Setronix desde 1966

OUTUBRO 2026

2.ª QUINZENA | PREVENÇÃO



CIBERSEGURANÇA
PARE E CONFIRME

Uma mensagem urgente não dispensa a verificação.

1. Perigos e riscos

Perigos: Mensagens falsas, anexos e ligações suspeitas.

Riscos: Roubo de dados, fraude e acesso indevido a contas.

2. Antes de começar

- Veja o endereço completo do remetente.
- Confirme pedidos por um contacto já conhecido.
- Use apenas aplicações e canais autorizados.

3. Pare e comunique

- Pedido de palavra-passe ou código de acesso.
- Urgência, segredo ou alteração de dados bancários.
- Já clicou ou enviou dados? Comunique de imediato.

4. Como atuar: quatro passos para prevenir

1 

Leia
Verifique remetente e contexto.

2 

Confirme
Use um contacto independente.

3 

Proteja
Não partilhe credenciais ou códigos.

4 

Comunique
Reporte pelo canal interno aplicável.

5. Escolha a medida adequada à situação

Situação	Medida preventiva
Email / SMS	Não abra anexos nem ligações cuja origem não confirmou.
Pedidos de pagamento	Valide alterações por outro canal já conhecido.
Contas / credenciais	Use palavras-passe únicas; ative MFA quando disponível.
Possível incidente	Guarde a mensagem; siga as instruções de apoio técnico.

Boas práticas: Não confie apenas no nome apresentado ou na aparência da mensagem. A autenticação multifator (MFA) reforça a proteção; nunca partilhe os respetivos códigos.

6. AÇÃO DA QUINZENA Na próxima mensagem inesperada, confirme a origem antes de clicar. Identifique o canal interno para comunicar uma suspeita.

LEIA • CONFIRME • PROTEJA • COMUNIQUE

CNCS: boas práticas CNCS: palavras-passe