

Checklist de prevenção a golpes

Leia com calma, marque o que já está combinado e guarde em local visível.

Antes de agir, pare.

Pressa, medo, pedido de sigilo ou promessa de solução imediata são sinais para encerrar o contato e confirmar por um canal oficial.

Na ligação ou mensagem

- ☐ Não informe senhas, códigos de autenticação, dados do cartão ou dados bancários.
- ☐ Não clique em links, não instale aplicativos e não siga comandos recebidos no contato suspeito.
- ☐ Não entregue cartão, documento, dinheiro ou aparelho a alguém enviado por telefone.
- ☐ Desligue quando a conversa criar urgência, medo ou pedir segredo.
- ☐ Converse com uma pessoa de confiança antes de tomar decisão que envolva dinheiro ou dados.

Confirme com segurança

- ❑ Abra o aplicativo oficial ou use o telefone do verso do cartão para falar com o banco.
- ❑ Digite você mesmo o endereço do site oficial; não use links enviados por mensagem.
- ❑ Confirme pedidos urgentes de familiares por outro canal que você já conhece.
- ❑ Ative a verificação em duas etapas quando o aplicativo oferecer essa opção.
- ❑ Guarde números oficiais e combine, em família, uma pausa para confirmar pedidos inesperados.

Se você já suspeita que caiu em um golpe

1. Encerre o contato.
2. Procure imediatamente o banco ou serviço pelos canais oficiais.
3. Siga a orientação de bloqueio e troca de credenciais, se aplicável.
4. Confira movimentações e registre BO no canal da Polícia Civil do seu estado, quando necessário.

Importante Nunca envie este checklist com dados pessoais preenchidos. Ele não substitui atendimento bancário, policial ou jurídico. Em risco imediato, procure os canais oficiais de emergência e segurança pública.

Fontes consultadas: Ministério da Justiça e Segurança Pública — “Falsa Central/Falso Funcionário”; Banco Central do Brasil — BC Protege+; CERT.br — Cartilha de Segurança para Internet. Atualizado em 28 ago. 2026.