

PROTEJA-SE NA INTERNET

Guia Básico de Cibersegurança

⊘ NUNCA FAÇA ISTO

● MAIS PERIGOSO - NUNCA, EM CASO ALGUM:

- Dar códigos ou palavras-passe por telefone
- Enviar dinheiro a desconhecidos
- Associar MB Way a pedido de terceiros
- Instalar programas a pedido de "técnicos"
- Clicar em links de SMS ou emails suspeitos

⚠ OUTROS COMPORTAMENTOS DE RISCO:

- Usar a mesma palavra-passe em vários sites
- Abrir anexos de emails inesperados
- Partilhar dados pessoais nas redes sociais
- Guardar passwords no telemóvel ou em papéis visíveis

⚠ SINAIS DE ALERTA

Desconfie sempre se a mensagem tiver:

- Urgência: "Tem de agir já!"
- Ameaças: "A sua conta será bloqueada"
- Prémios: "Ganhou um prémio!"
- Pedidos de ajuda: "Preciso de ajuda urgente"
- Ofertas demasiado boas: "Preço incrível só hoje"
- Erros de português ou traduções estranhas
- Email ou número desconhecido
- Pedido para não contar a ninguém

✅ FAÇA SEMPRE ISTO

- Use **palavras-passe longas** (mínimo 12 caracteres)
- **Pare e pense** antes de clicar ou pagar
- Confirme sempre **ligando para o número oficial**
- Peça ajuda a um **familiar ou amigo de confiança**
- Mantenha telemóvel e computador atualizados
- Verifique o **cadeado** 🔒 nos sites
- Guarde comprovativos de compras online
- Ative a **verificação em 2 passos** (2FA)

Exemplo prático:

Recebeu um SMS dos CTT ou da DHL?

👉 **Não clique.** Escreva o endereço do site manualmente ou ligue para o contacto oficial.

📠 BURLAS MAIS COMUNS

- **SMS dos CTT/DHL:** "Encomenda retida, pague taxa"
- **Email do banco:** "Confirme os seus dados"
- **Chamada telefónica:** "Sou do banco, dê-me o código"
- **MB WAY:** "Associe ao meu número"
- **Falso técnico Microsoft:** "O seu computador tem vírus"
- **Herança ou lotaria falsa**
- Mensagem "Olá Pai / Olá Mãe, perdi o telemóvel"
- Romance online com pedidos de dinheiro

⚠ REGRA DE OURO

O seu banco **NUNCA** pede códigos, palavras-passe ou dados do cartão.

👉 **Quem pede, é burla. Sempre.**

⚠ **ATENÇÃO:** O seu banco **NUNCA** pede códigos, palavras-passe ou dados do cartão por telefone, SMS ou email!

AS 3 REGRAS DE OURO DA SEGURANÇA ONLINE



DESCONFIE

De contactos inesperados que pedem dados ou dinheiro



PARE

Antes de clicar em links ou fazer pagamentos



CONFIRME

Sempre através do número oficial da entidade



CRIE PALAVRAS-PASSE FORTES

Uma boa palavra-passe é como uma frase secreta.

Exemplo:

"OCaoDoVizinhoCorre3Km!"

✓ Longa ✓ Maiúsculas ✓ Números ✓ Símbolos

Outras dicas importantes:

- Uma palavra-passe diferente para cada site
- Nunca use datas de nascimento ou nomes
- Mude a password se suspeitar de fraude
- Ative a verificação em dois passos (2FA)



SE FOI VÍTIMA DE BURLA

1. Contacte o seu banco imediatamente

Peça o cancelamento de cartões ou transferências.

2. Apresente queixa

PSP, GNR ou Ministério Público.

3. Guarde todas as provas

SMS, emails, comprovativos e números de telefone.

4. Altere as passwords

De todas as contas que possam estar em risco.



Não tenha vergonha. Pode acontecer a qualquer pessoa.



CONTACTOS ÚTEIS



Linha Internet Segura

800 21 90 90

Gratuita • Confidencial



Autoridades

PSP/GNR: 112

Polícia Judiciária: 211 967 000



CNCS

cert@cert.pt

Centro Nacional de Cibersegurança



LEMBRE-SE

Na dúvida:

não clique • não pague • não responda.



Pare e peça ajuda.

Informação do projeto “Envelhecimento Ativo e Saudável em Barcelos”, submetido ao Aviso NORTE2030-2024-6 | Planos de Ação Intermunicipais para a Inclusão Ativa de Grupos Vulneráveis (ITI):

www.cm-barcelos.pt/projeto-envelhecimento-ativo-e-saudavel