

Dicas Essenciais para Prevenção de Fraudes

Mantenha a calma e desconfie de pedidos urgentes:

Golpistas frequentemente criam um senso de urgência para pressionar as vítimas a agir rapidamente.

Se receber pedidos de dinheiro para emergências, acidentes ou fianças, não ceda ao impulso.

Verifique a identidade da chamada:

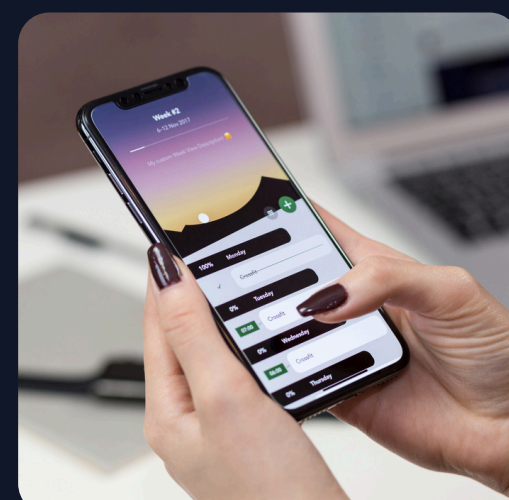
Esta é uma etapa crucial na sua cibersegurança.

Preste atenção aos detalhes da voz:

A IA pode replicar vozes, mas nuances ou sotaques incomuns podem ser um sinal de alerta.

Não forneça informações pessoais ou financeiras:

Nunca compartilhe senhas, números de cartão de crédito, dados bancários, números de segurança social ou outras informações confidenciais por telefone, especialmente em chamadas fraudulentas não solicitadas.



Ligue de volta:

Desligue a chamada suspeita e ligue diretamente para o familiar usando o número de telefone que você já conhece e salvou. Não utilize o número que ligou para si.

Chamada de vídeo:

Se possível, solicite uma videochamada para confirmar a identidade da pessoa.

Confirme por outro meio:

Envie uma mensagem de texto para o familiar ou entre em contato com outra pessoa próxima para verificar se a situação é real.



Proteja as suas informações online:

Nunca compartilhe senhas, números de cartão de crédito, dados bancários, números de segurança social ou outras informações confidenciais por telefone, especialmente em chamadas não solicitadas. Use senhas complexas e ative a autenticação de dois fatores em todas as suas contas. Isso adiciona uma camada extra de segurança e dificulta o acesso de criminosos, mesmo que consigam suas senhas. Evite compartilhar informações pessoais excessivas em redes sociais ou outros locais públicos.

Bloqueie chamadas indesejadas:

Utilize as ferramentas disponíveis no seu telefone ou aplicativos para bloquear números suspeitos ou indesejados.

O Que Fazer se For Vítima?

Se, infelizmente, for vítima, aja rapidamente:

- Denuncie imediatamente, às autoridades: PSP ou GNR.
- À instituição financeira: Se houve perda financeira, entre em contato com seu banco ou instituição financeira imediatamente para tentar bloquear transações e contestar pagamentos.
- À plataforma: Se o golpe ocorreu por meio de uma plataforma (WhatsApp, redes sociais), denuncie o contato ou perfil para a plataforma.
- Altere senhas: Mude as senhas de todas as contas comprometidas, utilizando senhas fortes e únicas.

- Monitore suas contas:

Fique atento a atividades suspeitas nas suas contas bancárias e digitais.

A Inteligência Artificial pode trazer muitos benefícios, mas também desafios.

Estar atento e tomar precauções é fundamental para se proteger contra essas novas formas de golpe.

Lembre-se:

estamos à espera daquele e-mail/contato/SMS?

E esse contato vem do endereço correto?

Mantenha a sua consciência digital em alta!

Se precisar de Assistência Técnica estamos aqui para o ajudar.