INSTITUTO FEDERAL
Tocantins

Comitê de Segurança da Informação

Resultados da Campanha de Phishing – Outubro 2025

Este documento apresenta os resultados consolidados das campanhas de simulação de phishing realizadas em outubro de 2025. A iniciativa faz parte do Programa de Conscientização, Educação e Treinamento em Privacidade e Segurança da Informação, e teve como objetivo central sensibilizar os usuários sobre os riscos de engenharia social.

A campanha foi dividida em duas fases para avaliar o impacto da abordagem na percepção de risco dos usuários:

- **Campanha I (Informativa):** Um e-mail passivo sobre uma atualização programada do SUAP.
- **Campanha II (Persuasiva):** Um e-mail com senso de urgência, solicitando a "validação de acesso" após a suposta atualização.

Taxa de Falha: Campanha I vs. Campanha II

A "Taxa de Falha" representa o percentual de servidores que não apenas clicaram no link, mas efetivamente submeteram seus dados (usuário e senha) na página de login falsa. O resultado demonstra o poder da engenharia social persuasiva.

0,90%	17,12%
Campanha I (Informativa)	Campanha II (Persuasiva)

Análise dos Resultados

Os dados consolidados revelam que a segunda campanha, utilizando gatilhos de **urgência e autoridade** ("valide seu acesso para evitar instabilidade"), foi **19 vezes mais eficaz** em induzir os usuários ao erro do que a primeira campanha, puramente informativa.

- Na Campanha I, apenas **13 servidores (0,90%)** submeteram suas credenciais.
- Na Campanha II, esse número saltou para **246 servidores (17,12%)**.

Um ponto crítico de atenção em ambas as campanhas foi a **taxa de reporte de 0%**. Nenhum dos 1.437 servidores utilizou a ferramenta ou respondeu ao e-mail para reportar a simulação de phishing à equipe de TI. Isso indica uma oportunidade de melhoria na comunicação dos canais de reporte de incidentes.

Detalhamento por Campanha e Campus

Campanha I: E-mail Informativo ("ATUALIZAÇÃO SUAPE")

Campus	E-mails Enviados	Links Clicados	Dados Submetidos	Taxa de Falha
Paraíso	104	3	2	1,92%
Dianópolis	80	1	1	1,25%
Colinas	83	2	1	1,20%
Araguatins	220	1	0	0,00%
Lagoa da Confusão	30	0	0	0,00%

Campus	E-mails Enviados	Links Clicados	Dados Submetidos	Taxa de Falha
Palmas	378	2	2	0,53%
Formoso	32	2	1	3,13%
Pedro Afonso	37	2	1	2,70%
Araguaína	105	1	0	0,00%
Gurupi	112	3	1	0,89%
Porto Nacional	110	1	1	0,91%
Reitoria	146	4	3	2,05%
TOTAL (Campanha I)	**1.437**	**22**	**13**	**0,90%**

Campanha II: E-mail Persuasivo ("Valide seu acesso")

Campus	E-mails Enviados	Links Clicados	Dados Submetidos	Taxa de Falha
Paraíso	104	19	17	16,35%
Dianópolis	80	9	7	8,75%
Colinas	83	34	22	**26,51%**
Araguatins	220	36	25	11,36%
Lagoa da Confusão	30	5	4	13,33%
Palmas	378	81	70	18,52%
Formoso	32	9	8	**25,00%**
Pedro Afonso	37	13	8	21,62%
Araguaína	105	26	24	22,86%
Gurupi	112	25	22	19,64%
Porto Nacional	110	24	20	18,18%
Reitoria	146	22	19	13,01%

Campus	E-mails Enviados	Links Clicados	Dados Submetidos	Taxa de Falha
TOTAL (Campanha II)	**1.437**	**303**	**246**	**17,12%**

Conclusão e Próximos Passos

A campanha atingiu seu objetivo de sensibilizar e, principalmente, de medir a atual postura de segurança dos usuários frente a diferentes táticas de engenharia social. Os resultados demonstram que, embora haja uma boa resistência a e-mails passivos, a vulnerabilidade a ataques persuasivos (que simulam urgência) é alta.

Os próximos passos planejados incluem:

1. Envio de um comunicado oficial a todos os servidores, explicando a campanha, apresentando os resultados e parabenizando os que não interagiram.
2. Divulgação do "Guia Rápido de Segurança Digital" (o PDF que criamos) como material de consulta oficial.
3. Disparo de um e-mail de orientação específico para os 246 servidores que submeteram seus dados, explicando o ocorrido e reforçando as boas práticas.
4. Inclusão, no Plano de Comunicação, de ações contínuas para educar os usuários sobre como e para quem reportar um e-mail suspeito de phishing.