XXI Escola Regional de Redes de Computadores / VIII Workshop de Segurança (ERRC). DOI : 10.5753/errc.2024.4579

Artigo Curto/Short Paper

Resiliência em Segurança Cibernética: A Importância do Treinamento na Prevenção de Phishing

Cybersecurity Resilience: The Importance of Training in Preventing Phishing

Leandro Girotto Cabrini Junior • leandrogirottocabrini@gmail.com
Universidade Tecnológica Federal do Paraná (UTFPR)

Braulino Silverio dos Santos Neto • braulino.neto@eversafe.info
Eversafe Tecnologia da Informação LTDA (Eversafe)

Newton Carlos Will • will@utfpr.edu.br
Universidade Tecnológica Federal do Paraná (UTFPR)

Resumo. Com a expansão das redes digitais, as empresas enfrentam sérios desafios em segurança da informação, demandando constantes investimentos na área. Em 2022, o Brasil foi alvo de 31,5 bilhões de tentativas de ataques cibernéticos, destacando-se na América Latina. O *phishing* é uma das ameaças mais prevalentes, utilizando técnicas de manipulação para obter dados confidenciais. Este artigo analisa os resultados de campanhas de *phishing* realizadas antes e depois do treinamento dos colaboradores, demonstrando a importância do treinamento na prevenção desses ataques. Para isso, foram coletados e analisados dados de três campanhas conduzidas antes e depois do treinamento dos colaboradores. A análise busca evidenciar como o treinamento pode reduzir a suscetibilidade dos colaboradores a esses ataques.

Abstract. With the expansion of digital networks, companies face serious challenges in information security, requiring constant investments in the area. In 2022, Brazil was the target of 31.5 billion cyberattack attempts, standing out in Latin America. *Phishing* is one of the most prevalent threats, using manipulation techniques to obtain confidential data. This paper analyzes the results of *phishing* campaigns conducted before and after employee training, demonstrating the importance of training in preventing these attacks. For this, data from three campaigns conducted before and after employee training was collected and analyzed. The analysis aims to show how training can reduce employees' susceptibility to these attacks.

Palavras-chave: Phishing • Campanhas • Conscientização • Treinamento
Keywords: Phishing • Campaigns • Awareness • Training

1 Introdução

Com o crescimento do uso da tecnologia e aumento da conectividade, as empresas enfrentam desafios significativos em segurança da informação, tornando o investimento nessa área crucial. Em 2022, o Brasil registrou 31,5 bilhões de tentativas de ataques cibernéticos, sendo o segundo país mais atacado na América Latina [1]. Entre as ameaças mais comuns está o *phishing*, que utiliza a manipulação psicológica para obter informações confidenciais, como senhas e dados bancários [2].

Apesar da conscientização sobre essas vulnerabilidades, muitas empresas não estão adequadamente preparadas para enfrentá-las devido à falta de políticas rigorosas e treinamento de funcionários [3]. Em 2023, foram registrados 31.672 incidentes de *phishing* no Brasil, conforme ilustrado na Figura 1 [4], e o custo médio de um ataque com vetor inicial sendo engenharia social foi de 4,55 milhões de dólares americanos [5]. Além do prejuízo financeiro, esses ataques podem causar danos significativos à reputação das empresas e à confiança do público.

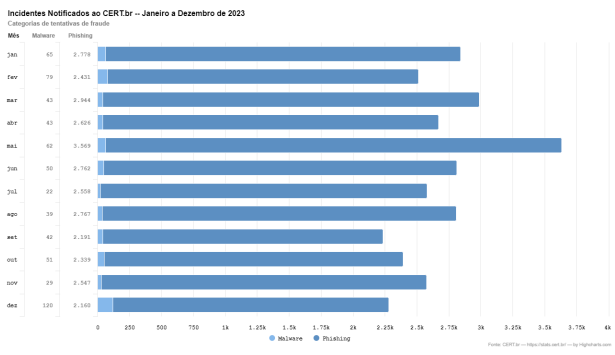

Figura 1. Incidentes notificados ao Cert.br nas categorias de fraude. Fonte: CERT.br [4].

Este artigo tem como objetivo aprofundar a compreensão sobre a relevância da conscientização e treinamento dos colaboradores de empresas na prevenção de ataques de *phishing*. Foram revisadas pesquisas an-

teriores sobre *phishing* e sua evolução, e analisados dados de resultados de campanhas de *phishing* antes e depois dos colaboradores receberem treinamento. O objetivo é demonstrar que colaboradores bem treinados e informados estão menos suscetíveis a esses ataques, destacando a importância do investimento em segurança da informação.

O presente trabalho está estruturado da seguinte forma: na Seção 2 é apresentada uma breve explanação sobre *phishing*; na Seção 3 apresenta-se os trabalhos relacionados ao tema; na Seção 4 está descrita a proposta desta pesquisa; na Seção 5 é detalhada a metodologia empregada; na Seção 6 são apresentados os resultados parciais; e na Seção 7 são apresentadas as conclusões.

2 *Phishing*

Ataques de *phishing* são considerados uma técnica de engenharia social, a definição de engenharia social, conforme descrita pela Kaspersky [6], envolve técnicas de manipulação que exploram erros humanos para obter informações privadas, acesso ou objetos de valor. No contexto do cibercrime, esses ataques tendem a enganar usuários para que exponham dados, espalhem *malware* ou concedam acesso a sistemas restritos. Os ataques podem ocorrer online, presencialmente ou por meio de outras interações [6]. *Phishing* consiste em uma simulação, na qual a vítima é atraída ou enganada para que, pensando se tratar de um conteúdo legítimo, clique em um link falso, acesse uma página falsa ou execute algum arquivo para que haja furto de dados, ou acesso e elevação de privilégios [7].

Na maioria dos ataques de *phishing*, o processo começa com a coleta de informações sobre o alvo. Após essa fase inicial, o *phisher* decide qual método de ataque será utilizado durante a fase de planejamento. A segunda fase é a preparação, onde o *phisher* busca identificar vulnerabilidades que possam ser exploradas para enganar a vítima. O ataque propriamente dito é executado na terceira fase, onde o *phisher* aguarda a resposta da vítima. Por fim, na fase de coleta dos resultados, o atacante coleta as informações ou recursos desejados, concluindo o processo de *phishing* [8].

3 Trabalhos Relacionados

Diversas bibliografias destacam a importância do treinamento contra *phishing* nas empresas como parte de um programa de conscientização sobre segurança da informação. O treinamento deve ser fornecido a novos usuários e repetido periodicamente. Além disso, o Instituto Nacional de Padrões e Tecnologia (NIST) recomenda que as organizações aprimorem o treinamento conduzindo exercícios que simulam ataques cibernéticos [9]. Campanhas de *phishing* combinadas com treinamento podem contribuir de maneira mais eficiente para reduzir o risco de os colaboradores se tornarem vítimas de futuros ataques de *phishing* [10]. Segundo Jansson; Solms [10], muitos usuários demonstraram maior segurança após receberem o treinamento, e o número de reações aos ataques simulados diminuiu. No entanto, poucos estudos mostram detalhadamente a evolução desses números após os colaboradores receberem treinamento. Este artigo pretende preencher essa lacuna ao mostrar a evolução das campanhas de *phishing* antes e depois do treinamento dos colaboradores.

4 Proposta

O objetivo geral deste artigo é analisar os resultados de campanhas de *phishing* realizadas antes e depois do treinamento dos colaboradores, demonstrando a importância do treinamento na prevenção de ataques de *phishing*. Especificamente, busca-se avaliar a eficácia das campanhas de *phishing* ao comparar os dados coletados antes e depois do treinamento dos colaboradores, determinando se há uma redução significativa na taxa de cliques em links maliciosos e no fornecimento de informações confidenciais. Além disso, pretende-se identificar pontos de melhoria nos treinamentos, analisando os resultados para destacar áreas onde a conscientização e a resposta dos colaboradores possam ser aprimoradas. Por fim, o estudo visa ressaltar a necessidade de investimentos contínuos em programas de conscientização e treinamento de segurança da informação para manter os colaboradores atualizados sobre as ameaças de *phishing*.

5 Metodologia

Para este estudo, foram utilizados dados fornecidos pela empresa Eversafe Tecnologia da Informação LTDA., especializada em serviços de segurança da informação e infraestrutura, incluindo a execução de campanhas de *phishing*. Essas campanhas envolvem simulações de ataques de *phishing* enviadas aos colaboradores da empresa contratante, gerando dados relevantes, como a abertura de e-mails, cliques em links maliciosos e dados transmitidos. A utilização desses dados foi autorizada pelo CEO da Eversafe, Braulino Neto, que concordou em fornecê-los anonimizados para este estudo.

A amostra total inclui três campanhas realizadas pela Eversafe em um de seus clientes, com cerca de 629 destinatários. A primeira campanha foi realizada em fevereiro de 2024, antes do treinamento dos colaboradores, e as duas subsequentes ocorreram em março e

abril, após o treinamento realizado em fevereiro. As campanhas foram conduzidas utilizando a ferramenta Knowbe4 [11], parceira da Eversafe, que permite a personalização de grupos de usuários, criação de campanhas e a coleta de dados detalhados para análise. Os parâmetros analisados incluem o número de e-mails enviados, quantos foram abertos, quantos desses resultaram em cliques em links maliciosos e, destes, quantos levaram ao envio de informações confidenciais. Essa abordagem permite uma visão detalhada dos comportamentos dos usuários antes e depois do treinamento.

Os treinamentos também foram realizados através da plataforma Knowbe4 [11], que oferece conteúdos por meio de vídeos online e *quizzes* interativos, promovendo a gamificação e o engajamento dos colaboradores. A escolha da Knowbe4 como ferramenta para treinamento e *phishing* deve-se à conveniência de parceria com a Eversafe Tecnologia da Informação LTDA, que já utilizava essa plataforma em seus serviços.

6 Resultados Preliminares

Inicialmente, foram realizadas três campanhas de *phishing* pela empresa Eversafe Tecnologia da Informação LTDA. em um dos seus clientes, com aproximadamente 629 e-mails destinatários. A primeira campanha foi realizada antes do treinamento sobre *phishing*, enquanto as duas seguintes foram realizadas após o treinamento, permitindo uma análise do impacto do treinamento na redução dos comportamentos inseguros.

A primeira campanha foi realizada em 20 de fevereiro de 2024, antes do treinamento sobre *phishing*. A segunda campanha foi realizada em 19 de março de 2024, após o treinamento dos colaboradores. Já a terceira e última campanha foi realizada em 17 de abril de 2024, também após o treinamento. Os resultados são apresentados na Figura 2.

Ao comparar os resultados das três campanhas, observa-se uma diminuição significativa nas interações inseguras após a realização do treinamento sobre *phishing*. A taxa de abertura de e-mails diminuiu de 33% na primeira campanha para 21,2% na terceira, indicando maior cautela por parte dos colaboradores. A taxa de cliques em links maliciosos caiu de 12,8% na primeira campanha para 4,9% na terceira. A abertura de anexos e habilitação de macros, que foram significativas na primeira campanha, não ocorreram na última, evidenciando uma maior conscientização sobre os riscos associados. Esses resultados sugerem que o treinamento sobre *phishing*, teve um impacto positivo na redução de comportamentos inseguros, contribuindo para a resiliência da empresa contra ataques de *phishing*.

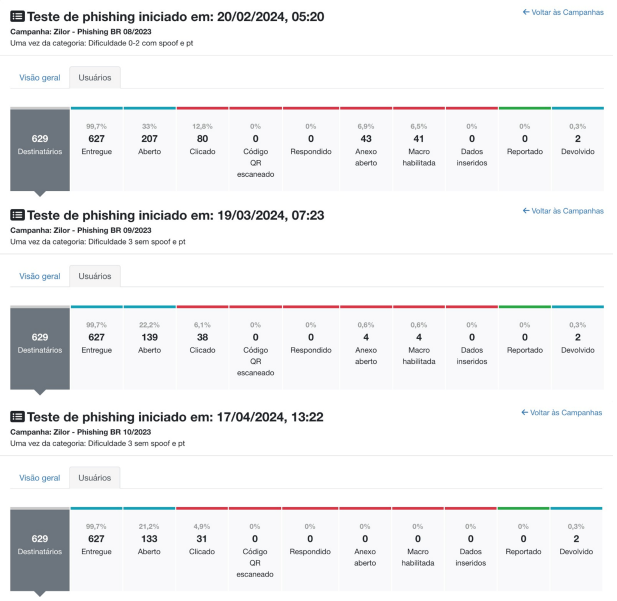

Figura 2. Resultados das campanhas de phishing realizadas entre fevereiro e abril de 2024.

7 Considerações Finais

Os ataques de *phishing* têm maior probabilidade de sucesso quando os alvos não possuem conhecimento sobre *phishing* e não conseguem reconhecer e-mails fraudulentos. Portanto, treinar os colaboradores é uma medida essencial para a prevenção contra esses ataques. Conforme as estatísticas das campanhas de *phishing* demonstram, houve uma redução significativa na taxa de sucesso dos ataques após os colaboradores receberem treinamento. Esses resultados reforçaram a importância do investimento contínuo em programas de treinamento de segurança da informação, evidenciando que colaboradores bem treinados são menos suscetíveis a ataques de *phishing* e mais eficazes na identificação de ameaças potenciais.

Como continuidade deste trabalho, planeja-se a realização de campanhas controladas de *phishing* em diferentes setores da organização. Esse tipo de abordagem visa permitir uma análise prática da eficácia das ações de conscientização e treinamento realizadas, além de possibilitar ajustes mais precisos nas estratégias de defesa. Também busca-se analisar a integração de simuladores interativos e *quizzes* em plataformas internas, garantindo que o processo de educação dos colaboradores seja contínuo e atualizado. Por fim, ampliar a amostra para incluir empresas de diferentes portes e segmentos pode ajudar a identificar vulnerabilidades específicas e oferecer uma visão mais ampla e comparativa, permitindo ajustar estratégias de treinamento e conscientização, garantindo que sejam mais direcionadas e eficazes para diferentes perfis organizacionais.

Referências

1 Fortinet. *Brasil é o Segundo País que Mais Sofre Ataques Cibernéticos na América Latina*. 2022. https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/brasil-e-o-segundo-pais-que-mais-sofre-ataques-ciberneticos-na-a. Acesso em: 19 maio 2024.

2 Aleroud, A.; Zhou, L. Phishing Environments, Techniques, and Countermeasures: A Survey. *Computers & Security*, v. 68, p. 160–196, 2017. DOI: 10.1016/j.cose.2017.04.006.

3 Sêmola, M. *Gestão da Segurança da Informação: Uma Visão Executiva da Segurança da Informação*. Rio de Janeiro, RJ, Brasil: Elsevier, 2013. ISBN 9788535271782.

4 CERT.br. *Estatísticas de Incidentes - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil*. 2024. https://stats.cert.br/incidentes/. Acesso em: 19 maio 2024.

5 IBM Security. *Cost of a Data Breach, 2023*. 2023. https://www.ibm.com/security/data-breach. Acesso em: 19 maio 2024.

6 Kaspersky. *What is Social Engineering? | Definition*. 2024. https://www.kaspersky.com/resource-center/definitions/social-engineering. Acesso em: 21 mai. 2024.

7 Pinheiro, P. P. *et al. Segurança Digital - Proteção de Dados nas Empresas*. São Paulo, SP, Brasil: Atlas, 2021. ISBN 9788597026054.

8 Hewage, C. *et al.* Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, v. 3, fev. 2021. DOI: 10.3389/fcomp.2021.563060.

9 Miranda, M. J. Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach. *International Management Review*, American Scholars Press, Inc., v. 14, n. 2, p. 5–10, 2018.

10 Jansson, K.; Solms, R. von. Phishing for Phishing Awareness. *Behaviour & Information Technology*, Taylor & Francis, v. 32, n. 6, p. 584–593, 2013. DOI: 10.1080/0144929X.2011.632650.

11 KnowBe4. *KnowBe4: Plataforma de Treinamento de Phishing*. 2024. https://www.knowbe4.com. Acesso em: 05 jun. 2024.