GUIA DE SEGURANÇA DE UM HACKER // INFOGRÁFICO 01/08

PHISHING E GOLPES: ANATOMIA DE UMA FRAUDE

Os atacantes imitam seu banco, suas redes sociais ou seu provedor para roubar seus dados e seu dinheiro. Aprenda a reconhecer o golpe antes de clicar.

>> SINAIS DE ALERTA

01 Urgência artificial
"Aja agora ou sua conta será bloqueada". Querem que você aja sem pensar.

02 Prêmios e dinheiro fácil
"Você ganhou um prêmio, informe seus dados para resgatá-lo". Exploram a ambição.

03 Endereço quase idêntico
www.faceb00k.com em vez de facebook.com: zeros que parecem letras "o".

04 Links encurtados
bit.ly/Ub1XC1 esconde o destino real. O navegador pode acabar em outro site.

05 Anexos inesperados
Arquivos que, ao serem abertos, instalam malware e roubam seus dados.

06 Visual "oficial"
Usam logos, textos e estética reais da empresa. Parecer bem-feito não prova nada.

>> VARIANTES DO MESMO Ggolpe

PHISHING – e-mail

SMISHING – SMS / WhatsApp

QUISHING – códigos QR falsos em parquímetros, restaurantes e mensagens

>> PROTOCOLO DIANTE DE QUALQUER MENSAGEM SUSPEITA

1. **Sempre desconfie**
Desconfie de toda mensagem que receber, de conhecidos ou não. Pense duas vezes antes de clicar.

2. **Não clique nem abra anexos de desconhecidos**
O ideal é ignorá-los diretamente.

3. **Nunca entregue seus dados por mensagem**
Os serviços legítimos não pedem usuário e senha dessa forma.

4. **Verifique pelo canal oficial**
Na dúvida, ligue para a empresa para confirmar se a mensagem é verdadeira.

5. **Inspecione o endereço exato**
Antes de digitar seus dados, confirme que a URL coincide exatamente com a do site verdadeiro.

REGRA DE OURO

Sempre desconfie e depois verifique antes de confiar.