CEFET/RJ

Manual de SEGURANÇA da Informação

Procedimentos oficiais para relato de e-mails de phishing

1 Introdução

A segurança da informação é uma responsabilidade de toda a comunidade acadêmica. Diariamente, instituições públicas federais são alvo de tentativas de fraudes eletrônicas, conhecidas como phishing. Essas mensagens maliciosas tentam enganar o usuário para que ele revele senhas e dados pessoais ou instale softwares nocivos em seus dispositivos.

Este manual tem como objetivo instruir formalmente sobre a maneira correta de agir ao identificar uma mensagem suspeita em sua caixa de entrada institucional.

2 Diretrizes principais: o que NÃO fazer e como proceder

ATENÇÃO: NUNCA ENCAMINHE UM E-MAIL SUSPEITO!

Evite encaminhar e-mails suspeitos ou mensagens de phishing, mesmo que seja para a equipe de TI.

O encaminhamento pode, inadvertidamente, ampliar a disseminação da ameaça entre usuários e comprometer informações técnicas importantes utilizadas pelos sistemas de segurança para análise e bloqueio da mensagem.

Sempre registre a ocorrência por meio da abertura de chamado, conforme as orientações institucionais.

ABERTURA DE CHAMADOS

Se você identificar uma possível tentativa de fraude e quiser registrá-la por meio de um chamado, envie uma imagem (print) do e-mail que mostre claramente o remetente e o assunto da mensagem.

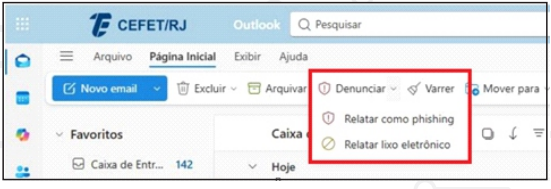
Com essas informações, a equipe técnica consegue localizar e bloquear o e-mail suspeito com segurança, sem que seja necessário encaminhar a mensagem maliciosa.

3 Como reportar phishing utilizando o Microsoft Outlook

A maneira mais eficaz e segura de lidar com um e-mail falso é utilizar a ferramenta nativa de denúncia do próprio Microsoft Outlook. Isso não apenas remove a mensagem da sua caixa de entrada, mas também treina os filtros de segurança da instituição e da Microsoft para bloquear ataques futuros.
Siga as instruções abaixo de acordo com a plataforma que você está utilizando.

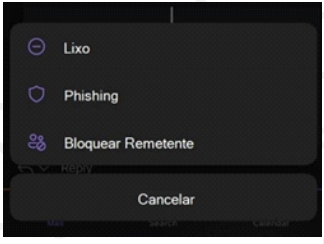
3.1 No Outlook na Web (navegador)

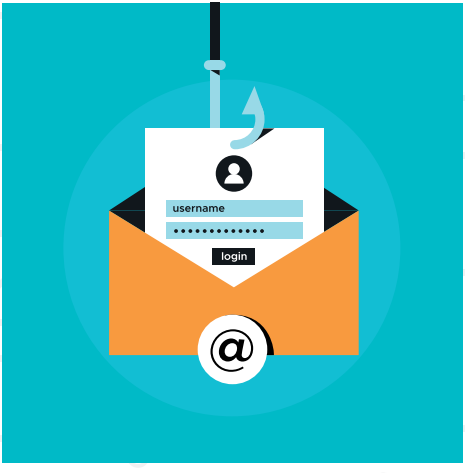
- Na sua lista de mensagens, selecione o e-mail que você considera suspeito.
- Na barra de ferramentas superior, localize e clique no botão Denunciar (representado por um ícone de escudo com um sinal de aviso).
- No menu suspenso que se abrirá, selecione a opção Relatar como phishing.
- O e-mail será automaticamente movido para a pasta de Lixo Eletrônico e os dados técnicos serão enviados para análise de segurança.



3.2 No aplicativo Outlook para dispositivos móveis (celular/tablet)

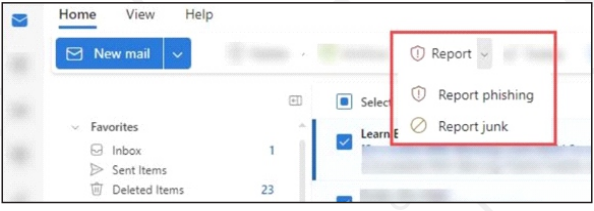
- Abra o aplicativo Outlook e selecione o e-mail suspeito.
- Toque no ícone de três pontos (⋮) localizado na parte superior direita da tela da mensagem.
- No menu que aparecer, selecione Denunciar Lixo Eletrônico (ou Report Junk).
- Em seguida, escolha a opção Phishing.





3.3 No aplicativo Outlook para desktop (Windows/Mac)

- Selecione a mensagem suspeita na sua lista de e-mails.
- Na faixa de opções superior (aba Página Inicial), procure pelo botão Reportar ou Denunciar Mensagem.
- Clique na seta para baixo para expandir as opções e selecione Relatar phishing (Report phishing).
- Confirme a ação se solicitado. A mensagem será tratada e removida da sua caixa de entrada.



4 O que fazer se você acha que caiu em um golpe?

Se você suspeita que possa ter clicado em um link malicioso ou fornecido suas credenciais inadvertidamente, é crucial agir com rapidez para minimizar os danos. Siga, imediatamente, os passos a seguir.

- **Registre os detalhes:** enquanto o evento está recente, anote o máximo de informações possível. Lembre-se de quais dados foram inseridos (nomes de usuário, senhas, matrículas) e onde o ataque ocorreu.
- **Altere suas senhas:** mude, imediatamente, a senha da sua conta institucional e de quaisquer outros serviços onde você utilize a mesma senha. Certifique-se de criar senhas fortes e exclusivas.
- **Verifique a Autenticação Multifator (MFA):** confirme se a verificação em duas etapas está ativada na sua conta. Isso adiciona uma camada vital de segurança.
- **Notifique a TI:** Abra um chamado para a equipe de Tecnologia da Informação imediatamente para relatar o comprometimento da conta institucional, permitindo que medidas de contenção sejam aplicadas.