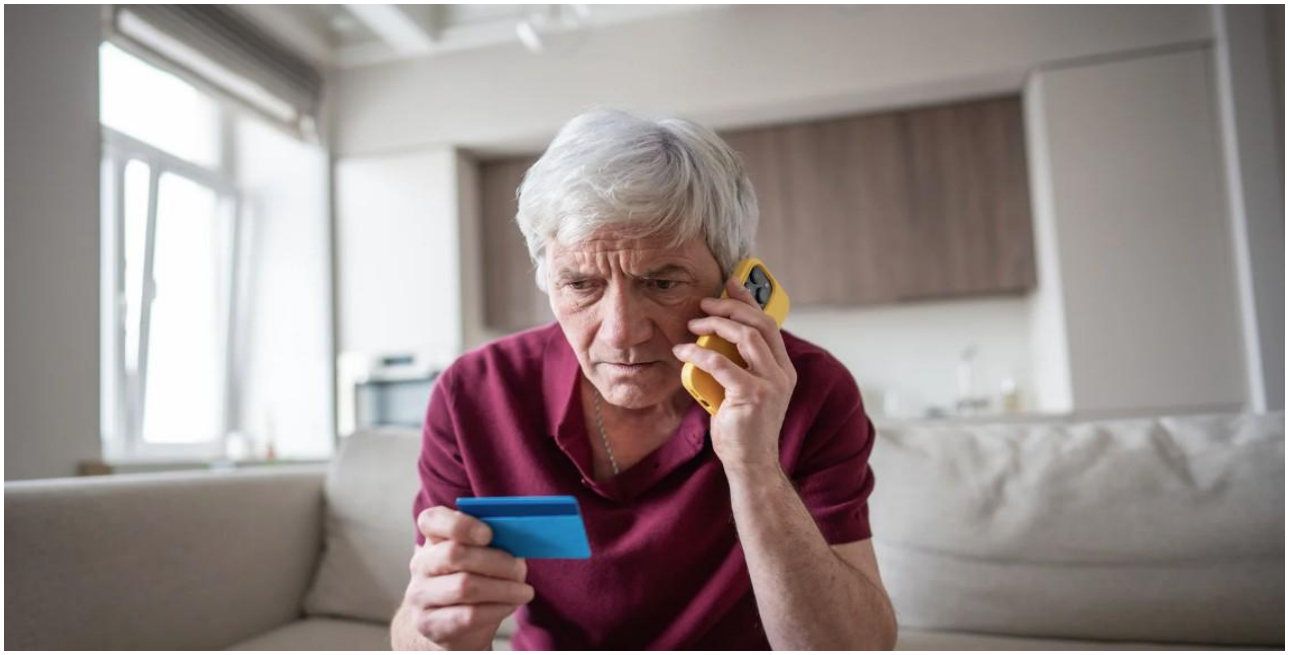
BOLETIM DE SEGURANÇA DA INFORMAÇÃO # 2

COMO SE PROTEGER DE FRAUDES E GOLPES ONLINE



As fraudes online estão cada vez mais sofisticadas. Golpistas utilizam **emails, mensagens no WhatsApp, SMS e até ligações telefônicas** com aparência muito profissional para enganar pessoas e obter informações pessoais[1].

Essas mensagens geralmente parecem reais porque usam **dados pessoais verdadeiros**, obtidos a partir de vazamentos: nome completo, endereço, compras recentes, hábitos de consumo, documentos e até informações sobre familiares. Isso aumenta a sensação de confiança — e é exatamente aí que mora o perigo.

Os golpistas tentam convencer a vítima a **clicar em links**, **instalar aplicativos falsos**, **compartilhar códigos de segurança**, ou até **informar senhas**. Ao fazer isso, a pessoa pode entregar acesso total ao seu celular, ao seu email ou à sua conta bancária. Por isso, o cuidado precisa ser redobrado.

Na dúvida, **não clique**, **não responda** e **não instale nada** sem ter absoluta certeza da origem.
Um simples descuido pode causar sérios prejuízos, tanto pessoais quanto profissionais.

[1] ESSE TIPO DE GOLPE É CONHECIDO COMO **PHISHING,** EXPRESSÃO QUE VEM DO INGLÊS *FISHING* ('PESCAR'): O GOLPISTA LANÇA UMA ISCA PARA CAPTURAR SEUS DADOS

CASO REAL: LIGAÇÃO FALSA DA LOJA

Um exemplo muito comum aconteceu com um senhor que vamos chamar aqui de **seu João**.

Ele recebeu uma ligação dizendo que havia um crediário aprovado para compra de uma televisão. O atendente sabia todas as suas informações: nome completo, RG, endereço, CPF e até detalhes de uma compra recente que ele tinha feito em outra loja. Tudo parecia legítimo.

Seu João disse que não havia comprado televisão nenhuma. O atendente então afirmou que poderia ser um golpe e, "para ajudar", enviou um **link para instalar um aplicativo de segurança** no celular. Confiando na conversa, ele instalou o aplicativo.

O aplicativo, no entanto, era um **vírus**. Assim que seu João digitou sua senha do banco, o programa capturou os dados e os golpistas fizeram uma transferência via PIX de **R$ 5.400,00**. Quando ele percebeu o golpe, o celular já estava travado e o dinheiro havia sido levado.

Esse caso mostra como as fraudes atuais usam **dados pessoais verdadeiros** para parecer confiáveis. Por isso, é fundamental desconfiar sempre.

RECOMENDAÇÕES PRÁTICAS DE PROTEÇÃO

✓ DESCONFIE DE MENSAGENS QUE PEDEM PARA CLICAR EM LINKS, INSTALAR APLICATIVOS OU COMPARTILHAR CÓDIGOS.

Golpes geralmente começam assim.

✓ VERIFIQUE SEMPRE O REMETENTE DO EMAIL E O NÚMERO DE TELEFONE.

Pequenas alterações podem indicar fraude.

✓ NUNCA INSTALE APLICATIVOS ENVIADOS POR DESCONHECIDOS.

Bancos e empresas **não enviam aplicativos por link**.

✓ NUNCA COMPARTILHE CÓDIGOS DE SEGURANÇA, ESPECIALMENTE CÓDIGOS ENVIADOS POR SMS.

Eles dão acesso direto à sua conta.

✓ NÃO INFORME SENHAS POR TELEFONE, WHATSAPP OU EMAIL.

Instituições sérias jamais pedem isso.

✓ ACESSE BANCOS E SERVIÇOS APENAS PELOS SITES E APLICATIVOS OFICIAIS.

Evite clicar em links recebidos.

✓ NA DÚVIDA, PARE E PERGUNTE.

Converse com alguém da sua equipe, do seu setor ou com o encarregado de dados.

✓ USE APENAS COMPUTADORES E REDES CONFIÁVEIS PARA OPERAÇÕES FINANCEIRAS.

Wi-Fi público pode expor seus dados.

LINK PARA O VÍDEO

https://vimeo.com/1145601073

Golpes
Como se proteger de fraudes e golpes