Um Relato de Experiência sobre um Minicurso de combate aos Golpes Digitais e à Conscientização em Segurança Digital no ICMC/USP

Renan P. Scarpin[1], **Felipe M. Salles**[1], **Gabriel A. Araujo**[1], **Guilherme P. Sá**[1], **Kalinka Castelo Branco**[1]

[1]Instituto de Ciências Matemáticas e de Computação (ICMC) - Universidade de São Paulo (USP)
São Carlos – SP – Brasil

{renanscarpin, felipesalles, gabriel.antunes.345, guilherme1478}@usp.br, kalinka@icmc.usp.br

Abstract. *The rise in digital scams in Brazil underscores the need for educational initiatives to raise awareness of digital security, particularly regarding the prevalence of social-engineering attacks. This article reports on the experiences gained in the mini-course "How to be safe on the Internet?", promoted by the Ganesh extension group at the Institute of Mathematical and Computer Sciences (ICMC) at the University of São Paulo (USP), which aims to share fundamental knowledge of computing and cybersecurity with the university community, both internal and external. The project addressed fundamental concepts in data protection, online fraud detection, and safe browsing practices to reduce vulnerabilities arising from misinformation and low digital literacy. The structure of the mini-course, the challenges faced, and the main lessons learned are presented, highlighting the role of university extension in promoting digital security education.*

Resumo. *O aumento dos golpes digitais no Brasil evidencia a necessidade de ações educativas voltadas à conscientização em segurança digital, especialmente diante da predominância de ataques baseados em engenharia social. Este artigo relata as experiências adquiridas no minicurso "Como estar seguro na Internet?", promovido pelo grupo de extensão Ganesh do Instituto de Ciências Matemáticas e de Computação (ICMC) da Universidade de São Paulo (USP), que visa compartilhar conhecimentos fundamentais de computação e cibersegurança com a comunidade interna e externa da universidade. O projeto abordou conceitos fundamentais de proteção de dados, identificação de fraudes online e boas práticas de navegação segura, com o objetivo de reduzir vulnerabilidades decorrentes da desinformação e do baixo nível de letramento digital. São apresentados a estrutura do minicurso, os desafios enfrentados e os principais aprendizados, destacando o papel da extensão universitária na promoção da educação em segurança digital.*

1. Introdução

O avanço das tecnologias digitais, impulsionado pelo crescimento exponencial de dispositivos e pelo acesso à Internet, promoveu a transformação social de processos e a

digitalização das relações sociais [Yildiz and Nur 2024]. Embora estas tecnologias tenham trazido ganhos produtivos e facilitado o cotidiano das pessoas, esse processo ampliou substancialmente a exposição dessas pessoas a ameaças cibernéticas, especialmente no contexto dos golpes digitais.

Em 2025, segundo o relatório do *FortiGuard Labs* sobre o Cenário Global de Ameaças [FortNet 2025], o Brasil registrou 314,8 bilhões de ataques cibernéticos apenas no primeiro semestre. Sendo assim, a Internet se tornou um ambiente perigoso para o indivíduo que desconhece os riscos do ambiente digital [Umbach et al. 2026, Jain et al. 2021]. Em 2016, a empresa de análise de segurança cibernética *Cyence* afirmou que os Estados Unidos eram o país mais visado por ataques de engenharia social e com o maior custo associado a esses ataques, seguidos pela Alemanha e pelo Japão. O custo estimado desses ataques nos EUA foi de U$ 121,22 bilhões [Salahdine and Kaabouch 2019] e está relacionado a aspectos educacionais, culturais e sociais [Chetioui et al. 2022].

Nesse contexto, é fundamental que as iniciativas promovam a educação em segurança digital, de modo a conscientizar as pessoas sobre os perigos e ensinar conceitos que, muitas vezes, parecem complexos, de forma gamificada, interativa e didática. Em um ambiente universitário, projetos de extensão, ao promoverem ensino, pesquisa e iniciativas educacionais, surgem como um espaço importante para a disseminação de conhecimento aplicado à comunidade interna e externa à universidade [Majumdar 2022]. Assim, o grupo de extensão *Ganesh*, desenvolvido no Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (ICMC/USP), apresenta, neste artigo, um relato de experiência sobre os dois últimos anos do minicurso "Como estar seguro na Internet?". Como contribuição, a estrutura do minicurso e as estratégias adotadas para o engajamento dos participantes são apresentadas com o objetivo de estimular novas iniciativas no Brasil.

Este artigo está dividido como segue: a Seção 2 descreve a Fundamentação Teórica que sustenta as práticas educacionais e pedagógicas do minicurso, a Seção 3 descreve a metodologia desenvolvida bem como os conteúdos abordados e suas estruturas, a Seção 4 discorre sobre os desafios e estratégias adotadas para ampliação da participação e sucesso da iniciativa, a Seção 5 descreve os resultados e impactos atingidos e a Seção 6, por fim, discorre sobre as considerações finais.

2. Fundamentação Teórica

As atividades de extensão universitária constituem um amplo espaço de aprendizagem ao inserirem estudantes de graduação em situações reais de aplicação do conhecimento ou em frentes de impacto social. O processo educativo é mais efetivo quando articulado com base nos problemas que a sociedade enfrenta e gera impactos significativos quando o saber é construído coletivamente [Freire 2014]. Nesse sentido, os elementos de jogos em contextos educacionais promovem a participação dos estudantes ao oferecer desafios e dinâmicas que estimulam o aprendizado ativo [Deterding et al. 2011].

Paralelamente, o uso de slides como recurso visual estruturador auxilia na compreensão gradual dos conceitos, especialmente quando combinados com exemplos práticos e figuras, especialmente quando o público não tem conhecimento prévio dos temas abordados [Mayer 2009, Astin 1984]. A Figura 1 ilustra a estrutura pedagógica que fundamenta o minicurso e outras iniciativas do *Ganesh*. Assim, as extensões es-

timulam o protagonismo estudantil (Figura 2), o desenvolvimento do ser humano e a troca de ideias, ao mesmo tempo em que ampliam o impacto social ao propagarem conhecimentos relevantes produzidos na universidade à sociedade como um todo [Morris et al. 2002, Fauzi et al. 2025].

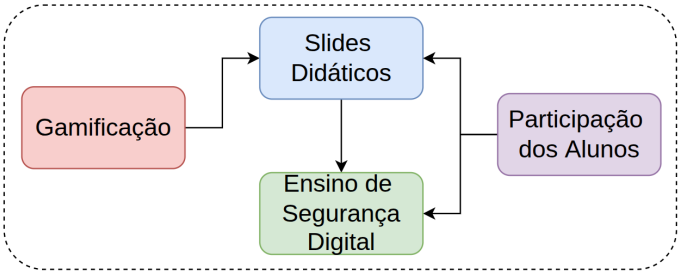

Figura 1. Estrutura pedagógica adotada nas iniciativas de ensino do Ganesh ICMC/USP, fundamentada no uso de gamificação e na estruturação de slides com exemplos práticos e dinâmicas interativas.

Figura 2. Apresentadores e membros do Ganesh após o fim das palestras do minicurso "Como estar seguro na Internet?".

A Engenharia Social é definida como um conjunto de técnicas utilizadas por criminosos para induzir indivíduos a divulgar informações confidenciais, a realizar ações indevidas ou a conceder acesso não autorizado a informações sensíveis, como senhas de contas bancárias [Birthriya et al. 2025]. Diferentemente de ataques técnicos, como o ataque de negação de serviço (DoS), essas estratégias exploram o comportamento humano. Com isso, soluções tecnológicas eficientes, como a autenticação de dois fatores, não são suficientes para mitigar diversos riscos cibernéticos, sendo necessárias a conscientização e o fortalecimento da cultura de segurança digital. Nesse sentido, o grupo de extensão *Ganesh* [Salles et al. 2025] desempenha um papel importante ao promover a conscientização em segurança digital.

3. Metodologia

Nesta seção, descrevemos a metodologia desenvolvida para a elaboração do minicurso, apresentada na Figura 3. Inicialmente, desde 2024, foram definidos quais temas devem ser

abordados e que necessitam de atualizações com base na coleta de dados provenientes dos participantes das edições anteriores. Os temas abordam conceitos fundamentais para o uso da Internet, com o objetivo de conscientizar o público participante. Posteriormente, *slides* foram elaborados colaborativamente para abordar conceitos densos de forma simplificada. Nesse sentido, o principal objetivo do minicurso é difundir conhecimento denso a pessoas distantes da área de computação, alcançando um público fora do contexto universitário. Em seguida, divulgamos o minicurso nas redes sociais do grupo e, em especial, na edição de 2025, ele foi exibido na TV local.

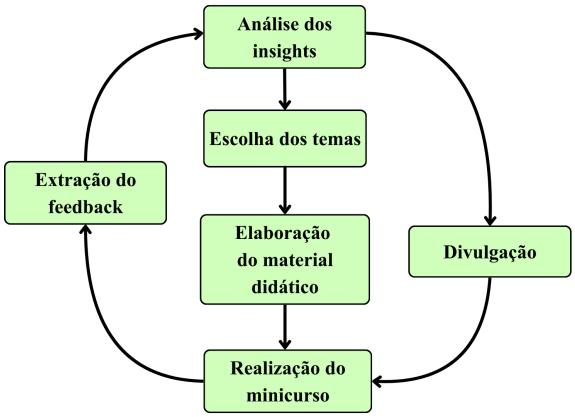

Figura 3. Metodologia adotada para a elaboração do minicurso, visando melhorar o engajamento do público e gerar dados relevantes para edições futuras.

Na etapa de divulgação, além da explicação sobre o funcionamento do evento, foi compartilhado um formulário de inscrição, responsável por coletar dados de contato dos interessados, como nome, e-mail, telefone, além de quando e como assistirão ao evento. O minicurso possui formato híbrido, com uma apresentação presencial no auditório do campus universitário e uma transmissão ao vivo nos canais do *Ganesh* e do ICMC no *Youtube*, com duas apresentações em horários e dias distintos. Por fim, uma avaliação dos usuários é coletada ao final de cada apresentação do curso, por meio de um formulário de *feedback*, visando identificar pontos de melhoria. No formulário, cada participante deveria avaliar o curso em uma escala de 1 a 10, informar quais temas já eram conhecidos, em quais teve mais dificuldade de aprendizado, se possuía algum vínculo com a universidade e incluir um espaço para adicionar suas próprias críticas e sugestões. Em ambas as edições, o curso seguiu uma estrutura de tópicos, com cada conteúdo apresentado individualmente.

3.1. Engenharia social e Malwares

Os golpes digitais são um dos temas mais conhecidos entre o público-alvo, dada a sua forte presença na mídia e o risco que representam. Assim, a ênfase foi dada à sua apresentação, contando com a definição de Engenharia Social, exemplificando golpes digitais, como o *Phishing* e golpes de extorsão (Figura 4 e Figura 5). Também foi abordado como o público deveria agir para identificá-los e evitá-los. Em relação à primeira edição, novos exemplos foram utilizados e o foco foi dado em como agir caso seja vítima de um golpe.

Já o tema de *Malwares* é conhecido pelo público-alvo, mas sob a perspectiva generalista dos vírus de computador. Embora semelhantes, a diferenciação entre eles é impor-

Figura 4. Exemplo de como um golpe *Phishing* é arquitetado: o atacante cria um anúncio de um produto falso que leva a vítima a um site falso, que se passa por legítimo, levando a vítima a comprar um produto que não será entregue.

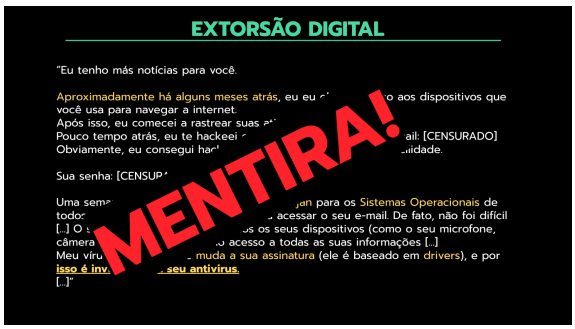

Figura 5. Um alerta reitera o cuidado que o público leigo deve ter, por exemplo, com um e-mail de extorsão, em que as informações pessoais da vítima já foram vazadas, como uma senha.

tante e foi abordada na primeira edição do curso de forma aprofundada, com a explicação dos diferentes tipos de *malware* presentes na Internet. Contudo, a apresentação foi extensa e ampliou o número de conceitos e termos técnicos, tornando-os mais distantes do público. Por isso, na segunda edição do curso, a definição geral de *malware* foi apresentada, desmistificando o termo técnico com exemplos e, posteriormente, foram explicados quais erros podem levar à infecção e quais são as boas práticas para se manter seguro. Assim, na última edição, os assuntos abordados focaram mais em informações que o público-alvo poderia verificar e aplicar no seu dia a dia.

3.2. Gerenciamento de Senhas Seguras e Criptografia

O tema de gerenciamento de senhas seguras tem como objetivo ensinar aos participantes como confeccionar senhas difíceis de serem descobertas por atacantes. Como forma de justificativa e motivação, são apresentados os métodos que permitem aos atacantes descobrir senhas fracas. Também é abordado como armazenar senhas com segurança. Foi recomendada uma série de boas práticas, como o uso de caracteres especiais, a adoção de senhas longas e a autenticação de dois fatores, além de alertar os participantes a evitar o uso de palavras, números ou frases diretamente relacionados ao usuário. Em ambas as edições, o conteúdo manteve a mesma estrutura.

Em seguida, foram apresentados os conceitos básicos de criptografia, uma vez que o tema, embora não seja amplamente conhecido pelo público-alvo, é útil para demons-

trar que, mesmo com falhas, os sistemas utilizados na Internet ainda empregam muitos mecanismos de defesa. Porém, diante da complexidade, a exposição precisou recorrer a analogias e a demonstrações práticas para promover um melhor entendimento entre o público. Em relação à primeira edição, o tema foi abordado de forma mais sucinta e com maior destaque para os fundamentos.

3.3. Lei Geral de Proteção de Dados (LGPD) e uso de *Cookies*

Um tema importante e recente na sociedade brasileira é a Lei Geral de Proteção de Dados (LGPD), que foi abordada sob a perspectiva de como sua adoção afeta a relação das pessoas na Internet [Garcia et al. 2020], mostrando como pode proporcionar maior segurança e proteção de dados sensíveis, bem como as consequências quando não é cumprida. Houve poucas mudanças em relação à primeira edição, concentradas nos exemplos apresentados, que foram substituídos por casos reais divulgados na mídia.

Figura 6. Casos reais de violação à LGPD. Exemplos de casos em que empresas e indivíduos foram penalizados após fiscalizações e investigações. Assim, reiterando ao público leigo que, embora recente, a LGPD já é aplicada no ambiente digital.

Na última parte do minicurso, o foco foi dado a temas de segurança digital com os quais o público já tem alguma familiaridade no dia a dia, mas que ainda geram muitas dúvidas. Após a definição do termo *Cookies* e do seu papel no funcionamento da *Web*, foram apresentadas as diferentes formas de utilização dessa solução, mostrando-a, a princípio, mais como um possível risco à privacidade do que à segurança. Posteriormente, a apresentação abordou boas práticas para evitar o vazamento não intencional de dados por parte dos usuários. Na segunda edição do curso, os conteúdos foram ampliados para abordar detalhes mais técnicos sobre seu funcionamento, já que foi relatada uma dificuldade de compreensão conceitual do termo na primeira edição.

3.4. *Virtual Private Networks* e *Hypertext Transfer Protocol Secure*

O tema foi escolhido por sua recente popularidade, já que uma série de empresas oferece o próprio serviço de *Virtual Private Networks* (VPNs) sob o pretexto de que essa rede torna a navegação de um usuário mais segura em uma rede pública. Dessa forma, foram

apresentados o funcionamento das VPNs, os possíveis problemas de segurança e como elas podem ser aplicadas como solução de privacidade.

No tema do protocolo *Hypertext Transfer Protocol Secure* (HTTPS), foi idealizado definir e explicar o protocolo ao público externo como um mecanismo de proteção contra uma infinidade de vulnerabilidades e pontos de exploração por pessoas mal-intencionadas, pois mitiga problemas de confidencialidade e de autenticidade na *Web*. Contudo, a existência do tema em um tópico próprio foi prejudicial na primeira edição do minicurso, pois os detalhes do protocolo tornaram a explicação excessivamente técnica e extensa, mesmo com o uso de abstrações e diagramas. Assim, na edição de 2025, foi mencionada brevemente como uma aplicação prática da criptografia para reduzir a densidade do tópico.

4. Desafios e Estratégias Adotadas

Em ambas as edições de 2024 e 2025, o projeto foi divulgado pelos canais oficiais do Instituto de Ciências Matemáticas e de Computação (ICMC), pelas mídias sociais do grupo *Ganesh* e por meio de uma entrevista em rádio local. Exclusivamente em 2025, a divulgação também foi realizada em uma emissora de televisão local. Essa expansão dos meios de divulgação justifica o aumento do número de participantes do curso e o maior alcance junto ao público externo à universidade.

Para maximizar o acesso ao conteúdo por públicos distintos, ambas as edições de 2024 e 2025 do minicurso foram realizadas presencialmente, em duas sessões, na quarta-feira à noite e no sábado à tarde. Os dados de *feedback* apresentados neste artigo foram coletados apenas dos participantes que frequentaram o minicurso presencialmente. A segunda exibição da edição de 2024 e ambas as exibições da edição de 2025 foram transmitidas ao vivo na plataforma *Youtube*, e suas gravações estão disponíveis gratuitamente nela. Durante a exibição, participantes que acompanhavam virtualmente enviaram dúvidas pelo *chat*, que eram respondidas em tempo real pelos apresentadores do minicurso.

5. Resultados do Minicurso e seus Impactos Educacionais

Como projeto de extensão, o objetivo do minicurso era ampliar o alcance da universidade junto ao público externo. Os dados coletados no formulário de *feedback* da edição de 2025, apresentados na Tabela 1, mostram não apenas um maior alcance geral, mas também um maior alcance entre o público externo, em comparação à edição anterior. Em 2024, dentre os 17 participantes, havia apenas um funcionário da universidade, oito alunos e oito sem vínculo com a universidade.

Os dados coletados do público no formulário de *feedback* da edição de 2025, apresentados na Tabela 1, demonstram que, dentre os 23 participantes da última edição, apenas um era funcionário da universidade, quatro eram alunos da universidade e dezoito não tinham vínculo com a universidade. Entre 2024 e 2025, o percentual de participantes externos à universidade aumentou de 47,1% para 78,3%. Esse aumento do público atingido e, principalmente, da proporção do público externo foi muito satisfatório para difundir conhecimento à sociedade gratuitamente.

A Tabela 2 apresenta a faixa etária dos participantes de ambas as edições do minicurso. Enquanto em 2024 apenas 11,8% dos participantes tinham mais de 65 anos, em

Tabela 1. Relação de categorias dos participantes dos minicursos entre 2024 e 2025

Categorias	**2024**	**%**	**2025**	**%**
Externo	8	47,1%	18	**78,3%**
Estudante USP	8	47,1%	4	17,4%
Funcionário	1	5,9%	1	4,3%
N. Participantes	**17**	**100,0%**	**23**	**100,0%**

2025 esse número cresceu para 30,4%. Isso representa um sucesso do projeto ao alcançar idosos que, muitas vezes, têm maior dificuldade em navegar com segurança na Internet ou receios decorrentes da falta de conhecimento.

Tabela 2. Faixa etária dos participantes dos minicursos entre 2024 e 2025

Faixa etária	**2024**	**%**	**2025**	**%**
< 18	1	5,9%	0	0,0%
18–24	7	41,2%	3	13,0%
25–34	0	0,0%	1	4,3%
35–49	4	23,5%	5	21,7%
50–64	3	17,6%	7	30,4%
> 65	2	11,8%	7	**30,4%**
N. Participantes	**17**	**100,0%**	**23**	**100,0%**

Os participantes podiam informar, no formulário de *feedback*, uma lista de temas abordados durante o minicurso, indicando quais já tinham conhecimento suficiente para que o minicurso não agregasse nada de novo. As respostas a essa pergunta podem ser observadas na Tabela 3, referente às edições de 2024 e 2025, para cada tema abordado.

Mais de 50% dos participantes não possuíam familiaridade com nenhum dos temas abordados e, portanto, o minicurso não deixou de ministrar nenhum tema por conta do conhecimento prévio de alguns participantes. O aumento de 58,8% para 65,2% da parcela dos participantes que não possuíam familiaridade com nenhum dos tópicos abordados demonstra um progresso no minicurso em atingir o público distante da área de computação.

Outra pergunta no formulário de *feedback* era sobre quais temas abordados no minicurso os participantes não conseguiram aprender durante a aula. As respostas a essa pergunta também podem ser observadas na Tabela 3. Em 2024, 29,4% dos participantes não compreenderam corretamente o tema HTTPS. Com isso, o *Ganesh* decidiu retirar esse tema da edição de 2025. Contudo, por se tratar de um assunto fundamental para a navegação segura na Internet, é do interesse do grupo abordar, em minicursos futuros, após a elaboração de novos materiais, a necessidade de priorizar o acesso a sites que utilizam HTTPS.

Outra observação é que mais de 30% dos participantes não conseguiram aprender sobre *Cookies* e VPN na última edição do minicurso. Novamente, a escolha de temas mais técnicos, que possivelmente foram abordados com profundidade elevada ou com uma metodologia distante do dia a dia, constitui um *trade-off* importante, com o qual se

pretende lidar melhor nas próximas edições.

O *Ganesh* espera que, mesmo que esses temas não tenham sido tão compreendidos, tenham, ao menos, sido desmistificados o suficiente para que os participantes tenham mais familiaridade para aceitar *Cookies* de um site confiável ou para não associar as VPNs sempre a um risco para a segurança digital. Todos os temas, com exceção da LGPD, registraram aumento na proporção de participantes que não compreenderam. Isso é um ponto a melhorar nas futuras edições, mas justifica-se pela maior participação do público externo à área de computação.

Tabela 3. Comparação dos temas de Segurança Digital previamente conhecidos e ainda não dominados pelos participantes nas edições de 2024 e 2025.

Tema	Já Conhecia? (2024) n=17 Resp. (%)	Já Conhecia? (2025) n=23 Resp. (%)	Não aprendeu? (2024) n=17 Resp. (%)	Não aprendeu? (2025) n=23 Resp. (%)
Tipos de Hacker	2 (11,8%)	3 (13%)	2 (11,8%)	3 (13%)
Engenharia Social	0 (0%)	2 (8,7%)	1 (5,9%)	2 (8,7%)
Senhas	3 (17,6%)	2 (8,7%)	0 (0%)	3 (13%)
Malware	2 (11,8%)	2 (8,7%)	1 (5,9%)	3 (13%)
Criptografia	3 (17,6%)	2 (8,7%)	1 (5,9%)	4 (17,4%)
HTTPS	2 (11,8%)	0 (0,0%)	5 (29,4%)	-
Cookies	2 (11,8%)	2 (8,7%)	1 (5,9%)	8 (34,8%)
VPN	2 (11,8%)	1 (4,3%)	2 (11,8%)	7 (30,4%)
LGPD	1 (5,9%)	2 (8,7%)	3 (17,6%)	3 (13%)
Nenhum	10 (58,8%)	**15 (65,2%)**	9 (52,9%)	8 (34,8%)

No formulário de *feedback*, os participantes poderiam atribuir uma nota à satisfação com a experiência do minicurso. A menor nota de satisfação foi 6, atribuída por apenas um participante, assim como as notas 7 e 8. Oito participantes atribuíram a nota 9 e doze a nota 10. A média das notas atribuídas pelos participantes foi de 9,26. Com base nessas notas, constatou-se que a experiência foi satisfatória para todos.

Somadas as transmissões em ambos os canais da segunda exibição de 2024 e as exibições de 2025, totalizaram 1190 visualizações e 113 curtidas. A transmissão de 2024 possui mais visualizações do que as de 2025, o que se justifica pelo maior tempo de disponibilidade na plataforma. Apesar do número de visualizações ser satisfatório, não é possível determinar quantas delas correspondem a participantes que assistiram a todo o conteúdo e realmente aprenderam algo novo. Para a próxima edição, coletar esse *feedback* dos participantes remotos será um importante ganho para a análise da qualidade do minicurso e do engajamento desses participantes.

6. Conclusão e Recomendações Finais

Este artigo apresenta um relato de experiência sobre as duas edições do minicurso "Como estar seguro na Internet?", promovido pelo grupo de extensão *Ganesh* no ICMC/USP, com o objetivo de ampliar a conscientização da sociedade sobre os riscos digitais e as boas práticas de segurança na Internet. Entre as edições de 2024 e 2025, foram alcançados

avanços significativos no número de participantes do público externo à universidade e na maior participação de pessoas com mais de 50 anos.

O aumento da proporção de participantes sem vínculo com a universidade e da faixa etária acima de 65 anos indica que as estratégias de divulgação adotadas em 2025, incluindo a ampliação para a televisão local, foram eficazes em alcançar públicos mais vulneráveis a golpes financeiros digitais. Esse relato de experiência destaca, como contribuição, que, nas ações educativas voltadas à comunidade em geral, a seleção de conteúdos deve priorizar a utilidade imediata, a linguagem acessível e exemplos contextualizados ao cotidiano dos participantes. Entre as perspectivas futuras, destaca-se a intenção de aprimorar os materiais didáticos, especialmente para temas que apresentaram maior dificuldade de compreensão, bem como de desenvolver mecanismos de coleta de *feedback* dos participantes remotos.

Com base nas experiências relatadas, recomenda-se que iniciativas semelhantes: (i) invistam em estratégias diversificadas de divulgação para alcançar públicos externos à universidade; (ii) adotem metodologias interativas e exemplos práticos, priorizando situações reais e estudos de caso; (iii) realizem avaliações sistemáticas por meio de formulários de *feedback*, utilizando os resultados como insumo para reestruturação contínua do conteúdo; e (iv) considerem a adaptação do nível técnico conforme o perfil do público-alvo.

7. Declaração sobre uso de Inteligência Artificial

Neste trabalho, em conformidade com o código de conduta da Sociedade Brasileira de Computação, os autores esclarecem que não foi utilizada nenhuma ferramenta de IA na redação do texto nem para correções gramaticais.

Referências

Astin, A. (1984). Student involvement: A development theory for higher education. *Journal of College Student Development*, 40:518–529.

Birthriya, S. K., Ahlawat, P., and Jain, A. K. (2025). A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies. *Journal of Applied Security Research*, 20(2):244–292.

Chetioui, K., Bah, B., Alami, A. O., and Bahnasse, A. (2022). Overview of social engineering attacks on social networks. *Procedia Computer Science*, 198:656–661. 12th International Conference on Emerging Ubiquitous Systems and Pervasive Networks / 11th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare.

Deterding, S., Dixon, D., Khaled, R., and Nacke, L. (2011). From game design elements to gamefulness: defining "gamification". In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, MindTrek '11, page 9–15, New York, NY, USA. Association for Computing Machinery.

Fauzi, M. A., Saad, Z. A., Aripin, M. A., and Sapuan, N. M. (2025). Let's play and learn: A state-of-the-art review on gamification-based learning with a bibliometric analysis in the higher education institutions. *Journal of Computer Assisted Learning*, 41(3):e70029.

FortNet (2025). Relatório da Fortinet do cenário de ameaças de 2025. `https://www.fortinet.com/br/resources/reports/threat-landscape-report`. [Accessed 28-02-2026].

Freire, P. (2014). *Educação como prática da liberdade*. Editora Paz e terra.

Garcia, L. R., Aguilera-Fernandes, E., Gonçalves, R. A. M., and Pereira-Barretto, M. R. (2020). *Lei Geral de Proteção de Dados (LGPD): guia de implantação*. Editora Blucher.

Jain, A. K., Sahoo, S. R., and Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex and Intelligent Systems*, 7(5):2157–2177.

Majumdar, S. (2022). Community engagement through extension and outreach activities: Scope of a college library. In *Handbook of Research on the Role of Libraries, Archives, and Museums in Achieving Civic Engagement and Social Justice in Smart Cities*, pages 121–138. IGI Global Scientific Publishing.

Mayer, R. E. (2009). *Multimedia Learning*. Cambridge University Press.

Morris, P. V., Pomery, J., and Murray, K. E. (2002). Service-learning: Going beyond traditional extension activities. *The Journal of Extension*, 40(2):17.

Salahdine, F. and Kaabouch, N. (2019). Social engineering attacks: A survey. *Future internet*, 11(4):89.

Salles, F. M., Marinho, E., Cruz, G., Scarpin, R. P., and Branco, K. (2025). Ganesh: um grupo de extensão para ensino de segurança da informação do icmc/usp. In *Simpósio Brasileiro de Sistemas Multimídia e Web (WebMedia)*, pages 195–201. SBC.

Umbach, R., Henry, N., Shelby, R., Stevens, G., and Gonzalez-Pons, K. (2026). Ai-generated image-based sexual abuse: Perpetration and consumption across three regions. *Computers in Human Behavior*, 179:108935.

Yildiz, D. and Nur, Z. (2024). Transformation of social interaction in the digital age: Impact, challenges, and prospects of technology in social relationships. *Bulletin of Science, Technology and Society*, 3(3):49–54.