

GUIA ANTI-BURLAS DIGITAL

EDIÇÃO PORTUGAL • 2026

Aprende a reconhecer mensagens falsas, proteger as tuas contas e reagir rapidamente a uma tentativa de fraude.

INFORMAÇÃO PRÁTICA. SEM COMPLICAÇÕES.

COMEÇA POR AQUI

Uma regra protege-te de muitas burlas

Antes de clicar, pagar, responder ou partilhar um código: pára e confirma por um canal independente.

- **1. Desconfia da urgência**

Mensagens que exigem pagamentos imediatos, ameaçam bloquear contas ou anunciam prémios inesperados merecem verificação.

- **2. Não uses o link recebido**

Abre diretamente a aplicação oficial ou escreve o endereço da entidade no navegador.

- **3. Confirma quem está a falar**

Um contacto conhecido pode ter sido comprometido. Telefona para um número que já guardaste.

- **4. Nunca partilhes códigos**

Códigos de SMS, autenticação e recuperação de conta destinam-se apenas a ti.

CINCO ESQUEMAS FREQUENTES

Reconhece os sinais

- **Falsas entregas**

SMS com uma taxa ou morada por confirmar. Confirma a encomenda no site ou app oficial da transportadora.

- **Falso apoio técnico**

Alguém pede acesso remoto ao dispositivo ou credenciais. Não instales ferramentas a pedido de contactos inesperados.

- **WhatsApp de um familiar**

Uma mensagem pede dinheiro com urgência. Contacta a pessoa pelo número habitual antes de pagar.

- **Falsos bancos e pagamentos**

Páginas e chamadas tentam recolher códigos, dados ou confirmar operações. Liga para o número oficial do banco.

- **Investimento garantido**

Promessas de rendimentos extraordinários e sem risco devem ser tratadas como sinais de alerta.

PROTEGE AS CONTAS

Checklist de segurança

- **Palavras-passe diferentes**

Usa uma palavra-passe longa e única por serviço. Considera um gestor de palavras-passe.

- **Autenticação de dois fatores**

Ativa sempre que possível, preferindo aplicações de autenticação ou chaves de segurança.

- **Atualizações em dia**

Mantém telemóvel, computador, browser e aplicações atualizados.

- **Avisos de sessão**

Ativa alertas de novos inícios de sessão e revê regularmente dispositivos ligados.

- **Privacidade e cópias**

Partilha o mínimo de dados pessoais e mantém cópias de segurança dos ficheiros essenciais.

SE JÁ FOSTE ENGANADO

Age por esta ordem

- **1. Interrompe a interação**

Deixa de responder. Não instales aplicações nem faças novos pagamentos.

- **2. Protege o acesso**

Se partilhaste credenciais, altera-as através do serviço oficial e termina sessões desconhecidas.

- **3. Contacta o banco**

Se houve pagamento ou dados bancários expostos, contacta imediatamente o banco pelos canais oficiais.

- **4. Guarda evidências**

Conserva capturas de ecrã, números, links, datas e comprovativos de transferências.

- **5. Participa e pede ajuda**

Comunica às autoridades competentes e, quando aplicável, reporta o incidente à plataforma.

CASOS PRÁTICOS

Exemplos de resposta segura

- **"A tua encomenda ficou retida. Paga 1,95 €."**

Não abras o link. Consulta a encomenda na app da transportadora e confirma se existe alguma pendência.

- **"Sou o teu filho. Mudei de número. Preciso de 300 €."**

Liga para o número antigo ou fala pessoalmente com a pessoa. Não transfiras dinheiro sem confirmar.

- **"Envia-me o código que recebeste por SMS."**

Nunca envies o código. Abre a aplicação oficial e verifica se houve tentativas de acesso.

- **"A tua conta do banco está bloqueada. Clica aqui."**

Abre a app do banco manualmente ou contacta o apoio através do número oficial.

RECURSOS E PRÓXIMOS PASSOS

Mantém-te informado

Consulta entidades oficiais e os canais de apoio da tua instituição bancária, da transportadora ou do serviço afetado.

- **Centro Nacional de Cibersegurança**

www.cncs.gov.pt

- **Banco de Portugal**

www.bportugal.pt

- **Polícia Judiciária**

www.policiajudiciaria.pt

Continua a aprender connosco

Segue @minutodigital.pt para dicas práticas de tecnologia, inteligência artificial e segurança digital para Portugal.

Partilha este guia com quem mais precise.

Conteúdo educativo geral. Em caso de prejuízo ou crime, procura ajuda junto das autoridades e entidades competentes.