MÓDULO 3

# PHISHING NA PRÁTICA

## Desmascarando o e-mail falso

O *Phishing* continua sendo uma das táticas de ataque mais prevalentes e perigosas, especialmente em instituições financeiras como cooperativas de crédito. Este artigo serve como um guia prático para identificar e neutralizar e-mails maliciosos. Detalhamos os **quatro sinais de alerta** cruciais que todo colaborador deve observar (remetente, links, anexos e linguagem) para desmascarar uma tentativa de *phishing*. Exploramos as consequências devastadoras de clicar em um link perigoso e, o mais importante, estabelecemos o **procedimento correto** e sem medo para reportar e-mails suspeitos, transformando a desconfiança em uma ação de segurança coletiva.

# 1. O phishing e a ilusão da comunicação

O termo *Phishing* deriva da palavra "fishing" (pescar), pois o criminoso "lança uma isca" (o e-mail falso) na esperança de que a vítima "morda" (clique no link ou forneça dados). É uma forma de Engenharia Social que utiliza a comunicação eletrônica para se passar por uma entidade confiável (banco, colega, fornecedor, TI) e induzir o destinatário a realizar uma ação que comprometa a segurança [1].

Para uma cooperativa de crédito, o *phishing* é uma ameaça constante, pois os fraudadores buscam acessar informações financeiras e dados sensíveis dos cooperados. A defesa contra o *phishing* não reside em softwares complexos, mas sim na **capacidade de observação e desconfiança** de cada colaborador.

# 2. Os 4 sinais de alerta de um e-mail malicioso

Apesar de os e-mails de *phishing* estarem cada vez mais sofisticados, eles quase sempre contêm falhas que os denunciam. O colaborador deve treinar o olhar para identificar os **quatro sinais de alerta** antes de tomar qualquer atitude.

## 2.1. Sinal 1: O endereço do remetente é suspeito

O primeiro e mais importante passo é verificar o endereço de e-mail completo, e não apenas o nome de exibição.

**Domínio incorreto:** Vamos imagina que o endereço de e-mail legítimo seja suporte@crediseara.coop.br então um e-mail suspeito seria suporte@credseara.coop.br sem o “i” de Credi.

**Substituição de Caracteres:** Outra situação comum é caracteres serem trocados como a letra ”O” pelo número “0”(zero), dessa forma teríamos suporte@crediseara.c00p.br.

**Uso de E-mails Pessoais:** O mais evidente de todos um e-mail com domínio comum como suporte@gmail.com.

**Diretriz Prática:** Se o e-mail for de uma empresa conhecida (Google, Microsoft, Receita Federal), verifique se o domínio é o oficial. Se for interno, verifique se o endereço corresponde ao padrão da cooperativa.

### 2.2. Sinal 2: Links e URLs Desconhecidos

Os criminosos tentam fazer com que o link pareça legítimo, mas o destino real é sempre um site falso, para verificar **passe o mouse sobre o link (não clique!)** e observe o endereço que aparece na parte inferior da tela ou em uma pequena caixa de texto, se o texto do link diz "www.cooperativa.com.br" mas o endereço que aparece ao passar o mouse é "www.fraude.xyz/login", **é um ataque**, além disso tenha em mente qie links encurtados ou com sequências aleatórias de números e letras também são altamente suspeitos.

### 2.3. Sinal 3: Anexos Inesperados ou Estranhos

O objetivo do anexo é instalar um *malware* (software malicioso), como um *ransomware*, no computador, então ao receber um anexo sem esperar **não abra, a chance de ser uma encrenca é grande.**, mesmo que pareçam vir de um colega conhecido. O e-mail dele pode ter sido comprometido. Uma boa prática é observar sempre a extensão do arquivo, por isso tenha especial cuidado com arquivos executáveis (.exe), arquivos compactados (.zip, .rar, já que não se sabe o conteúdo até descompactar) ou documentos que exigem a "habilitação de macros" para serem visualizados, geralmente arquivos do Office(Word, Excel ou PowerPoint).

### 2.4. Sinal 4: Linguagem de Urgência, Ameaça ou Erros Gramaticais

O texto do e-mail é projetado para induzir a vítima a agir por impulso (Engenharia Social) como vimos no módulo anterior. Fique especialmente atento a todos e-mails que estão solicitando algum tipo de urgência, que ameacem cancelamento de contas, acessos ou bloqueio e restrições documentais. Observe que normalmente esses e-mail contém erros básicos de português que podem ser facilmente notados, basta ter atenção.

## 3. O Que acontece ao clicar em um link perigoso

O colaborador precisa entender a gravidade da ação para internalizar a importância da prevenção. Clicar em um link de *phishing* ou abrir um anexo malicioso pode ter consequências imediatas e catastróficas [3] pois os atacantes usam técnicas bastante robustas para capturar, infectar ou roubar dados e informações como por exemplo o **roubo de credenciais** em que o link clicado leva a uma página de *login* falsa, idêntica à da cooperativa. Ao digitar seu usuário e senha, você os entrega diretamente ao fraudador (*Keylogging*), **infecção por *malware*** onde o clique ou o anexo instala um software malicioso que pode criptografar todos os arquivos do seu computador e da rede da cooperativa, paralisando as operações, **vazamento de dados** em que o *malware* instalado pode roubar informações sensíveis, como dados de cooperados (violando a LGPD) ou segredos de negócio, enviando-os para o criminoso ou **comprometimento da rede** onde seu computador se torna um "agente" do criminoso dentro da rede da cooperativa, que pode ser usado para atacar outros sistemas internos.

## 4. O procedimento correto para reportar e-mails suspeitos

A ação mais importante após identificar um e-mail suspeito é **reportá-lo imediatamente** à equipe de segurança ou TI da cooperativa, seguindo o protocolo interno. O reporte rápido pode proteger toda a organização.

| Passo | Ação | Por que Fazer? |
|---|---|---|
| **Passo 1: Não Clique, Não Responda** | **NÃO** interaja com o e-mail. Não clique em links, não abra anexos e não responda ao remetente. | Qualquer interação pode confirmar ao criminoso que seu endereço é válido, aumentando os ataques futuros. |

| | | |
|---|---|---|
| **Passo 2: Encaminhe com Cautela** | Encaminhe o e-mail suspeito para o canal oficial de reporte da cooperativa (geralmente um endereço como seguranca@coop.com.br ou abuse@coop.com.br). | O encaminhamento permite que a equipe de TI analise os cabeçalhos do e-mail para rastrear a origem e bloquear o remetente. |
| **Passo 3: Delete** | Após o encaminhamento, delete o e-mail da sua caixa de entrada e da lixeira. | Reduz o risco de clicar acidentalmente nele mais tarde. |
| **Passo 4: Alerte a Equipe** | Se o e-mail parecer vir de um colega, ligue para ele (em um canal de comunicação diferente) para alertá-lo que o e-mail dele pode ter sido comprometido. | Ajuda a conter a propagação do ataque dentro da cooperativa. |

**Diretriz Fundamental: Reporte sem medo de culpas.** O objetivo da cooperativa é a segurança coletiva, e o reporte rápido é uma atitude de responsabilidade. A equipe de TI prefere mil reportes falsos a um único incidente real.

# 5. Conclusão

O *phishing* é uma batalha de inteligência e atenção. Ao dominar a arte de desmascarar o e-mail falso através da observação dos quatro sinais de alerta, o colaborador se torna um filtro de segurança vital. Lembre-se: **a dúvida é a sua melhor defesa**. Se algo parece estranho, pare, pense e reporte. Essa atitude proativa é o que garante a segurança dos dados da cooperativa e a confiança dos cooperados.

Referências Bibliográficas

[1] Arcserve. **Não Entre em Pânico! O Que Fazer se Você Receber um E-mail de Phishing**. Disponível em: https://www.arcserve.com/pt/blog/nao-entre-em-panico-o-que-fazer-se-voce-receber-um-e-mail-de-phishing

[2] Lumiun. **4 sinais de que sua empresa recebeu um e-mail de phishing**. Disponível em: https://www.lumiun.com/blog/4-sinais-de-que-sua-empresa-recebeu-um-e-mail-de-phishing/

[3] Rastek Soluções. **Engenharia social: como proteger sua empresa e colaboradores**. Disponível em: https://rasteksolucoes.com.br/2023/01/engenharia-social-como-proteger-sua-empresa-e-colaboradores/

[4] (Adicionar referências adicionais conforme aprofundamento da pesquisa, se necessário).