FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Luciana Rodrigues Lopes

ANÁLISE DA EFICIÊNCIA DE ESTRATÉGIAS DE CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA

Impacto de Treinamentos na Redução de Cliques em Simulações de *Phishing* em uma Empresa do Setor de Energia Elétrica

Americana, SP
2025

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Luciana Rodrigues Lopes

ANÁLISE DA EFICIÊNCIA DE ESTRATÉGIAS DE CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA

Impacto de Treinamentos na Redução de Cliques em Simulações de *Phishing* em uma Empresa do Setor de Energia Elétrica

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação do Prof. Me. Edson Roberto Gaseta

Área de concentração: Segurança da Informação.

Americana, SP

2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

LOPES, Luciana Rodrigues

Análise da eficiência de estratégias de conscientização em segurança cibernética: impacto de treinamentos na redução de cliques em simulações de phishing em uma empresa do setor de energia elétrica. / Luciana Rodrigues Lopes – Americana, 2025.

35f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Edson Roberto Gaseta

1. Gestão do conhecimento 2. Segurança em sistemas de informação. I. LOPES, Luciana Rodrigues II. GASETA, Edson Roberto III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 316.77
681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Luciana Rodrigues Lopes

Análise da eficiência de estratégias de conscientização em segurança cibernética: impacto de treinamentos na redução de cliques em simulações de phishing em uma empresa do setor de energia elétrica

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 23 de junho de 2025.

Banca Examinadora:

Edson Roberto Gaseta
Mestre
Fatec Americana "Ministro Ralph Biasi"

Rafael Rodrigo Martinati
Mestre
Fatec Americana "Ministro Ralph Biasi"

Mariana Godoy Vazquez Miano
Doutora
Fatec Americana "Ministro Ralph Biasi"

AGRADECIMENTO

Agradeço primeiramente a Deus, por me conceder força e sabedoria durante toda esta jornada.
À minha família e, em especial, ao meu marido, pelo apoio, compreensão e incentivo nos momentos mais desafiadores.
Ao meu orientador, pelas contribuições fundamentais e pela confiança ao longo do desenvolvimento deste trabalho.
A todos que, de alguma forma, contribuíram para a realização deste projeto, meus sinceros agradecimentos.

RESUMO

A segurança cibernética tornou-se uma prioridade global nas organizações no contexto pós pandemia. Estudos apontam que 90% dos ataques bem-sucedidos iniciam através de e-mails de *phishing*, tornando essa prática como uma das principais ameaças às organizações e a segurança da informação. Este trabalho tem como objetivo analisar a eficácia de estratégias de conscientização voltadas à elevação da maturidade dos colaboradores em segurança cibernética, com foco na identificação e prevenção de ataques de *phishing*. A pesquisa caracteriza-se como exploratória, combinando revisão bibliográfica e análise quantitativa de dados obtidos por meio de simulações de *phishing* realizadas em uma organização do setor de energia. Os dados coletados serão analisados para mensurar o impacto de treinamentos personalizados e frequentes na redução de cliques em e-mails fraudulentos. O estudo visa fornecer subsídios para a criação de programas de treinamento mais eficazes, contribuindo para a proteção de ativos organizacionais e a continuidade das operações em setores críticos. Ao abordar a relevância e a viabilidade de ações educativas no contexto organizacional, espera-se que os resultados desta pesquisa sirvam de base para fortalecer a cultura de segurança digital nas organizações.

Palavras-chave: *Phishing*; Programa de Conscientização; Incidente de Segurança.

ABSTRACT

Cyber security has become a global priority for organizations in the post-pandemic context. Studies show that 90% of successful attacks start through phishing emails, making this practice one of the main threats to organizations and information security. The aim of this study is to analyze the effectiveness of awareness-raising strategies aimed at increasing employees' maturity in cybersecurity, with a focus on identifying and preventing phishing attacks. The research is characterized as exploratory, combining a literature review and quantitative analysis of data obtained through phishing simulations carried out in an organization in the energy sector. The data collected will be analyzed to measure the impact of personalized and frequent training on reducing clicks on fraudulent emails. The study aims to provide subsidies for the creation of more effective training programs, contributing to the protection of organizational assets and the continuity of operations in critical sectors. By addressing the relevance and feasibility of educational actions in the organizational context, it is hoped that the results of this research will serve as a basis for strengthening the culture of digital security in organizations.

Keywords: *Phishing; Awareness Program; Security Incident.*

LISTA DE ABREVIATURAS E SIGLAS

CERT.BR: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil;

CUES: Número e tipo de pistas visíveis na mensagem de *phishing*

IBSEC: Instituto Brasileiro de Cibersegurança;

NIST: *National Institute of Standards in Tecnology*

PSI: Política de Segurança da Informação;

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

SUMÁRIO

INTRODUÇÃO

No contexto pós pandemia, a segurança digital tornou-se uma das maiores prioridades das organizações em todo o mundo. Após o ano do término da pandemia, descobriu-se que cerca de 90% dos ataques às organizações começam com um e-mail enviado com informações que levam o destinatário a ações que que facilitam a atuação de cibercriminosos, sendo conhecido como *phishing*, portanto, em um curto espaço de tempo, tornou-se claro que essa prática reforça seu domínio como a principal porta de entrada para cibercriminosos e fraudadores envolvidos em operações de empresas e roubo de informações. (Security Leaders, 2024). Diante desta realidade, ações de sensibilização e formação devem ser tomadas para proteger sua organização do risco de ataque e promover a integridade na comunidade em geral.

O aumento do número de ataques de *phishing* em que coloca as organizações do setor elétrico em risco, torna-se importante a necessidade de reforço na prática de conscientização dos usuários de sistemas informatizados, além de representar um risco alto tanto para a segurança dos dados quanto para a continuidade do negócio. Nesse cenário torna-se importante a necessidade de aperfeiçoar as práticas de segurança existentes e reforçar o processo de formação sobre as ameaças digitais que podem ser protegidas.

A relevância deste trabalho para as organizações do setor elétrico objetiva em atender às suas prioridades: para a administração, significa proteger a infraestrutura de rede contra ameaças cibernéticas; para os funcionários, promove a conscientização e a capacitação em segurança digital. Além disso, a prevenção de incidentes de *phishing* reduz riscos de segurança e evita prejuízos, contribuindo para a continuidade das atividades. Como o setor de energia é essencial para a sociedade, práticas de segurança robustas garantem que a produção se mantenha sem interrupções, protegendo tanto consumidores quanto setores com infraestrutura de energia considerados críticos.

A realização de ações de conscientização em segurança da informação é viável uma vez que explora aspectos bastante acessíveis e aplicáveis ao contexto das organizações. Sendo assim, proteger a infraestrutura de rede de energia com ações mais seguras, aumenta a conscientização dos funcionários em segurança digital e

reduz riscos de segurança e prejuízos. No setor de energia, a segurança cibernética garante a continuidade das operações, beneficiando consumidores e setores críticos da sociedade.

O objetivo do trabalho é analisar a eficácia de estratégias de conscientização no âmbito da tecnologia que promovem a mudança no comportamento dos colaboradores.

Como objetivos específicos observar a elevação da maturidade dos colaboradores em segurança cibernética, por meio da implementação de estratégias de treinamento personalizadas e recorrentes, visando aumentar a capacidade de identificar e evitar ameaças, como *phishing*, e fortalecer a cultura de segurança na organização.

A hipótese é evidenciar que colaboradores que participam ativamente dos treinamentos de conscientização sobre Segurança Cibernética personalizados e frequentes composto de conteúdo teórico, e as atividades práticas, como simulação de *phishing*, tendem uma redução na taxa de cliques em e-mails fraudulentos. Ao final desta pesquisa poderá contribuir para desenvolvimento de um programa de treinamento eficiente e personalizado, tendendo mitigar riscos de incidentes de segurança e proteger ativos da organização.

O percurso metodológico deste trabalho é uma pesquisa exploratória e descritiva. Os usuários de amostra serão os colaboradores que desempenham funções administrativas e operacionais, e que por serem usuários de e-mail, estão expostos a potenciais ataques de *phishing* da empresa no setor energético. Os indicadores serão os números de falhas em campanhas de simulação de *phishing*. Os dados levantados serão analisados de forma quantitativa.

O trabalho está organizado em três capítulos, sendo que no capítulo 1 está fundamentação teórica, no capítulo 2 a metodologia, no capítulo 3 o estudo de caso e o capítulo 4 conterá os resultados, análise e discussão dos dados.

1 FUNDAMENTAÇÃO TEÓRICA

No embasamento desta pesquisa, optou-se por apresentar os principais fundamentos teóricos que sustentam a presente pesquisa, com base em estudos e referências relevantes da última década. Para isso, são abordados os conceitos centrais relacionados à segurança da informação, especialmente aqueles que se conectam ao comportamento dos usuários diante de ameaças digitais.

1.1 Software Maliciosos

O panorama da segurança digital se torna ainda mais intrincada devido às inúmeras ameaças, como o *malware*, um tipo de *software* nocivo projetado para executar ações prejudiciais em sistemas, frequentemente sem o conhecimento do usuário (Kaspersky, 2021). As ameaças que o *Malware* envolve incluem vírus, *trojans*, *ransomware*, *adware* e *spyware*, cada um com características e formas de atuação distintas, mas todos criados para comprometer a segurança dos sistemas e dos dados guardados. Conforme a empresa global especializada em soluções de conscientização KnowBe4 (2025), o *malware* é uma das ameaças mais frequentes utilizadas por cibercriminosos para aproveitar as falhas do sistema e da segurança humana. Ele é disseminado por meio de *e-mails* de *phishing* que incluem links prejudiciais e anexos que aparentam ser documentos comuns, levando o usuário a acreditar que é seguro clicar neles sem perceber que está executando um programa enganoso, esse método é chamado de *phishing*.

Ao longo dos anos houve uma mudança na sofisticação e nos objetivos dos ataques. Se, no passado, o objetivo era causar danos visíveis aos sistemas, atualmente, o *malware* muitas vezes age de forma silenciosa e furtiva, com foco em roubo de dados e espionagem. Em setores como o de energia, onde uma interrupção pode gerar consequências econômicas e sociais graves, a proteção contra malware é de importância fundamental. Campanhas de *phishing* direcionadas, combinadas com software malicioso, permitem que os atacantes penetrem em sistemas críticos, podendo até obter acesso a operações que controlam a distribuição de energia. Assim, a conscientização sobre o malware, aliada aos treinamentos de segurança que

mostram os métodos comuns de ataque e as formas de prevenção, é uma medida essencial para mitigar os riscos desse tipo de ameaça (KnowBe4, 2024).

1.2 Phishing

A palavra *phishing* tem origem do inglês “*fishing”,* que significa “pescar”, ou seja, vem de uma analogia do pescador que lança uma isca com a finalidade de atrair vítimas. Segundo *OXFORD ENGLISH DICTIONARY* ([s.d.]) *phishing* pode ser definido como uma técnica fraudulenta utilizada para enganar usuários por intermédio de e-mails, em vista de extrair informações privilegiadas, como senhas e números de cartão de crédito, com o objetivo de roubar dinheiro.

Esse tipo de fraude é realizado por uma pessoa mal-intencionada se passando por uma instituição legitima que influi ao individuo realizar uma ação como clicar no link indicado, baixar anexo ou compartilhamento de dados. Utilizando engenharia social os ataques de *phishing* tem como alvo erros humanos, ao contrário de outros ataques cibernéticos que explora vulnerabilidades tecnológicas (IBM, 2024).

Os vazamentos de dados representam uma ameaça crescente para organizações de diversos setores, causando prejuízos financeiros significativos e impactos na reputação. De acordo com a IBM ([s.d.]), o *phishing* é o incidente mais comum equivalente a 16% de todas as violações, o custo médio de uma violação causada por *phishing* chega a US$4,88 milhões,

O *phishing* representa um risco a segurança, ainda que exista a muito tempo e se tornou uma prática fraudulenta comum, os ataques se tornaram convincentes com a sofisticação e a exploração da utilização de métodos de engenharia social, tornando desafiador a identificação de mensagens maliciosas para o usuário e mais para ferramentas.de detecção (ZIENI; MASSARI; CALZAROSSA, 2023). Os ataques de *phishing* podem assumir diferentes formas, com variações no grau de direcionamento e nos seus objetivos. A seguir, apresenta-se no Quadro 1 com os principais tipos de *phishing*, seus alvos e focos de atuação:

Quadro 1 – Tipos de *Phishing*.

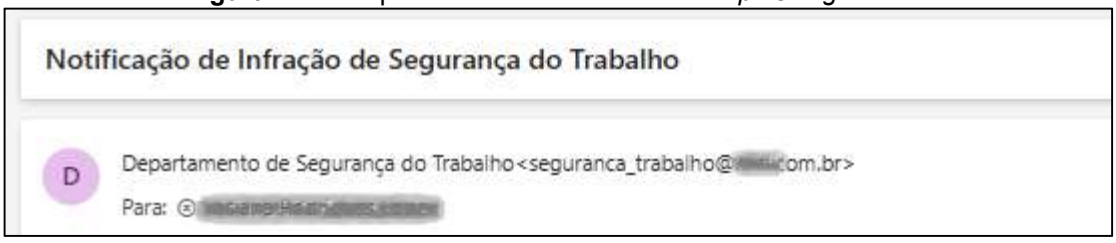
Tipo de *phishing*	Direcionado	Principais Focos
Spear Phishing	Indivíduos ou empresas específicas	Uso de informações pessoais ou organizacionais para parecer legítimo
Whaling	Executivos seniores	Ordens de pagamento, acesso a dados confidenciais e fraudes financeiras
Pharming	Usuários em geral	Redirecionamento silencioso a sites falsos para roubo de credenciais
Clone Phishing	Contatos de vítimas anteriores	Reenvio de e-mails legítimos clonados com links ou anexos maliciosos
Evil twin	Usuários conectados a redes públicas	Interceptação de dados por meio de Wi-Fi falsa semelhante à rede real
Vishing	Usuários de serviços bancários/ telefônicos	Engano via chamada ou mensagem de voz para roubo de dados bancários e senhas
Smishing	Usuários de dispositivos móveis	Links por SMS que solicitam dados ou instalam malware
Phishing de calendário	Usuários de serviços de e-mail/ calendário	Convites de eventos falsos com links maliciosos
Sequestro de página	Usuários de sites legítimos	Redirecionamento por XSS para sites clonados com coleta de credenciais e infecção por malware

Fonte: IBSEC - INSTITUTO BRASILEIRO DE CIBERSEGURANÇA (2024).

A construção de uma mensagem de *phishing* eficaz é cuidadosamente planejada para explorar gatilhos emocionais e contextos profissionais que aumentam a probabilidade de o usuário interagir com o conteúdo malicioso. Os cibercriminosos utilizam elementos que conferem credibilidade ao e-mail, como linguagem formal,

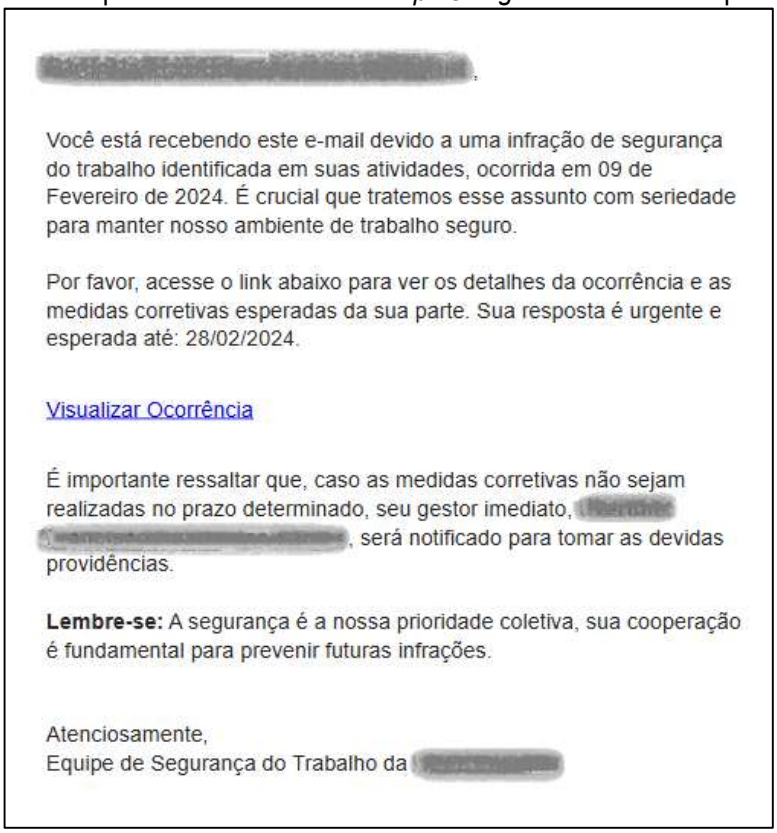
nomes de departamentos reais, prazos curtos e links que imitam sites legítimos. Na Figura 1, apresenta-se um exemplo de e-mail falso que simula uma notificação de infração de segurança do trabalho, enviado supostamente por uma área interna da empresa. Na Figura 2 contempla a mensagem direcionada nominalmente ao colaborador, utiliza tom sério e urgente, menciona datas específicas e ainda contém a assinatura da organização com o logotipo, tudo isso para reforçar a autenticidade da comunicação. O objetivo central desse tipo de ataque é induzir o destinatário a clicar no link fornecido (“Visualizar Ocorrência”), o qual, na prática, redireciona para um site falso que coleta credenciais de acesso ou instala malware. Esse tipo de ataque evidencia o quanto a engenharia social se aproveita do contexto corporativo e da rotina operacional para enganar colaboradores, tornando-se uma das formas mais eficazes de invasão em ambientes organizacionais.

Figura 1– Exemplo de remetente simulado de *phishing*



Fonte: Elaborado para simulação interna de conscientização (2024).

Figura 2 - Exemplo de e-mail simulado de *phishing* com temática corporativa.



[redacted],

Você está recebendo este e-mail devido a uma infração de segurança do trabalho identificada em suas atividades, ocorrida em 09 de Fevereiro de 2024. É crucial que tratemos esse assunto com seriedade para manter nosso ambiente de trabalho seguro.

Por favor, acesse o link abaixo para ver os detalhes da ocorrência e as medidas corretivas esperadas da sua parte. Sua resposta é urgente e esperada até: 28/02/2024.

Visualizar Ocorrência

É importante ressaltar que, caso as medidas corretivas não sejam realizadas no prazo determinado, seu gestor imediato, [redacted], será notificado para tomar as devidas providências.

Lembre-se: A segurança é a nossa prioridade coletiva, sua cooperação é fundamental para prevenir futuras infrações.

Atenciosamente,
Equipe de Segurança do Trabalho da [redacted]

Fonte: Elaborado para simulação interna de conscientização (2024).

Outro ponto relevante para a compreensão da ameaça de *phishing* é o ciclo completo de execução desse tipo de ataque, que pode ser dividido em quatro fases principais: entrega, exploração, comando de controle e exfiltração de dados. Esse fluxo demonstra como os cibercriminosos se aproveitam de vulnerabilidades humanas e técnicas para comprometer sistemas organizacionais.

A primeira fase, conhecida como entrega, ocorre quando o atacante direciona campanhas de *phishing* aos colaboradores da organização, por meio de e-mails fraudulentos que contêm links maliciosos ou anexos infectados. O objetivo, nessa etapa, é atrair a atenção da vítima, simulando mensagens confiáveis, geralmente com apelos urgentes ou enganosos.

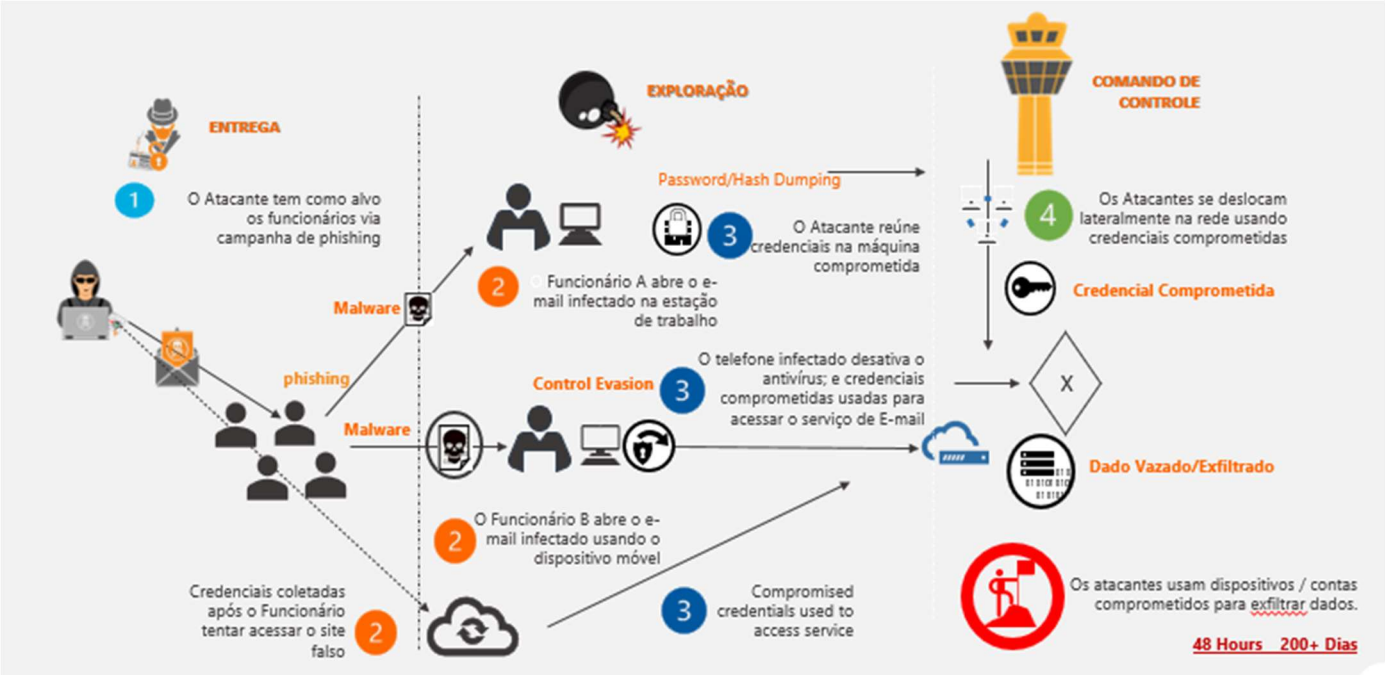
Na sequência, inicia-se a fase de exploração, que acontece assim que o colaborador interage com o e-mail malicioso. Essa interação pode ocorrer ao clicar em links que levam a sites falsos para roubo de credenciais ou ao abrir arquivos infectados, que permitem a instalação de malware. O *software* malicioso então coleta informações ou explora brechas no sistema, podendo desativar mecanismos de segurança e facilitar o acesso remoto do invasor.

Com as credenciais comprometidas, os atacantes avançam para a fase de comando de controle, em que utilizam os dados obtidos para se movimentar lateralmente dentro da rede corporativa. Essa movimentação permite acessar outras áreas sensíveis da organização, inclusive servidores e sistemas de gestão críticos.

Por fim, ocorre a exfiltração dos dados, etapa em que as informações capturadas são extraídas e enviadas para servidores externos controlados pelos criminosos. Esses dados podem incluir senhas, informações financeiras, estratégicas ou dados pessoais dos usuários e clientes. Em muitos casos, os atacantes permanecem por dias ou até semanas dentro da rede antes de serem detectados, agravando os danos.

A Figura 3 ilustra de forma esquemática esse ciclo de ataque, destacando a progressão e a gravidade das ações a partir do simples clique de um usuário desavisado.

Figura 3 - Etapas de um ataque de *phishing*.



Fonte: Adaptado de material institucional de segurança cibernética (2024).

1.3 Incidente de Segurança

O termo incidente de segurança é utilizado para descrever qualquer situação ou evento que possa comprometer a segurança das informações e da estrutura de uma organização. Segundo o CENTRO DE ESTUDOS, RESPOSTA E

TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR) (2022) Incidente é um evento que compromete a segurança de um sistema, ocasionando uma violação de segurança da informação ou outra situação semelhante. Isso pode incluir acessos indevidos, perda de dados, quebra de sigilo, entre outros. Considerando que a maioria dos ataques de *phishing* foi usando e-mails falsos para ludibriar os usuários e garantir acesso irrestrito a sistemas internos, não é difícil entender como ocorrera incidentes de segurança. No âmbito organizacional, a proteção dos sistemas de controle operacional e dos dados sigilosos desempenham um papel vital e, portanto, o efeito de incidentes de segurança pode ser devastador. Ele corre o risco de interromper a continuidade do serviço, intervir na satisfação de clientes, e abalar a integridade das informações.

Os incidentes de segurança não apenas colocam as operações em risco, mas também causam um impacto financeiro e de reputação significativo ao serem revelados ao público e às autoridades reguladoras relevantes. Em ataques de *phishing*, os colaboradores são comumente induzidos a interagir com e-mails que simulam comunicações legítimas, abrindo brechas que os atacantes exploram para acessar sistemas internos. Para organizações especializadas em fornecer energia, apenas um tempo de queda significativo no sistema é suficiente para influenciar negativamente a sociedade. Portanto, é extremamente importante evitar incidentes com medidas proativas. Essas medidas incluem a implementação de políticas de segurança rigorosas e programas de conscientização que ajudem os colaboradores a reconhecerem e evitar interações suspeitas que possam resultar em incidentes de segurança.

1.4 Engenharia social

Um dos métodos mais eficazes para facilitar esses incidentes é a engenharia social, técnica que utiliza a persuasão para induzir indivíduos a realizarem ações específicas, frequentemente comprometendo a segurança organizacional (CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR), 2022). De acordo com KNOWBE4 (2024) a engenharia social é um ataque ao comportamento humano que induz a manipulação dos alvos para efetivar a exploração. Portanto, fraude por meio *phishing* é o golpe em que a engenharia social é comumente usada para enganar colaboradores com ações como

e-mails, mensagens de texto e até mesmo chamadas de telefone, levando-os a acreditar que estão interagindo com fontes confiáveis.

A força da engenharia social está em seu poder de manipular o comportamento humano, acessando emoções como curiosidade, medo e urgência. Esse tipo de ataque é criado intencionalmente, com cenários que tornam o usuário vulnerável e o incentivam a clicar em links ou fornecer informações confidenciais, acreditando estar respondendo a uma comunicação legítima. Nas empresas, a engenharia social é uma das ameaças mais perigosas, pois atinge o elo mais fraco da segurança cibernética: as pessoas. É, portanto, vital para os funcionários de uma organização conhecer os métodos dessa abordagem e saber como identificar os sinais de alerta e resistir a tentativas de *phishing* e variações semelhantes.

1.5 Política de Segurança da Informação

A Política de Segurança da Informação (PSI) é um conjunto de diretrizes, normas e procedimentos estabelecidos pela organização com o objetivo de proteger seus ativos de informação contra ameaças internas e externas. De acordo com a ISO/IEC 27001, a política deve refletir o compromisso da organização com a preservação da confidencialidade, integridade e disponibilidade das informações, sendo considerada um pilar fundamental para a gestão da segurança cibernética.

Uma política de segurança deve ser bem estruturada, com escrita clara, acessível e atualizada periodicamente para atender as necessidades da empresa e acompanhar o avanço das ameaças cibernéticas. Possui a finalidade de documentar regras de boas práticas de uso de recursos de tecnologia, comportamentos esperados dos usuários e a responsabilidade de cada área perante as informações organizacionais. Uma implementação adequada coopera para o desenvolvimento da cultura de segurança, reduzindo possíveis vulnerabilidades que podem ser exploradas revertendo-se em incidente como vazamento de dados, roubo de identidade e ataques de *phishing*.

As políticas de segurança podem ser classificadas em duas categorias principais: política geral e políticas focadas. A política geral é um documento abrangente, que estabelece os princípios e diretrizes básicas de segurança da informação válidas para toda a organização. Ela é responsável por definir a visão institucional sobre segurança, os objetivos estratégicos e o compromisso da alta

direção com a proteção das informações. Já as políticas focadas detalham regras e procedimentos específicos para áreas ou situações particulares, como política de uso aceitável de e-mail, política de controle de acesso, política de resposta a incidentes e política de proteção contra *phishing*. Essas políticas complementam a política geral, aprofundando orientações específicas e adaptando as medidas de segurança às realidades e riscos de cada ambiente ou processo.

A existência de política formalizada é essencial para certificar conformidade com legislações específicas como a Lei Geral de Proteção de Dados (LGPD) no Brasil, todavia, no contexto organizacional a PSI não se limita apenas à criação de documentos formais, é necessário ser integrada a rotina e aos processos por meio de treinamentos, campanhas educativas e ações práticas para ser implementada de forma eficiente.

1.6 Programa de conscientização

Para a construção de um ambiente organizacional seguro, a conscientização em segurança da informação é um dos pilares fundamentais. A conscientização vai além da capacitação técnica do usuário, pois possui o propósito de promover mudanças comportamentais e culturais incentivando atitudes seguras no uso de tecnologias e no manuseio de informações sensíveis. Segundo a ISO/IEC 27001 (2022), é responsabilidade da organização garantir que seus colaboradores estejam cientes de suas responsabilidades em relação à segurança da informação, o que reforça a importância da implementação de programas estruturados de conscientização.

A ausência de conscientização em segurança da informação pode trazer consequências sérias para as organizações. De acordo com PÉREZ (2022), quando não há uma cultura de segurança bem estabelecida, os colaboradores tornam-se alvos fáceis para ataques cibernéticos, especialmente os que envolvem engenharia social, como o *phishing*. Isso porque a falta de preparo leva à adoção de comportamentos inseguros, como o clique em links suspeitos, o uso de senhas fracas ou o compartilhamento indevido de informações confidenciais.

Casos reais demonstram o impacto da falta de conscientização. Segundo a ASSESSORIA DE IMPRENSA E COMUNICAÇÃO DA SECRETARIA DA SEGURANÇA PÚBLICA (2025), fraudes eletrônicas têm se multiplicado rapidamente

no Brasil, muitas delas iniciadas por comunicações fraudulentas que exploram o despreparo das vítimas. Em um dos casos relatados, criminosos enviaram e-mails se passando por instituições legítimas para capturar dados bancários de funcionários públicos, resultando em prejuízos financeiros e vazamento de informações sensíveis. Esse cenário reforça a urgência de programas educativos dentro das organizações, como estratégia de proteção proativa.

Um programa educacional eficiente deve ser contínuo, engajado e adaptado ao perfil dos colaboradores. O programa de conscientização pode assumir diferentes formas, dentre elas o *onboarding* direcionado a integração dos novos colaboradores, apresentar a área e o conceito de segurança da informação proporcionando o nivelamento ao usuário. Aplicar treinamentos periódicos e consistentes abordando temas de segurança com conteúdo simplificado aplicáveis no cotidiano do colaborador, e relembrando a importância da segurança cibernética é a maneira mais eficiente de gerara a mudança cultural dos usuários. Adotar campanha de simulação de *phishing* além de mensurar o nível de vulnerabilidade dos colaboradores, permite personalizar os demais conteúdos considerando o contexto e os riscos específicos da organização, aumenta a eficácia do programa e contribui diretamente para a elevação da maturidade em segurança.

2 METODOLOGIA

A presente pesquisa tem como objetivo principal analisar o impacto de diferentes estratégias de conscientização em segurança da informação na redução da taxa de cliques em simulações de *phishing*, com foco na elevação da maturidade dos colaboradores de uma empresa do setor de energia elétrica.

2.1 Caracterização de Pesquisa.

A presente pesquisa caracteriza-se como exploratória e descritiva, com abordagem quantitativa, e será conduzida por meio de um estudo de caso em uma empresa do setor de energia elétrica. O foco principal é analisar o impacto de estratégias de conscientização em segurança da informação sobre o comportamento dos colaboradores, especialmente no que se refere à redução da taxa de cliques em simulações de *phishing*.

A pesquisa é classificada como exploratória porque busca aprofundar o conhecimento sobre a influência de diferentes abordagens de treinamento na elevação da maturidade em segurança digital. De acordo com D´ARTAGNAN ALMEIDA (2021), esse tipo de pesquisa visa proporcionar maior familiaridade com o tema estudado, por meio da análise de fenômenos sob uma nova perspectiva, permitindo a formulação de hipóteses ou a ampliação do conhecimento sobre o problema.

Além disso, a pesquisa assume um caráter descritivo, uma vez que tem como propósito registrar, analisar e esmiuçar os dados coletados durante a aplicação das estratégias de treinamento. Conforme a definição apresentada por D´ARTAGNAN ALMEIDA (2021), a pesquisa descritiva possui o propósito de observar, registrar e descrever as características de um determinado fenômeno sem manipulá-lo, permitindo a identificação de padrões de comportamento e possíveis relações entre variáveis.

A combinação desses dois tipos de pesquisa é adequada ao presente estudo, uma vez que se pretende, além de levantar dados sobre o comportamento dos colaboradores diante de ataques simulados, avaliar os efeitos de programas de conscientização aplicados ao longo do tempo.

2.1.1 Quanto ao delineamento

Quanto ao delineamento, esta pesquisa é classificada como um estudo de caso, por investigar, em profundidade, uma situação específica dentro de seu contexto real: a aplicação de estratégias de conscientização em segurança da informação em uma empresa do setor de energia elétrica. O estudo busca compreender, analisar e mensurar os efeitos dessas estratégias na redução de cliques em simulações de *phishing*, observando o comportamento de um grupo definido de colaboradores.

De acordo com D´ARTAGNAN ALMEIDA (2021), o estudo de caso é um tipo de pesquisa que se caracteriza por examinar intensivamente um ou poucos objetos, permitindo o aprofundamento da análise a partir de uma perspectiva contextualizada. Esse tipo de delineamento é especialmente útil quando se busca compreender fenômenos complexos e contemporâneos dentro de ambientes específicos.

Nesse sentido, a escolha do estudo de caso como delineamento se mostra adequada, pois permite explorar com profundidade os impactos de ações educativas em segurança digital, considerando os aspectos culturais, operacionais e comportamentais da organização analisada.

3 ESTUDO DE CASO

A pesquisa foi desenvolvida em uma empresa privada no setor de energia elétrica, sua atuação está relacionada a geração, transmissão, distribuição e manutenção da rede elétrica. Por atuar em um setor considerado crítico e essencial, a empresa representa um cenário altamente relevante para a análise de estratégias de conscientização em segurança da informação. De acordo com a Security Leaders (2023), 80% das empresas do setor de energia já foram alvo de ataques cibernéticos, o que evidencia a vulnerabilidade dessa área frente às ameaças digitais, como o *phishing*. Esse contexto reforça a necessidade de fortalecer a maturidade de segurança dos colaboradores, promovendo ações educativas que reduzam os riscos de incidentes e garantam a continuidade dos serviços prestados à sociedade.

A amostra da pesquisa será composta por colaboradores das áreas administrativa e operacional, que utilizam o e-mail corporativo como ferramenta de comunicação. Estes profissionais foram selecionados por estarem diretamente expostos a tentativas de ataques baseados em engenharia social, o que os torna público-alvo de campanhas de conscientização. A escolha da amostra se dá de forma não probabilística e intencional, sendo composta por aproximadamente 12.600 colaboradores.

O procedimento para coleta e análise dos dados foi baseado no monitoramento de campanhas simuladas de *phishing*, realizadas antes e após a intervenção educativa. Os relatórios de taxa de cliques serão utilizados como indicadores de eficácia do programa de conscientização. Os resultados serão organizados em planilhas e interpretados por meio de análise comparativa, buscando evidenciar a evolução do comportamento dos usuários ao longo do processo.

A natureza da análise de dados adotada nesta pesquisa é quantitativa, pois os dados obtidos por meio das simulações de *phishing* serão expressos numericamente e analisados com base em métodos estatísticos simples, como percentuais e comparações diretas entre os períodos pré e pós-intervenção educativa.

Segundo D´ARTAGNAN ALMEIDA (2021), a abordagem quantitativa caracteriza-se pelo uso de instrumentos formais e estruturados para a coleta de dados, permitindo uma análise objetiva dos fenômenos observados, com base em

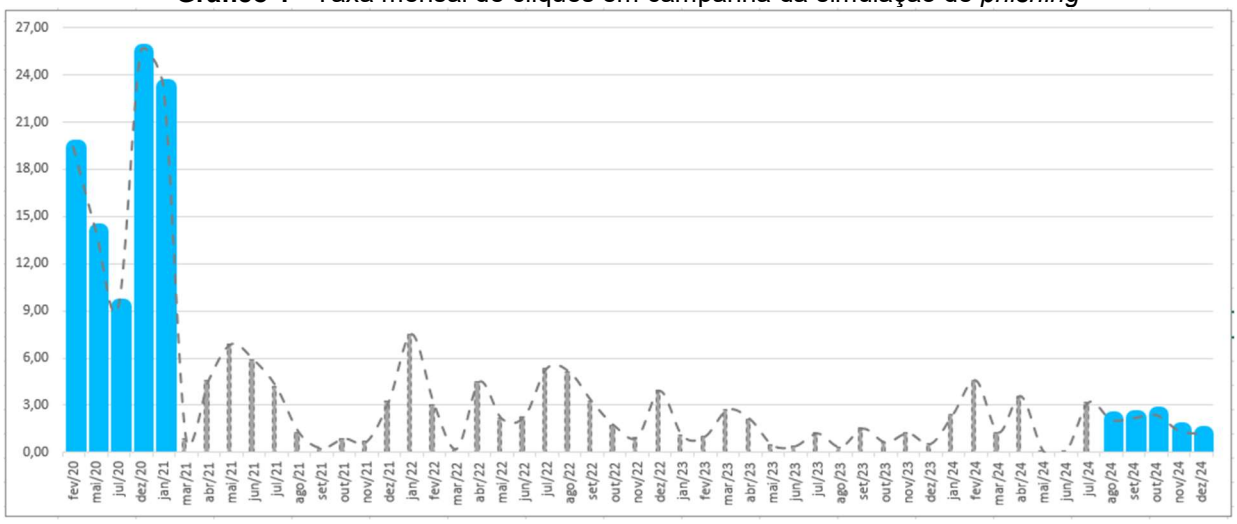
critérios mensuráveis. Esse tipo de análise é apropriado quando se busca testar hipóteses ou verificar relações entre variáveis com base em dados concretos.

Neste estudo, os resultados das campanhas simuladas serão organizados em planilhas eletrônicas e analisados por meio de estatística descritiva, com foco na comparação da porcentagem de cliques antes e após as intervenções educativas. Essa análise permitirá verificar a eficácia das estratégias de conscientização aplicadas e seu impacto na redução do comportamento vulnerável frente a ataques de engenharia social.

3.1 Análise de dados.

No período de 2020 a 2024, foram realizadas campanhas mensais de simulação de *phishing* na empresa, com o objetivo de avaliar a vulnerabilidade dos colaboradores diante de mensagens fraudulentas. Os dados coletados correspondem à porcentagem de cliques registrados em cada campanha, sendo esse o principal indicador de risco comportamental. A seguir, apresenta-se a evolução das taxas de cliques ao longo dos 52 meses avaliados.

Gráfico 1 - Taxa mensal de cliques em campanha da simulação de *phishing*



Fonte: Elaborado pela autora (2025)

Tabela 1 - Média de cliques mensais (2020–2024)

Ano	Nº de Campanhas	Média de cliques (%)	Maior Taxa (%)	Menor Taxa (%)
2020	4	17,07%	25,5%	9,3%

Ano	Nº de Campanhas	Média de cliques (%)	Maior Taxa (%)	Menor Taxa (%)
2021	12	4,74%	23,2%	0,7%
2022	12	3,35%	7,54%	0,26%
2023	12	1,12%	2,73%	0,37%
2024	12	2,05%	3,06%	0,1%

Fonte: Elaborado pela autora (2025)

O Gráfico 1 apresenta a evolução mensal da taxa de cliques em campanhas simuladas de *phishing* realizadas na organização entre os anos de 2020 e 2024. Em complemento, a Tabela 1 exibe o número total de campanhas por ano, a média anual de cliques e os valores máximos e mínimos registrados no período.

O ano de 2020, com apenas quatro campanhas aplicadas, apresentou os índices mais elevados de cliques, atingindo até 25,5% em determinados meses. Esse resultado reflete um nível inicial de maturidade em segurança da informação entre os colaboradores e a ausência, até então, de um programa estruturado de conscientização.

A partir de 2021, foi iniciado um processo contínuo de fortalecimento da cultura de segurança, com a aplicação mensal de campanhas simuladas. A esse esforço foram incorporadas duas estratégias de reforço educativo: o *onboarding* com foco em segurança da informação, voltado a novos colaboradores, e a realização de treinamentos direcionados imediatamente após falhas em simulações de *phishing*, de modo a transformar os incidentes em oportunidades de aprendizado. Como resultado, houve uma redução expressiva na média anual de cliques, que caiu de 17,07% em 2020 para 4,74% em 2021, com continuidade dessa tendência nos anos seguintes.

Entre 2022 e 2023, os dados revelam níveis consistentemente baixos de cliques, com médias inferiores a 3,5% e picos cada vez mais raros. Esse comportamento indica uma evolução no reconhecimento e na rejeição de mensagens suspeitas por parte dos usuários, reflexo do amadurecimento do programa de conscientização e da consolidação de uma cultura preventiva.

Em 2024, embora se registre uma leve oscilação na média anual (2,05%), esse resultado permanece significativamente inferior aos anos iniciais da série histórica. Um avanço importante neste ano foi a adoção da metodologia do *National Institute of Standards na Technology (NIST) Phish Scale*, utilizada para classificar os *templates*

de *phishing* de acordo com seu nível de dificuldade percebida pelos usuários. Essa classificação baseou-se na combinação de dois critérios principais, número e tipo de pistas visíveis na mensagem *cues* observáveis e Alinhamento da premissa da mensagem com o contexto profissional do usuário DAWKINS; JACOBS (2023).

Quadro 2 - Tipos de *Cues*

Tipo de Sugestão	**Nome da Sugestão**	**Exemplos e critérios de contagem**
Erro	Ortografia, gramática, inconsistência	Erros visíveis no corpo do e-mail
Indicador Técnico	Link suspeito, tipo de anexo, domínio falsificado	Uso de URLs não seguras, anexos executáveis, e-mails falsos
Apresentação visual	Logotipo desatualizado, aparência duvidosa	Marca mal aplicada, identidade visual alterada
Conteúdo e linguagem	Urgência, apelos emocionais, pedidos de senha	Tom alarmista, ameaças, ofertas fora do comum
Táticas comuns	Simulação de processos, autoridade, familiaridade	E-mails que imitam chefes, colegas ou sistemas internos

Fonte: Adaptado do NIST TN 2276 (2023), p. 9

Além dos *cues*, foi utilizada uma escala de alinhamento de premissas, conforme o modelo apresentado no Quadro 3, que avalia o quanto a mensagem se encaixa no contexto profissional da vítima. Com base nas pontuações obtidas por cada *template* (máximo 32 pontos), a organização passou a classificar os e-mails simulados por nível de dificuldade, conforme o Quadro 4.

Quadro 3 - Avaliação do Alinhamento de Premissas

Critério avaliado	**Pontuação**
Imita um processo de trabalho real	0 a 8
Tem relevância no local de trabalho	0 a 8
Alinha-se com eventos ou comunicações internas/externas	0 a 8
Gera preocupação com o não cumprimento	0 a 8
Foi alvo de treinamento ou campanhas anteriores	0 a 8

Fonte: Adaptado do NIST TN 2276 (2023), p. 13

Quadro 4 - Classificação da dificuldade com base no alinhamento de premissas

Pontuação Total	**Classificação**
24 a 32	Alinhamento muito alto - **Muito difícil de detectar**
16 a 23	Alinhamento significativo - **Moderadamente difícil**
0 a 15	Baixo alinhamento - **Menos difícil**

Fonte: Adaptado do NIST TN 2276 (2023), p. 14

Essa abordagem permitiu identificar variações no desempenho dos usuários conforme o grau de complexidade das mensagens simuladas, fornecendo dados mais precisos para o ajuste das estratégias de conscientização. As campanhas passaram a ser classificadas, monitoradas e refinadas de forma técnica e padronizada, alinhando a prática organizacional com os padrões internacionais de avaliação comportamental frente a ataques de *phishing*.

De forma geral, os dados demonstram que a execução contínua de campanhas simuladas, aliada a ações de *onboarding*, treinamentos corretivos e personalização por dificuldade, contribuíram diretamente para o desenvolvimento da maturidade organizacional em segurança digital. A queda significativa nas taxas de cliques entre 2020 e 2024 evidencia a eficácia das estratégias de conscientização adotadas, resultando na mitigação do risco humano como vetor de ataques cibernéticos.

4 CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objetivo analisar o impacto de estratégias de conscientização em segurança da informação na redução da taxa de cliques em campanhas simuladas de *phishing*, ao longo do período de 2020 a 2024, em uma empresa do setor de energia elétrica. Ao longo desse período, observou-se uma queda significativa na vulnerabilidade dos colaboradores diante de mensagens fraudulentas, evidenciada por uma redução consistente nas taxas de cliques.

As ações educativas implementadas como o *onboarding* voltado à segurança, os treinamentos reativos e a personalização dos *templates* com base no NIST *Phish Scale* contribuíram diretamente para a mudança de comportamento dos colaboradores frente às ameaças digitais. Esses resultados reforçam a ideia de que a transformação da cultura organizacional em relação à segurança cibernética não ocorre de forma imediata, mas sim como fruto de um processo contínuo, cumulativo e estratégico.

O tempo, nesse contexto, mostrou-se um elemento fundamental. As campanhas mensais aplicadas de forma sistemática permitiram reforçar, testar e consolidar o aprendizado dos colaboradores, promovendo a assimilação progressiva de boas práticas. A repetição das simulações e a evolução gradual dos desafios propostos permitiram um amadurecimento natural da percepção de risco e da postura preventiva dos usuários.

REFERÊNCIAS

ASSESSORIA DE IMPRENSA E COMUNICAÇÃO DA SECRETARIA DA SEGURANÇA PÚBLICA. **Polícia prende trio em operação contra associação criminosa responsável por fraudes cibernéticas**. Disponível em: <https://www.ssp.sp.gov.br/noticia/58651>. Acesso em: 7 jun. 2025, às 11h26.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001. **Segurança da informação, segurança cibernética e proteção à privacidade -Sistemas de gestão da segurança da informação - Requisitos *Information security, cybersecurity and privacy protection - Information security management systems -Requirements* NORMA BRASILEIRA,** 2022.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). **O que é um incidente de segurança?** Disponível em: <https://www.cert.br/docs/certbr-faq.html>. Acesso em: 6 jun. 2025, às 11h26.

D´ARTAGNAN ALMEIDA, Í. **METODOLOGIA DO TRABALHO CIENTÍFICO**. [s.l: s.n.]. Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/49435/1/METODOLOGIA%20DO%20TRABALHO%20CIENT%C3%8DFICO.pdf>.

DAWKINS, S.; JACOBS, J. NIST **Phish Scale User Guide**. **csrc.nist.gov**, v. NIST TN 2276, n. 2276, 15 nov. 2023, às 22h41.

IBM. **Custo das violações de dados 2023 | IBM**. Disponível em: <https://www.ibm.com/br-pt/reports/data-breach>. Acesso em: 6 jun. 2025, às 22h47.

IBM. **Custo das violações de dados 2024 | IBM**. Disponível em: <https://www.ibm.com/br-pt/reports/data-breach>. Acesso em: 6 jun. 2025, às 22h50.

IBSEC - INSTITUTO BRASILEIRO DE CIBERSEGURANÇA. **Ataques de phishing: O que são e como funcionam?** Disponível em: <https://ibsec.com.br/ataques-de-phishing-o-que-sao-e-como-funcionam/>. Acesso em: 6 jun. 2025, às 22h53.

KASPERSKY. **What are the different types of malware?** Disponível em: <https://www.kaspersky.com/resource-center/threats/types-of-malware>. Acesso em: 6 jun. 2025, às 22h58.

KNOWBE4. **Social Engineering: Definition & Examples | KnowBe4**. Disponível em: <https://www.knowbe4.com/what-is-social-engineering>. Acesso em: 7 jun. 2025 às 11h15.

KNOWBE4. **Five Generations Of Cybercrime | KnowBe4**. Disponível em: <https://www.knowbe4.com/resources/five-generations-of-cybercrime>. Acesso em: 6 jun. 2025, às 23h00.

OXFORD UNIVERSITY PRESS. **phishing noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com**. Disponível em: <https://www.oxfordlearnersdictionaries.com/definition/english/phishing?q=phishing>. Acesso em: 7 jun. 2025, às 11h20.

PÉREZ, T. **Por que um programa de conscientização em segurança da informação é importante? - WOMCY Latam Women in Cybersecurity**. Disponível em: <https://womcy.org/por-que-um-programa-de-conscientizacao-em-seguranca-da-informacao-e-importante/>. Acesso em: 7 jun. 2025, às 11h37.

SECURITY LEADERS. **80% das empresas de energia já foram alvo de ataques cibernéticos - Security Leaders**. Disponível em: <https://securityleaders.com.br/80-das-empresas-de-energia-ja-foram-alvo-de-ataques-ciberneticos/>. Acesso em: 7 jun. 2025, às 11h29.

SECURITY LEADERS. **90% dos ataques a empresas começam com um e-mail de phishing, alerta estudo - Security Leaders**. Disponível em:

<https://securityleaders.com.br/90-dos-ataques-a-empresas-comecam-com-um-e-mail-de-phishing-alerta-estudo/>. Acesso em: 7 jun. 2025, às 11h32.

ZIENI, R.; MASSARI, L.; CALZAROSSA, M. C. Phishing or Not Phishing? A Survey on the Detection of Phishing Websites. **IEEE Access**, v. 11, p. 18499–18519, 2023.