CIBERSEGURANÇA EM FOCO: EDUCAÇÃO COMO FERRAMENTA NO COMBATE AOS CRIMES CIBERNÉTICOS

LARISSA SCHONHOFEN[1]; CHARLLYNSON CARVALHO CAXIAS[2]; AMY KUHN HAMMES[3]; LEOMAR SOARES DA ROSA JR.[4]

[1]*Universidade Federal de Pelotas – lssilva@inf.ufpel.edu.br*
[2]*Universidade Federal de Pelotas – cccaxias@inf.ufpel.edu.br*
[3]*Universidade Federal de Pelotas – amy@inf.ufpel.edu.br*
[4]*Universidade Federal de Pelotas – leomarjr@inf.ufpel.edu.br*

1. INTRODUÇÃO

A cibersegurança é uma área que tem ganhado destaque nas últimas décadas devido ao crescimento exponencial dos crimes cibernéticos em todo o mundo. Ela consiste em um conjunto de práticas, tecnologias e medidas de proteção que visam garantir a integridade, confidencialidade e disponibilidade de dados em sistemas computacionais. Com a crescente digitalização da sociedade, a cibersegurança se tornou uma necessidade fundamental para proteger informações sensíveis de indivíduos, empresas e governos contra acessos não autorizados, ataques maliciosos e possíveis danos que possam comprometer a segurança de sistemas e redes.

Conforme dados da pesquisa "Panorama de Ameaças" realizada pela Kaspersky em 2023, o Brasil está entre os países mais afetados por crimes cibernéticos na América Latina, registrando mais de 40 milhões de tentativas de ataques em apenas seis meses. Entre os principais objetivos dos cibercriminosos no país estão o roubo de dados pessoais, roubo de identidade e fraudes bancárias, que têm se tornado cada vez mais frequentes e sofisticados, gerando impactos financeiros e de reputação tanto para empresas quanto para cidadãos. Esses números evidenciam a urgência de estudos e práticas que visem fortalecer a cibersegurança, tornando-a um tema crucial para a sociedade contemporânea.

De acordo com ANDERSON (2022), a conscientização sobre cibersegurança é um fator crucial para a proteção da sociedade moderna. Seu estudo destaca que, embora sejam necessárias medidas técnicas e avançadas para combater os cibercrimes, o comportamento humano e a educação em cibersegurança desempenham papéis igualmente importantes na prevenção de ataques. ANDERSON (2022) sugere que programas de educação e treinamento em cibersegurança voltados para diferentes setores da população podem reduzir significativamente a exposição a riscos cibernéticos, ao aumentar a capacidade de identificação e reação frente a possíveis ameaças.

Portanto, o presente estudo tem como objetivo principal conscientizar e educar sobre a importância da cibersegurança, com foco em prevenir e mitigar riscos associados a crimes cibernéticos. Para isso, este trabalho buscará apresentar os principais tipos de cibercrimes, suas implicações e estratégias de prevenção, contribuindo para o fortalecimento da cultura de segurança digital e a redução da vulnerabilidade aos cibercrimes.

2. ATIVIDADES REALIZADAS

O projeto "Cibersegurança em Foco," desenvolvido pelo Programa de Educação Tutorial (PET) Computação, surgiu com o objetivo de oferecer conteúdo informativo sobre cibersegurança para os alunos dos cursos de Ciência da

Computação e Engenharia de Computação da Universidade Federal de Pelotas (UFPel). O foco principal do projeto é explicar os tipos de cibercrimes mais comuns, os objetivos dos cibercriminosos, os riscos envolvidos e as formas de prevenção contra essas ameaças. Embora o projeto seja inicialmente destinado aos alunos de Computação, a intenção é atingir toda a comunidade acadêmica da universidade, aproveitando o alcance das redes sociais.

Para garantir o máximo engajamento, os materiais informativos foram produzidos no formato de posts para serem publicados em sequência no Instagram do PET Computação, @petcompufpel. A escolha da rede social como veículo informativo se fundamenta em pesquisas como a de Auxier e Anderson (2021), que mostram que o Instagram é uma das plataformas mais populares entre jovens adultos, o que reforça sua eficácia como ferramenta para disseminar conhecimento. Além disso, a abordagem sucinta e visual dos posts facilita a leitura e compreensão, como observado por Morkunas et al. (2019), que apontam que informações apresentadas em formatos visuais e de fácil acesso têm maior probabilidade de prender a atenção e promover o entendimento do público-alvo.

A seleção dos temas abordados nos posts foi baseada em dados de relatórios sobre cibercrimes no Brasil. De acordo com o relatório "Cibersegurança na América Latina e Caribe" da Organização dos Estados Americanos (OEA) e Symantec (2016), o *phishing* e os *malwares* estão entre os tipos de cibercrimes mais comuns no Brasil, causando prejuízos significativos a indivíduos e organizações. Assim, o projeto priorizou a explicação destes e outros tipos de ataques cibernéticos, abordando suas características, modos de operação e estratégias de prevenção.

Outro aspecto importante abordado nos posts é a explicação de medidas de segurança convencionais, como a criação de senhas fortes e a autenticação de dois fatores. A pesquisa de Bonneau et al. (2015) destaca que senhas fortes e a autenticação em duas etapas são consideradas medidas altamente eficazes para evitar acessos não autorizados, reforçando a importância de sua divulgação. Portanto, os posts também enfatizam a necessidade de adotar essas práticas, fornecendo instruções claras sobre como implementá-las para aumentar a segurança online.

O formato dos posts foi planejado para criar uma sequência lógica de leitura para o usuário. Nos posts sobre tipos de cibercrimes, o título apresenta o nome do cibercrime, seguido por uma explicação sucinta e clara, semelhante a um dicionário. Em seguida, são descritos os objetivos dos cibercriminosos, os riscos para os usuários e uma lista de medidas de proteção que podem ser adotadas para evitar ser alvo desses ataques. Nos posts que tratam de medidas de cibersegurança, como a criação de senhas fortes e a implementação de autenticação em dois fatores, começamos contextualizando o significado e a importância dessas práticas, seguido de um guia prático que orienta o usuário sobre como adotá-las de maneira efetiva.

A seguir, apresentamos na Figura 1 a imagem do post sobre o cibercrime *phishing*. Além dos exemplos mencionados, nosso projeto busca expandir a gama de tópicos abordados, trazendo informações atualizadas sobre os tipos de cibercrimes mais recorrentes na sociedade, reforçando a ideia de continuidade e conscientização sobre a segurança digital.

Figura 1 - Imagem do post sobre *phishing*.

3. CONSIDERAÇÕES FINAIS

O presente estudo encontra-se em constante desenvolvimento devido à natureza dinâmica e evolutiva da área da cibersegurança. O principal resultado obtido até o momento foi a conscientização e educação da comunidade acadêmica dos cursos de Ciência da Computação e Engenharia de Computação da UFPel sobre os tipos de cibercrimes e as principais medidas de segurança online.

Entre os desafios enfrentados durante o desenvolvimento do projeto, destacam-se a seleção dos cibercrimes a serem abordados e a definição do formato de divulgação que seria mais eficaz para alcançar o público-alvo, garantindo que as informações fossem transmitidas de forma clara e sucinta. Essa abordagem é especialmente relevante para estudantes da área, que, como futuros profissionais de Computação, devem estar cientes da importância da cibersegurança em sua prática profissional.

O impacto inicial do projeto sugere que a conscientização dos estudantes pode contribuir para a ampliação de pesquisas em cibersegurança e para a redução da incidência de cibercrimes, ao atuar diretamente na base da área afetada. Em um estudo realizado por Tushar et al. (2020), foi observado que a conscientização sobre cibersegurança entre estudantes de TI pode ter um efeito multiplicador na disseminação de boas práticas e na redução de vulnerabilidades em ambientes digitais.

4. REFERÊNCIAS BIBLIOGRÁFICAS

ANDERSON, J. Cibersegurança: uma abordagem sobre a importância da conscientização. Revista de Segurança Digital, São Paulo, v. 4, n. 2, p. 45-60, 2022.

AUXIER, B.; ANDERSON, M. Social Media Use in 2021. Washington, DC: Pew Research Center, 2021. Disponível em: Pew Research Center. Acessado em 25 set. 2024.

BONNEAU, J.; HERLEY, C.; VAN OORSCHOT, P. C.; STAJANO, F. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. IEEE Symposium on Security and Privacy, San Jose, 2015. Proceedings… IEEE, p. 553-567, 2015.

KASPERSKY. Panorama de Ameaças na América Latina: 2023. São Paulo, 2023. Disponível em: Kaspersky. Acessado em 25 set. 2024.

MORKUNAS, V. J.; PASCH, E.; PAUL, A. Designing for attention: The effects of visual organization on content perception in digital communication. International Journal of Human-Computer Studies, London, v. 129, p. 64-75, 2019.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA); SYMANTEC. Cibersegurança na América Latina e Caribe: O estado da questão. Washington, DC, 2016.

TUSHAR, P.; KUMAR, A.; KUMAR, V.; SINGH, V. Awareness of cybersecurity among students: A study of educational institutions. Journal of Information Security and Applications, v. 54, p. 102588, 2020.