

Em conclusão, a segurança da informação efetiva no cenário contemporâneo requer reconhecimento explícito de que humanos são simultaneamente o elo mais fraco e o recurso mais valioso na defesa cibernética. O desenvolvimento de cultura de segurança através de práticas educativas permanentes, onde toda a comunidade acadêmica compreende sua responsabilidade e desenvolve competências para identificar e responder apropriadamente a ameaças digitais, representa elemento fundamental da formação contemporânea em instituições de ensino. A integração da educação em cibersegurança ao processo formativo não apenas protege a instituição, mas prepara estudantes, docentes e servidores como cidadãos digitalmente conscientes e resilientes.

REFERÊNCIAS

ANDERSON, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3. ed. Indianapolis: Wiley, 2020.

CIALDINI, R. B. *Influence: The Psychology of Persuasion*. Revised ed. New York: Harper Business, 2021.

KROMBHOLZ, K.; HOBEL, H.; HUBER, M.; WEIPPL, E. Advanced Social Engineering Attacks. *Journal of Information Security and Applications*, v. 22, p. 113–122, 2015.

MITNICK, K. D.; SIMON, W. L. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley, 2002.

PRODANOV, C. C.; FREITAS, E. C. de. *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico*. 2. ed. Novo Hamburgo: Feevale, 2013.

SCHNEIER, B. *Secrets and Lies: Digital Security in a Networked World*. 15th Anniversary ed. Indianapolis: Wiley, 2015.

VERIZON. *2024 Data Breach Investigations Report*. New York: Verizon Enterprise Solutions, 2024.

WHITMAN, M. E.; MATTORD, H. J. *Principles of Information Security*. 7. ed. Boston: Cengage Learning, 2021.