Cartilha de Segurança: Como se Proteger de Phishing no E-mail Institucional

O que é Phishing?

Phishing é uma técnica de fraude digital em que criminosos se passam por pessoas ou empresas confiáveis para roubar dados sensíveis, como senhas, números de cartão e credenciais de acesso. O e-mail institucional é um dos principais alvos desse tipo de ataque.

Principais Métodos de Ataque

1. E-mails Falsos (Spoofing): Utilizam endereços de e-mail parecidos com os oficiais.
2. Links Maliciosos: Levam o usuário a páginas falsas ou instalam malwares.
3. Anexos Infectados: Arquivos disfarçados que instalam vírus.
4. Engenharia Social: Fingem ser colegas ou superiores e pedem ações urgentes.

Como Identificar um E-mail de Phishing

- Verifique o Remetente: Confirme se o e-mail é realmente institucional.
- Desconfie de Urgência ou Ameaças: Frases alarmistas são comuns em golpes.
- Passe o Mouse Sobre os Links: Veja se o link bate com o que é exibido.
- Observe Erros de Ortografia: Erros grosseiros são sinais de alerta.
- Anexos Inesperados: Não abra arquivos de remetentes desconhecidos.

Boas Práticas para Evitar Phishing

- Nunca compartilhe senhas por e-mail.
- Confirme com o remetente por outros meios.
- Atualize suas senhas periodicamente.
- Mantenha-se atento, mesmo com e-mails aparentemente confiáveis.
- Não clique em links ou baixe arquivos sem verificar.
- Reporte e-mails suspeitos à equipe de TI ou Segurança.

Exemplo de E-mail Suspeito

De: suporte@empresa-suporte.com

Assunto: URGENTE: Sua conta será desativada

Cartilha de Segurança: Como se Proteger de Phishing no E-mail Institucional

Mensagem:

Clique aqui para confirmar suas credenciais e evitar o bloqueio da sua conta.

Esse e-mail contém:

- Domínio estranho
- Linguagem de ameaça
- Pedido urgente
- Link suspeito

Contato da Equipe de Segurança

Em caso de dúvida ou suspeita, entre em contato com:

Equipe de Segurança da Informação

Email: ti@macae.rj.gov.br