# CRIMES VIRTUAIS

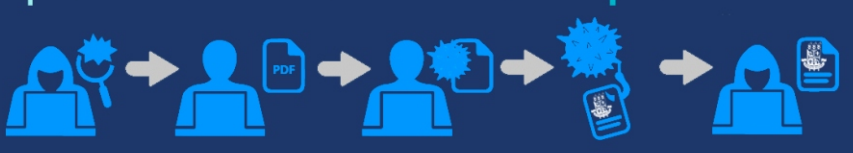
## PHISHING

**Phishing** é um termo oriundo do inglês, **fishing** - que significa pesca, e uma forma de ataque normalmente eletrônico, que pode resultar em fraude.


Seu objetivo é roubar os **dados sigilosos de usuários** de computadores como dados de banco,senhas e informações pessoais.

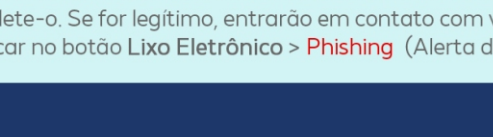
Um ou mais alvos são contatados por
**email**, **telefone** ou **mensagem de texto**
por alguém que se apresenta como uma instituição legítima.

## Exemplo de um Cenário de Ataque




1. O atacante realiza um ataque de reconhecimento.
2. O usuário recebe um email com um anexo de arquivo pdf supostamente do Suporte de TI da Uneb.
3. O usuário abre o arquivo anexado que executa o malware.
4. O malware rouba credenciais do usuário e dados confidenciais.
5. O malware envia os dados roubados para um usuário remoto.

## BRASIL É O PAÍS COM MAIS USUÁRIOS ATACADOS POR PHISHING



Relatório da fabricante de antivírus Kaspersky Lab aponta que um em cada cinco brasileiros recebe mensagens fraudulentas.

Em 2019, o total mensal de incidentes teve um aumento de

**232%**

Fonte: www.apwg.org



Os ataques através de esquemas de phishing em dispositivos móveis aumentaram em média **85%** ao ano, desde 2011

**O golpe é responsável por mais de:**

**90%** das infecções por malware

**72%** das violações de dados nas organizações

Fonte: Agência da União Europeia para Segurança das Redes e da Informação (2019)

Fonte: El Pescador

## 5 MANEIRAS PARA EVITAR UM ATAQUE DE PHISHING

### 1 Quem é o verdadeiro remetente?

Um ataque de phishing geralmente é enviado a partir de um e-mail que parece ser familiar, mas que não tem nenhuma relação com você, com o seu setor ou a Uneb. **Fique atento!**

### 2 Confira a saudação

Desconfie quando a saudação inicial do e-mail é genérica ou quando se refere à você como seu nome de e-mail. **É suspeito!**

### 3 Passe o mouse

Ao passar o mouse em cima de um link, ele identifica o hiperlink ou botão para onde você será direcionado, **sem clicar**.

**ATENÇÃO:** O destino será exibido no **canto inferior esquerdo da tela.** Faça o teste! **Sem clicar, é claro!**

### 4 O que tem no rodapé?

Um endereço legítimo sempre tem **dados** no rodapé, como:

**Um endereço físico da instituição ou marca;**
**Uma opção para cancelar o recebimento de e-mails futuros.**

Se um dos itens acima não existir, pode ser um link **falso**.




### 5 Em dúvida? Delete.

Se você não conhece o remetente ou não tem certeza se o e-mail é verdadeiro, delete-o. Se for legítimo, entrarão em contato com você novamente. Outra opção é clicar no botão **Lixo Eletrônico** > Phishing (Alerta de Phish) para denunciar o email.

## NUNCA FORNEÇA A SUA SENHA A NINGUÉM!

Informe-se, conheça a Política de Segurança da Informação da UNEB em:

**www.gerinf.uneb.br**

contato: sd@uneb.br

UNEB UNIVERSIDADE DO ESTADO DA BAHIA

GERINF GERÊNCIA DE INFORMÁTICA