MARCELLA AMADO

O QUE VOCE PRECISA SABER PARA NÃO CAIR EM GOLPES DIGITAIS.

Entendendo os crimes digitais. Parte 1

MARCELLA AMADO
SOLUÇÕES DIGITAIS E LGPD

P**hishing: Não morda a isca!**

Phishing é um tipo de ataque cibernético cada vez mais comum, onde criminosos tentam enganar as pessoas para roubar informações confidenciais, como senhas e dados de cartão de crédito. É essencial estar sempre atento e saber identificar esses ataques para se proteger. Neste documento, vamos explorar o que é o phishing, como ele funciona, e as melhores formas de se prevenir e reagir caso seja vítima.

O que é o Phishing?

O phishing é uma forma de fraude online em que o criminoso se passa por uma pessoa ou empresa confiável para tentar obter informações pessoais e financeiras da vítima. Através de e-mails, mensagens de texto, ligações telefônicas ou até mesmo perfis falsos em redes sociais, os criminosos enviam comunicações enganosas com o objetivo de convencer a vítima a compartilhar dados sensíveis, como números de cartão de crédito, senhas de acesso e informações de login.

Como funciona o Phishing?

Métodos de Contato

Os fraudadores utilizam diversos métodos para entrar em contato com as vítimas, como:

- E-mails fraudulentos
- Mensagens em redes sociais
- SMS (smishing)
- Chamadas telefônicas (vishing)

Aspectos Comuns

Esses ataques geralmente têm algumas características em comum, como:
Parecem ser de fontes confiáveis
Contêm links ou anexos maliciosos
Pedem informações pessoais ou financeiras
Urgência em ação solicitada

Identificando o Phishing

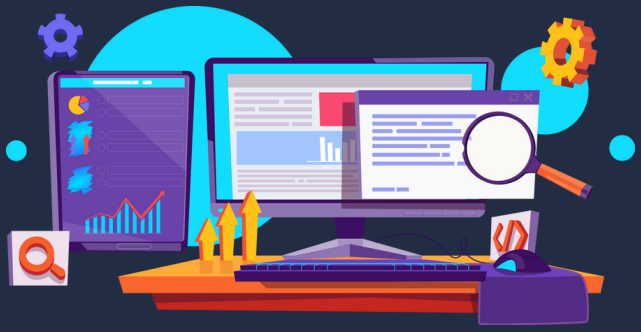
Algumas dicas para identificar um ataque de phishing:

- Verificar o remetente do e-mail
- Ficar atento a erros de gramática ou ortografia
- Evitar clicar em links ou baixar anexos suspeitos
- Usar autenticação multifator para proteger suas contas

Como se Prevenir do Phishing?

Educação sobre Segurança

Investir em treinamentos e campanhas de conscientização sobre os riscos do phishing é fundamental para que as pessoas saibam identificar e evitar esses ataques.



Soluções de Segurança

Instalar softwares de segurança confiáveis, como antivírus e firewalls, pode ajudar a proteger seus dispositivos e informações contra ameaças de phishing.

Manter Atualizações

Manter seus sistemas operacionais, aplicativos e programas de segurança sempre atualizados é essencial para fechar brechas que possam ser exploradas pelos golpistas.

Fazer Backups Regularmente

Criar backups regulares de seus dados importantes é uma ótima maneira de se proteger caso suas informações sejam comprometidas por um ataque de phishing.

O que Fazer se for Vítima de Phishing?

Mude as Senhas

Caso suas informações de login tenham sido roubadas, mude imediatamente as senhas de todas as suas contas, especialmente as mais importantes.

Alerte as Instituições

Entre em contato com o banco, empresa ou serviço afetado e informe sobre o incidente para que eles possam tomar as medidas necessárias.

Denuncie o Ataque

Reporte o ataque de phishing às autoridades competentes, como a polícia ou órgãos de proteção ao consumidor, para ajudar a combater esse tipo de fraude.

Monitore suas Contas

Fique atento a qualquer atividade suspeita em suas contas e cartões de crédito, e informe imediatamente se notar algo irregular.

Informaçoes Adicionais

Guia da Polícia Federal sobre Phishing:

https://www.gov.br/pf/pt-br/assuntos/prevencao-a-fraudes/golpes-financeiros/phishing

Dicas do Procon sobre Fraudes Virtuais:

https://www.procon.sp.gov.br/dicas-de-seguranca/fraudes-virtuais/

Informações do CERT.br sobre Ataques de Phishing:

https://www.cert.br/docs/cartilhas/cartilha-phishing.pdf

MARCELLA AMADO
SOLUÇÕES DIGITAIS E LGPD