VIDA DIGITAL

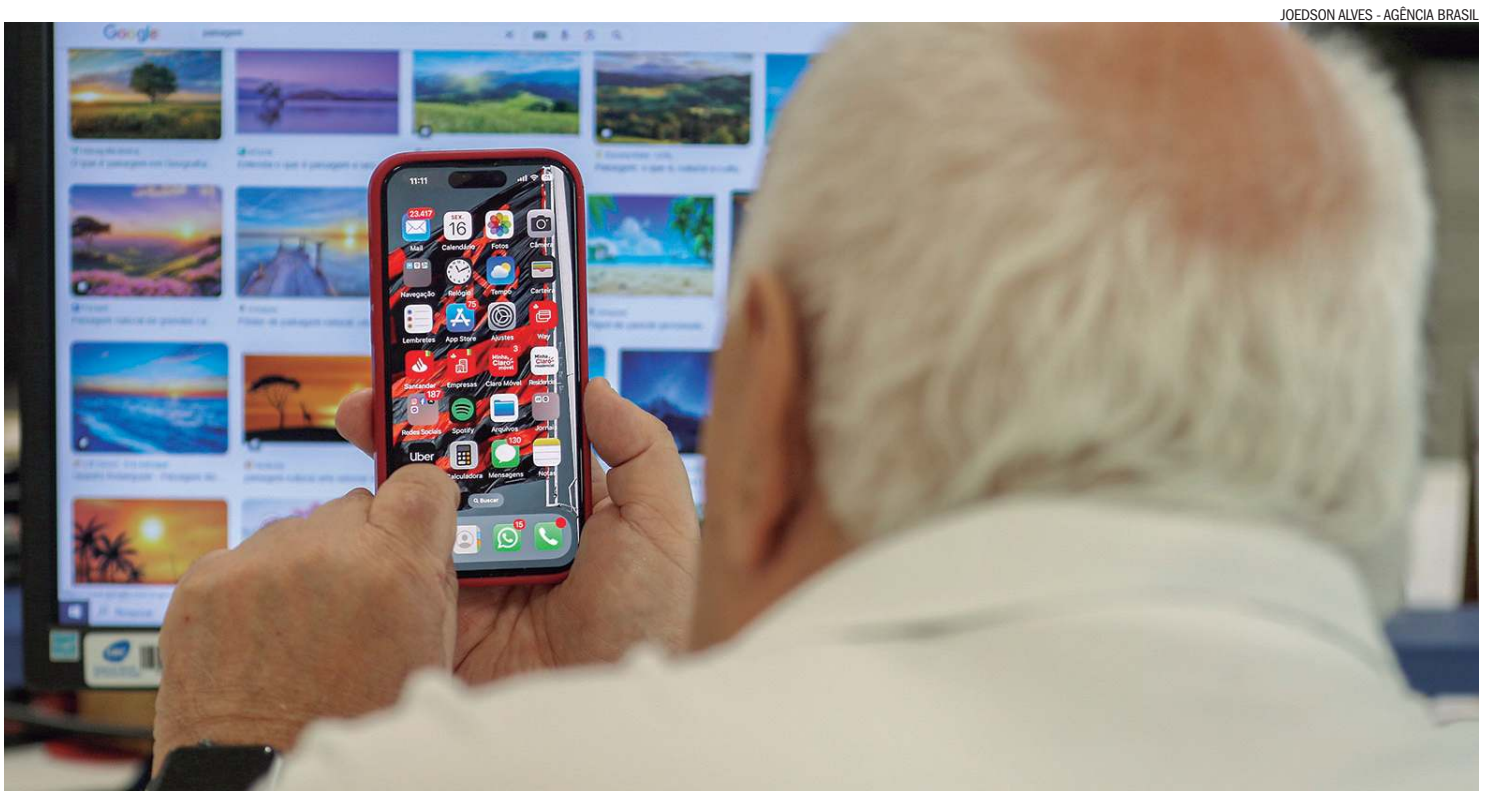
CRIMES VIRTUAIS

Um em cada quatro brasileiros já foi alvo de golpe cibernético

Dados são de pesquisa realizada pelo Instituto DataSenado; especialista aponta cuidados para o uso de tecnologia

DA REDAÇÃO

JOEDSON ALVES - AGÊNCIA BRASIL



Idoso usa o celular e o computador ao mesmo tempo: pesquisa revela que brasileiros de diferentes perfis etários e sociais já foram vítimas de golpes

Clonagem de cartões, invasão de contas em redes sociais, fraudes na Internet ou desvio em contas bancárias. Cerca de 24% da população brasileira - o equivalente a uma em cada quatro pessoas - já foi vítima de golpes cibernéticos. Os dados são de uma pesquisa realizada pelo Instituto DataSenado.

Com distribuição praticamente uniforme entre os estados brasileiros, apenas dois deles têm um percentual abaixo de 20%: Piauí (18%) e Ceará).

O instituto investigou variáveis como tamanho do município, situação de domicílio (se urbano ou rural), religião, situação no mercado de trabalho, renda, escolaridade, faixa etária, sexo, cor e raça.

Os resultados mostram a ausência de um perfil claro de alvos dos bandidos, já que as respostas positivas para golpes tentados ou consumados vieram em proporção semelhante às características socioeconômicas da população brasileira

É o que revela o caso de um professor universitário de Ribeirão Preto, no interior de São Paulo, vítima do chamado "golpe do pix" dentro de uma agência bancária da cidade. Ele recebeu a ligação de um golpista, supostamente o alertando sobre transações suspeitas em sua conta. Acreditando estar no telefone com um funcionário da instituição financeira, ele fez transações bancárias e empréstimos pelo caixa eletrônico, além de transferências via PIX.

Para o especialista em segurança estratégica e perícia Sandro Christovam Bearare, o uso cada vez mais frequente do celular facilitou a atuação de criminosos especializados nesse tipo de fraude.

"Existem grupos que atuam de forma organizada, utilizando roteiros profissionais e técnicas de engenharia social para convencer até pessoas com mais instrução de que são agentes legítimos de grandes empresas ou instituições financeiras. O celular é hoje uma extensão do corpo das pessoas — praticamente todo mundo tem e faz uso o dia todo. Mais do que criar uma cultura de segurança digital, é fundamental haver maior publicidade sobre esses problemas, além de instruir amigos e familiares para que estejam atentos e saibam se proteger", explica Sandro Bearare.

DICAS DE SEGURANÇA DIGITAL

O perito em segurança aponta cuidados tecnológicos e comportamentais que podem reduzir a chance de sucesso dos golpistas. Confira:

DESCONFIE DE LINKS RECEBIDOS POR MENSAGENS

Receber link por SMS, WhatsApp, e-mail ou rede social já virou rotina. Mas tem muito golpe por trás disso. Golpista manda link falso pra te jogar numa página clonada e capturar seus dados. Regra simples: se você não pediu, não clique. Confirme antes com a pessoa ou empresa.

ATIVE A AUTENTICAÇÃO EM DOIS FATORES (2FA)

Essa é uma camada extra de segurança que faz diferença. Mesmo que o criminoso descubra sua senha, sem o segundo código (geralmente no seu celular), ele não entra. Use isso em tudo: e-mail, redes sociais, banco, aplicativos... segurança reforçada nunca é demais.

MANTENHA SEU CELULAR E COMPUTADOR ATUALIZADOS

Muita gente ignora as atualizações, mas elas corrigem falhas de segurança. Se você adia, fica vulnerável. Golpista vive de brecha, e essas atualizações tapam essas portas abertas. Não deixe pra depois — atualizou, protegeu.

CUIDADO COM E-MAILS DE PROMOÇÕES OU COBRANÇAS URGENTES

Sabe aquele e-mail "imperdível" ou "urgente" que parece bom demais ou assustador? Respira. O golpe é justamente te fazer agir no impulso. Sempre verifique o remetente e acesse o site digitando o endereço manualmente, sem clicar direto no link.

INSTALE ANTIVÍRUS CONFIÁVEL E MANTENHA-O ATIVO

Hoje em dia, não dá para andar sem antivírus. Ele é quem vai bloquear programas espiões e alertar sobre sites perigosos. Escolha um de confiança, mantenha atualizado e não desative por conveniência. É sua linha de frente contra ameaças digitais.

VERIFIQUE O ENDEREÇO DO SITE ANTES DE COMPRAR ONLINE

Na pressa, não reparamos, mas tem muito site falso que imita os originais trocando um caractere ou mudando a terminação. Veja se tem HTTPS e cadeado, e confira se o endereço é o correto mesmo. Um detalhe pode te salvar de uma baita dor de cabeça.

DESATIVE O BLUETOOTH E A LOCALIZAÇÃO QUANDO NÃO ESTIVER USANDO

Deixar essas funções ligadas o tempo todo é convite para encrenca. Hackers podem explorar essas portas abertas pra rastrear, acessar arquivos ou invadir seu aparelho. Se não tá usando, desliga. Simples assim.

REVISE AS PERMISSÕES DOS APPS NO SEU CELULAR

Tem aplicativo pedindo acesso à câmera, microfone, localização... e você nem percebe. Dê uma revisada nas permissões, nas configurações e limite o que não for essencial. Não faz sentido um jogo querer acessar seus contatos, por exemplo.

DESCONFIE DE LIGAÇÕES DIZENDO QUE SEU CARTÃO FOI CLONADO

Esse é um clássico! A pessoa liga dizendo que é do banco, que seu cartão foi clonado e que você precisa passar dados ou entregar o cartão pro motoboy. Não caia. Desligue e ligue pro número oficial do banco. Nunca passe nada por telefone.

EVITE ACESSAR CONTAS BANCÁRIAS EM WI-FI PÚBLICO

Wi-Fi grátis em café, aeroporto, hotel? Pode parecer prático, mas é uma armadilha perfeita para aqueles que querem interceptar seus dados. Nada de acessar banco ou fazer compras em rede aberta. Se for urgente, use 4G ou VPN.

EVITE EXPOR DADOS PESSOAIS NAS REDES SOCIAIS

Tem gente que compartilha CPF, RG, nome da mãe, endereço... achando que não dá em nada. Só que golpista junta essas informações e monta um perfil seu pra aplicar golpes mais elaborados. Expor demais é facilitar a vida dos bandidos.

USE CARTÃO VIRTUAL PARA COMPRAS ONLINE

É uma opção mais segura que o cartão físico. Se alguém pegar os dados, não consegue usar depois. Muitos bancos já oferecem isso no app. Crie, use e delete. É prático e muito mais seguro.

CONFIGURE ALERTAS NO APLICATIVO DO BANCO

Ative notificações de transações por SMS ou push. Assim, se alguém tentar movimentar sua conta, você sabe na hora. Qualquer coisa suspeita, já corre pra bloquear e evitar prejuízo.