MANUAL DE PREVENÇÃO A GOLPES DIGITAIS (PHISHING)

Guia prático para usuários iniciantes — Educação e Segurança Digital

1. O que é Phishing?

Phishing é uma tática criminosa que tenta *enganar o usuário* para que ele entregue informações pessoais como senhas, CPF, dados bancários e número do cartão de crédito.

Os golpistas fazem isso imitando:

* E-mails de lojas (ex.: Magazine Luiza, Amazon, Mercado Livre)

* Mensagens de bancos ou fintechs (ex.: Nubank, Itaú)

* Sites falsos que parecem reais

* SMS e WhatsApp com links maliciosos

É basicamente um disfarce digital: parece verdadeiro, mas serve para roubar dados.

🔹 2. Como os golpistas convencem a vítima?

Normalmente através de:

🟥 **Senso de urgência**:

Ex: “Seu pedido será cancelado em 1 hora!”,

“Atualize seus dados agora ou sua conta será bloqueada!”.

🟥 **Promoções boas demais para ser verdade:**

Ex: iPhone por R$ 199, cupom exclusivo, brinde grátis.

🟥 **Imitação de marcas famosas, que usam logos, cores e layouts reais para parecerem legítimos.**

🟥 **Links encurtados ou URLs parecidas:**

Exemplos de URLs falsas:

* magaz1neluiza.com

* oferta-magalu.store

* atualizar-magalu.shop

3. Principais meios usados nos golpes

* *E-mails falsos*
* *Sites clonados*
* *SMS (smishing)*
* *WhatsApp (phishing social)*
* *Anúncios patrocinados falsos* no Google ou Instagram
* *QR Code malicioso*

🔹 4. Como identificar um golpe? (Checklist do usuário)

Sempre verifique:

✔ 1. O remetente / número:

* Bancos usam domínios oficiais (ex.: @nubank.com.br)

* Lojas não enviam e-mails com domínios estranhos (ex.: @ofertas-magalu.xyz)

✔ 2. A URL antes de clicar:

Passe o mouse por cima do link → confira se é realmente .com.br.

✔ 3. Erros de português:

Fraudes costumam ter erros de ortografia ou frases estranhas.

🔹 4. Como identificar um golpe? (Checklist do usuário)

✔ 4. Pedido de dados pessoais:

Nenhuma empresa legítima pede:

* Senha

* Token

* Código de 2FA

* Dados do cartão

✔ 5. Promessas exageradas:

Desconto alto demais → 99% de chance de ser golpe.

✔ 6. Layout estranho:

Cores, botões desalinhados, imagens borradas, logotipos antigos.

5. E se eu já tiver clicado?

1. **Troque imediatamente suas senhas.**
2. **Ative o 2FA em todas as contas.**
3. **Entre em contato com o banco* para bloquear cartão.**
4. **Verifique se há logins suspeitos em e-mail e redes sociais**
5. **Denuncie:**

   *** Para a loja/banco imitado**

   *** Para a Polícia Civil (delegacia virtual)**

   *** Para o CERT.br**