



Uma Viagem pelo Tempo do Phishing

MOOC de Educação em Cibersegurança

Thales Sgarbi Salata¹ Daniel Fernando Pigatto¹

¹UTFPR - Câmpus Curitiba, Bacharelado em Sistemas de Informação



A viagem pelo tempo: seis paradas, uma por época



P0 • 1980s
O início do cibercrime
→ curiosidade vira ameaça
Visual: terminal verde



P1 • 1990s
A origem do *phishing*
→ iniciantes viram alvo
Visual: janela Windows 95



P2 • 2000s
A ascensão
→ o golpe vira negócio
Visual: web comercial azul



P3 • 2010s
O ataque direcionado
→ da massa ao alvo
Visual: sóbrio • Simulação I



P4 • 2020s
Sofisticação e automação
→ a máquina escreve o golpe
Visual: editor de código



P5 • O agora
Como se proteger
→ da história à ação
Visual: verde • Simulação II

Por que falar de phishing?

553 mi

ataques de *phishing* bloqueados no Brasil (jul/2024 a jul/2025) [4]

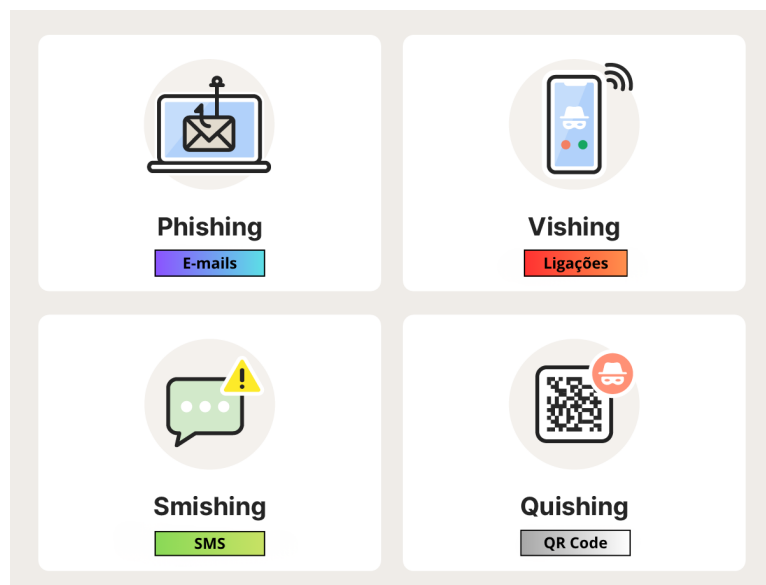
68-95%

das violações de segurança envolvem erro humano [7]

Tecnologia sozinha não basta: **é preciso educar pessoas.**

Objetivo: criar, aplicar e avaliar um **curso on-line aberto (MOOC)** sobre *phishing* para o público geral, no Portal Sophia-CT (Moodle da UTFPR).

O phishing multifacetado

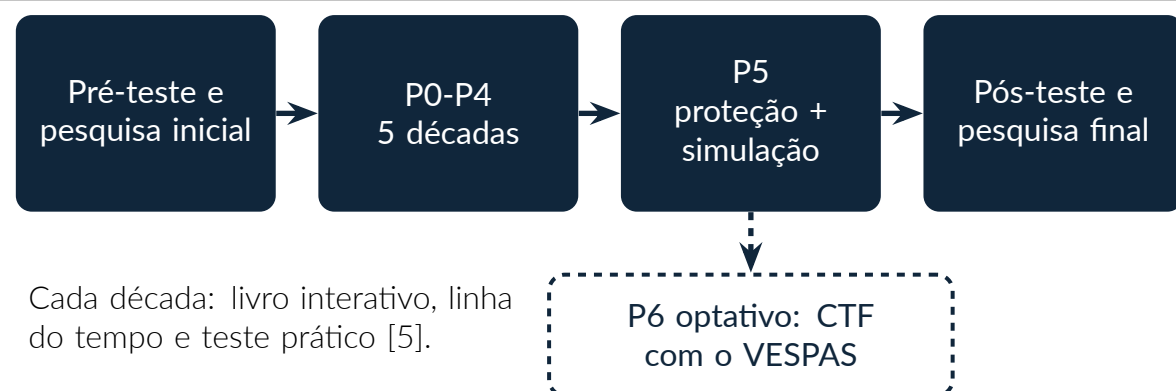


Chega por e-mail, SMS (*smishing*), ligação (*vishing*) e QR Code (*quishing*) - e sempre explora a **Engenharia Social**: urgência, autoridade e confiança.

Por canal	Por alvo	Por técnica
E-mail phishing e-mails fraudulentos Smishing SMS ou mensagem curta Vishing ligação ou voz Quishing QR Code adulterado	Spear phishing pessoas ou grupos específicos Whaling / BEC executivos e alto perfil	Malware phishing anexos e links maliciosos Clone phishing cópia de mensagem ou página legítima

IA generativa deixa o golpe mais convincente [1]; no MITRE ATT&CK é a técnica de acesso inicial T1566 [6].

Como o curso funciona



Cada década: livro interativo, linha do tempo e teste prático [5].

Próximos passos e acesso ao curso

Turmas maiores e diversas com grupo de controle • medir retenção semanas depois • consolidar a trilha CTF com o VESPAS.

Acesse o curso no Portal Sophia-CT:
sophia.ct.utfpr.edu.br/course/view.php?id=118

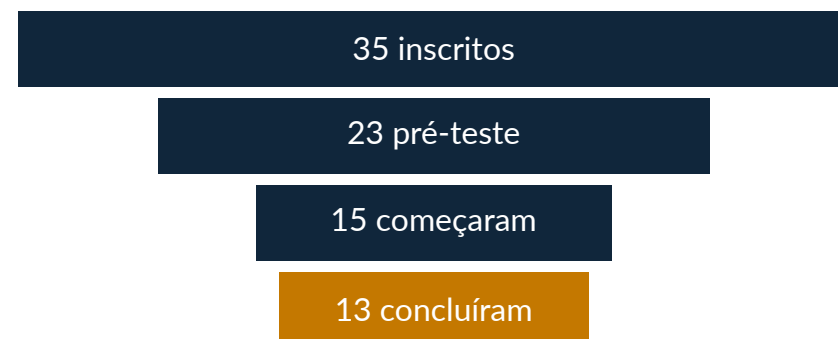


Evolução do phishing em palavras-chave



Adaptado do mapa mental da evolução do *phishing* (TCC, Cap. 2) [5].

Fase-piloto (jun/2026)



Amostra pequena e de conveniência, sem grupo de controle: **indícios, não prova.**

Ressalvas: evasão e quedas da plataforma [3]; efeito-teto (7,54 → 9,85); golpes caricatos, já revisados.

Reflexões

40 anos, a mesma isca.

Muda o canal, não o golpe: urgência, autoridade e confiança. Reconhecer o padrão vale mais que decorar golpes.

Comportamento antes de técnica.

Se o erro é humano, a defesa do leigo é reconhecer sinais - e a prática (simulações) foi o mais lembrado [2].

A IA apagou os sinais clássicos.

Sem erros de escrita, resta a regra de ouro: **confirmar por outro canal.**

Educar não é ser resiliente.

O curso mede conhecimento, confiança e intenção - não hábito duradouro. Resiliência é sistêmica e cultural.

Referências

- [1] Mohamed Amine Ferrag, Fatima Alwahedi, Ammar Battah, Bilel Cherif, Abdechakour Mechri, Norbert Tihanyi, Tamas Bisztray, and Merouane Debbah. Generative ai in cybersecurity: A comprehensive review of llm applications and vulnerabilities. *Internet of Things and Cyber-Physical Systems*, 5:1–46, 2025.
- [2] Hoxhunt. Does gamified cyber security training actually work? <https://hoxhunt.com/blog/gamified-cyber-security-training>, 2025.
- [3] Katy Jordan. Initial trends in enrolment and completion of massive open online courses. *The International Review of Research in Open and Distributed Learning*, 15(1):133–160, 2014.
- [4] Kaspersky. Panorama de ameaças 2025: o crescimento do phishing impulsionado pela ia no brasil. <https://www.kaspersky.com.br/blog/panorama-ameacas-2025/>, 2025.
- [5] KnowBe4. History of phishing. <https://www.knowbe4.com/resource-center/phishing>, 2025.
- [6] MITRE ATT&CK. T1566 - phishing. <https://attack.mitre.org/techniques/T1566/>, 2025.
- [7] Lay Hoon Yeo and Jill Banfield. Human factors in electronic health records cybersecurity breach: An exploratory analysis. *Perspectives in Health Information Management*, 19(Spring), 2022.