

# Phishing, o que é?

## Segurança da Informação



## Informativos Gerais



# Phishing, O que é?

Phishing é um termo derivado de fishing (palavra em inglês que significa "pesca") e faz alusão ao ato de se lançar uma isca e esperar que "mordam". Trata-se de uma forma de golpe digital em que criminosos se passam por entidades confiáveis, como bancos ou empresas, para enganar pessoas e conseguir acesso a informações sigilosas.

**O objetivo é fazer  
com que você:**

- **Forneça dados pessoais ou profissionais;**
- **Instale programas maliciosos no computador ou celular;**
- **Clique em links perigosos;**
- **Baixe arquivos contaminados com vírus.**

Esses golpes costumam chegar por e-mail, mensagens de texto ou sites falsos que imitam empresas conhecidas.

# Como pode te prejudicar?

Caso seus dados sejam roubados, você pode ser vítima de:

- Cobranças desconhecidas no seu cartão de crédito;
- Contratações indevidas de serviços em seu nome;
- Crimes de estelionato cometidos em seu nome;
- Reprovação inesperada de crédito.

# Como pode prejudicar uma empresa?

Se informações da empresa forem expostas ou roubadas:

- A reputação da organização pode ser manchada;
- A competitividade no mercado pode ser afetada;
- Podem ocorrer perdas financeiras;
- A empresa pode responder legalmente.

# Como identificar um phishing?

## Verifique o endereço do remetente

Golpistas podem usar e-mails parecidos com os de empresas reais.

Exemplo: suporte@bancco.com no lugar de suporte@banco.com

- Sempre confira o endereço completo;
- Se parecer estranho, não abra e não clique.

# Como identificar um phishing?

## Cuidado com links e anexos

- Passe o mouse sobre o link para ver o endereço real;
- Se o endereço parecer suspeito, não clique;
- Não abra anexos não solicitados — eles podem conter vírus ou malware.

## Desconfie de mensagens urgentes ou alarmantes

Golpes de phishing costumam usar urgência ou medo para enganar você.

Exemplo: “Atualize seus dados AGORA ou sua conta será bloqueada!”  
Se a mensagem for exagerada, suspeite.

## Atenção com promoções boas demais para ser verdade

Mensagens oferecendo viagens muito baratas, presentes grátis ou prêmios relâmpagos geralmente são armadilhas.

Desconfie de e-mails com “clique aqui para receber algo”.

# Como identificar um phishing?

## Empresas sérias não solicitam informações sigilosas por e-mail

- O e-mail está pedindo dados pessoais, bancários ou senhas?
- Usa logo de empresa conhecida, mas com e-mail estranho?
- Não tem assinatura ou meios oficiais de contato?

### **Antes de agir, verifique:**

- Você conhece o remetente?
- Há links suspeitos na mensagem?
- O e-mail tem anexos que você não esperava?

Segurança é responsabilidade de todas as pessoas.  
Atente-se aos detalhes e aja com cautela para evitar prejuízos.



Rede  
**Américas**

paixão por cuidar