ÁREA TEMÁTICA DE EXTENSÃO: *Tecnologias & Produção*

TREINAMENTO ANTIPHISHING - ESTRATÉGIAS PARA PROTEGER ORGANIZAÇÕES E INDIVÍDUOS CONTRA AMEAÇAS CIBERNÉTICAS[1]

ANTIPHISHING TRAINING - STRATEGIES TO PROTECT ORGANIZATIONS AND INDIVIDUALS AGAINST CYBER THREATS

ENTRENAMIENTO ANTI-PHISHING - ESTRATEGIAS PARA PROTEGER A ORGANIZACIONES E INDIVIDUOS CONTRA AMENAZAS CIBERNÉTICAS

ODS[2]: Educação de Qualidade

Jéssica Silva De Oliveira [3]

Bruno Hollyver Alves dos Mártires [4]

Lucas Raphael de Souza Pereira [5]

José Gabriel Fideles Silva [6]

Orientador (a): Jario José dos Santos Junior [7] https://orcid.org/0000-0001-5149-9305

Resumo: Este projeto buscou analisar os impactos da inserção de novas tecnologias na sociedade local com foco na segurança digital e na conscientização sobre ameaças virtuais, com foco em phishing. O estudo foi conduzido através de um curso online intitulado "Treinamento Anti-Phishing", composto por sete módulos que abordaram desde a Lei Geral de Proteção de Dados (LGPD) até táticas avançadas de defesa contra ataques cibernéticos. Mesmo com poucos inscritos, através do projeto, executou-se um curso, cujos resultados houve demonstração de grande eficácia em capacitar os participantes na identificação e prevenção de phishing. A flexibilidade do formato virtual de execução do curso e o suporte contínuo dos tutores foram cruciais para o sucesso da iniciativa. Por fim, o projeto evidenciou a importância da conscientização digital e ressaltou como a inserção tecnológica influencia diretamente a segurança e os hábitos sociais na era da informação. **Palavras-chave:** tecnologias emergentes; phishing; segurança digital; LGPD; sociedade digital.

Abstract: This project aimed to analyze the impacts of the introduction of new technologies in the local society, focusing on digital security and awareness of virtual threats, with an emphasis on phishing. The study was conducted through an online course titled "Anti-Phishing Training," consisting of seven modules that covered everything from the General Data Protection Law (LGPD) to advanced tactics for defending against cyberattacks. Despite having few participants, the course proved highly effective in training participants to identify and prevent phishing. The flexibility of the virtual format and the ongoing support from tutors were crucial to the initiative's success. Finally, the project highlighted the importance of digital awareness and underscored how technological integration directly influences security and social behaviors in the information age. **Keywords:** emerging technologies; phishing; digital security; LGPD; digital society.

Resumen: Este proyecto buscó analizar los impactos de la inserción de nuevas tecnologías en la sociedad local, con un enfoque en la seguridad digital y la concientización sobre amenazas virtuales, con énfasis en el phishing.

[1] Este texto é um produto de Extensão decorrente de uma exposição oral de experiência extensionista em COMUNICAÇÃO ORAL, realizada na Semana de Extensão e Cultura (SEMAEXC-2024).
[2] Este trabalho vincula-se a um ODS - Objetivos de Desenvolvimento Sustentável
[3] Universidade Federal de Alagoas, graduação em Sistemas de Informação.
[4] Universidade Federal de Alagoas, graduação em Sistemas de Informação.
[5] Universidade Federal de Alagoas, graduação em Sistemas de Informação.
[6] Universidade Federal de Alagoas, graduação em Sistemas de Informação.
[7] Universidade de São Paulo, Doutorado em Inteligência Artificial.

ÁREA TEMÁTICA DE EXTENSÃO: *Tecnologias & Produção*

El estudio se llevó a cabo a través de un curso en línea titulado "Entrenamiento Anti-Phishing", compuesto por siete módulos que abarcaron desde la Ley General de Protección de Datos (LGPD) hasta tácticas avanzadas de defensa contra ciberataques. A pesar de tener pocos inscritos, el curso demostró ser muy eficaz para capacitar a los participantes en la identificación y prevención de phishing. La flexibilidad del formato virtual y el apoyo continuo de los tutores fueron cruciales para el éxito de la iniciativa. Finalmente, el proyecto destacó la importancia de la concientización digital y subrayó cómo la inserción tecnológica influye directamente en la seguridad y los hábitos sociales en la era de la información. **Palabras-claves:** tecnologías emergentes; suplantación de identidad; seguridad digital; LGPD; sociedad digital.

Introdução:

Desde a comercialização dos primeiros computadores para o público doméstico, o phishing emergiu como um dos problemas mais significativos enfrentados pelos usuários da internet. Nos últimos anos, o crescimento desses ataques causou prejuízos financeiros exorbitantes para empresas e indivíduos em todo o mundo. De acordo com a Psafe, uma pesquisa realizada em 2022 mostrou um aumento de 97% nas tentativas de phishing entre 2021 e 2022. O phishing é uma técnica de fraude online onde criminosos se passam por entidades confiáveis com o objetivo de enganar as vítimas e obter informações pessoais, como senhas e dados financeiros.

Existem quatro tipos de phishing bastante comuns no Brasil: scam, spear phishing, whaling e vishing.

O **scam** é a forma mais simples, geralmente envolvendo e-mails e/ou SMS falsos que solicitam informações bancárias ou pessoais. Já o **spear phishing** é um ataque mais direcionado, onde o golpista se passa por alguém conhecido da vítima, como um colega de trabalho, para invadir sistemas de segurança. O **whaling** é uma forma ainda mais sofisticada e focada em altos executivos, visando obter grandes quantias de dinheiro ou informações sensíveis. O **vishing**, por sua vez, é a forma mais comum de phishing no Brasil, geralmente feita por telefone, onde criminosos se passam por sequestradores ou autoridades para extorquir dinheiro.

As consequências do phishing vão além dos danos financeiros diretos: as vítimas também podem enfrentar sérios riscos à segurança de suas identidades e informações pessoais, e empresas podem sofrer com a perda de dados sensíveis, danos à reputação e grandes prejuízos financeiros. O incidente envolvendo a criptomoeda Ethereum, que foi alvo de um ataque de phishing em grande escala, resultou em perdas significativas e abalou a confiança nas transações virtuais.

Com a crescente sofisticação desses ataques e as constantes mudanças tecnológicas, identificar e prevenir ataques de phishing tornou-se uma tarefa difícil. O presente trabalho visou alertar e ensinar

aos alunos como identificar, denunciar e se proteger desses ataques, proporcionando ferramentas para aumentar a conscientização e a segurança digital.

Metodologia:

A metodologia do curso foi desenvolvida ao longo de três meses de planejamento, com reuniões semanais. Após várias discussões, decidimos que o curso seria oferecido de forma virtual, pois assim todos os inscritos poderiam participar no horário que fosse mais conveniente, sem atrapalhar suas rotinas diárias. Além disso, o formato online permitiria que os alunos assistissem às aulas quantas vezes fosse necessário para compreenderem o conteúdo.

O curso foi dividido em sete módulos distintos e disponibilizado gratuitamente pelo Google Drive. Cada membro do grupo teve liberdade para criar suas aulas de forma personalizada, utilizando ferramentas como slides, gravação de tela e webcam. Essa liberdade gerou um curso dinâmico e prático, que foi bem recebido pelos participantes. As inscrições foram feitas por meio de um formulário no Google, onde os alunos forneciam informações como nome, idade e email. Eles também precisavam autorizar o uso de seus dados e imagens para fins acadêmicos. As inscrições, que estavam previstas para acontecer entre 19 e 25 de fevereiro, acabaram se estendendo até o dia 3 de março, permitindo que mais pessoas se inscrevessem. Ao todo, tivemos 29 inscritos, sendo que 25 permitiram o uso de seus dados no projeto.

Após a inscrição, os participantes recebiam um link para entrar em um grupo de WhatsApp, onde nós publicamos diariamente avisos sobre o curso. Os alunos também puderam usar o grupo para tirar dúvidas. Além do WhatsApp, os avisos foram enviados por e-mail para quem preferiu não participar do grupo.

Para atrair inscritos, criamos um panfleto digital utilizando o Adobe XD, com um QR Code que levava diretamente para a página de inscrição. No final do curso, os participantes passaram por uma avaliação que continha 5 perguntas, sendo 1 fechada e 4 abertas. Cada questão valia 2 pontos, e para obter o certificado, os alunos precisavam atingir uma nota mínima de 6 pontos.

Por fim, pedimos um feedback anônimo dos alunos através de um formulário no Google Forms. Isso permitiu que eles expressassem suas opiniões de forma livre, sem se identificar. Essa metodologia garantiu que o curso fosse acessível e flexível para todos, com boa interação entre os envolvidos e um aprendizado de qualidade.

Resultados e Discussão:

Durante o curso, contou-se com a presença de 29 inscritos. Foi realizada uma avaliação para mensurar a eficácia do programa. Dos participantes, 10 pessoas completaram com sucesso a prova, demonstrando um nível satisfatório de compreensão e habilidades adquiridas. Esses resultados indicam uma participação ativa e um bom aproveitamento por parte dos envolvidos no treinamento antiphishing.

O curso contou com cerca de 7 módulos: introdução, LGPD, tipos de Phishing, como identificar, consequências e prevenção, conscientização, e treinamento CBT.

O conteúdo do curso abrangeu uma variedade de tópicos essenciais, distribuídos ao longo de aproximadamente seis módulos cuidadosamente estruturados. Desde a introdução até a conscientização final, os participantes foram guiados por uma jornada educativa e prática.

O curso abordou diversos tópicos importantes relacionados à prevenção de ataques de phishing, divididos em sete módulos.

Primeiro Módulo: Apresentou o conceito de phishing, suas origens e os tipos de ataques existentes, ilustrando com casos reais. Os alunos se tornaram mais aptos a identificar possíveis ataques de phishing.

Segundo Módulo: Introduziu a LGPD (Lei Geral de Proteção de Dados), explicando suas diretrizes e como a segurança digital é tratada sob essa legislação. Exemplos de violações em grandes empresas, como Google, Facebook e Uber, ajudaram a ilustrar as implicações da LGPD. Os alunos aprenderam a aplicar seus direitos digitais e identificar possíveis violações.

Terceiro Módulo: Focado em explicar as diferentes formas de phishing, suas características e como identificar cada uma. O estudo de caso ajudou a reforçar o aprendizado sobre os tipos mais comuns no cotidiano.

Quarto Módulo: Explorou as vulnerabilidades humanas e tecnológicas que facilitam ataques de phishing, mostrando como golpistas aproveitam brechas de segurança e fraquezas humanas como ganância e desatenção. Estudos revelam que 58% das violações de segurança no Brasil são causadas por erro humano.

Quinto Módulo: Destacou as consequências dos ataques de phishing, como roubo de dados, perda de acesso a contas e "nome sujo". Foram apresentadas formas de prevenção, com foco na importância de proteger informações pessoais.

Sexto Módulo: Enfatizou a importância da conscientização cibernética, destacando a identificação de ataques de phishing, sinais de alerta e métodos de prevenção. Também reforçou a relevância da LGPD e promoveu estudos de caso sobre ataques e suas consequências.

Sétimo Módulo: Tratou da prevenção contra phishing, como o uso de filtros de e-mail e autenticação em duas etapas. O módulo também destacou o treinamento baseado em computador (CBT), que é eficiente na prevenção de phishing, útil tanto para empresas quanto para usuários comuns. Formas de prevenção, como evitar sites suspeitos e confirmar a veracidade de mensagens recebidas, foram enfatizadas.

Ao final do curso, uma avaliação foi aplicada. Apesar de apenas 10 participantes realizarem a prova, todos atingiram notas acima do mínimo exigido. Os feedbacks foram majoritariamente positivos, com um aumento significativo no conhecimento dos alunos sobre phishing e medidas preventivas.

Conclusões:

O curso de treinamento anti-phishing foi um sucesso, alcançando seu principal objetivo de conscientizar e capacitar os participantes para identificar e prevenir ataques de phishing. Por ser em formato virtual, o curso foi flexível e de fácil acesso, tornando o aprendizado mais dinâmico e eficaz. Os resultados demonstram que os alunos não apenas absorveram o conteúdo, mas também ficaram satisfeitos com o processo de ensino.

A importância da conscientização digital ficou clara, e o curso serviu para reforçar essa necessidade em tempos de crescente atividade cibernética maliciosa. Ao final, o curso contribuiu significativamente para criar uma cultura de segurança digital mais forte entre os participantes, preparando-os para protegerem a si mesmos e suas redes contra ameaças futuras, e, além disso, o curso também forneceu conhecimento didático aos seus participantes, fazendo com que os mesmos contribuíssem para ensinar conhecidos/amigos a terem cuidado com as ações que realizam pela internet, tornando o curso o estopim para o aprimoramento do conhecimento de diversas pessoas além das que se inscreveram no curso.

Referência:

ALEROUD, Ahmed; **ZHOU**, Lina. Phishing environments, techniques, and countermeasures: A survey. Computers & Security, v. 68, p. 160-196, jul. 2017. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167404817300810. Acesso em: 04 mar. 2024

CERT. Cartilha de segurança da internet. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 02 mar. 2024.

HADNAGY, Christopher; FINCHER, Michele. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. 1. ed. Estados Unidos: Wiley, 2015.

PSAFE. O que é Phishing? Conheça essa fraude e saiba como se proteger. Disponível em: https://www.psafe.com/blog/o-que-e-phishing/. Acesso em 19 fev. 2024.

TEMPEST. Phishing: a importância da conscientização e do treinamento em segurança na prevenção desta ameaça. Disponível em: <https://www.tempest.com.br/blog/phishing-a-importancia-da-conscientizacao-e-do-treinamento-em-seguranca-na-prevencao-desta-ameaca/>. Acesso em: 20 fev. 2024.