CRIMES DIGITAIS: Pharming, Smishing e Phishing, como evitar?

O Brasil se consolidou como o maior alvo de ciberataques da América Latina, registrando mais de 500 mil ocorrências somente no primeiro semestre de 2025, segundo levantamento da Check Point Research. O dado reflete uma realidade preocupante: ataques digitais se tornaram rotina no país, afetando tanto usuários comuns quanto empresas de diferentes portes.

Ataques como pharming, smishing e phishing estão entre as ameaças digitais que mais crescem no mundo, explorando vulnerabilidades humanas e técnicas para roubar dados, credenciais e até dinheiro. Apesar de cada vez mais frequentes, muitos usuários ainda desconhecem como funcionam e quais medidas adotar para se proteger, o que aumenta o risco de perda de dados, credenciais e até dinheiro.

Para Daniel Tieppo, especialista em cibersegurança e Diretor Executivo da HexaDigital, a prevenção é a principal arma contra esse tipo de ameaça. “Esses golpes exploram a confiança e a desatenção das pessoas. Por isso, o primeiro passo é entender como funcionam para evitar cair em armadilhas digitais. Além disso, empresas precisam fortalecer processos internos e adotar tecnologias de monitoramento e proteção em tempo real”, explica o executivo.

Pharming: o golpe invisível que troca seu destino online

O pharming redireciona o usuário, de forma invisível, para sites falsos mesmo quando o endereço correto é digitado. Isso pode ocorrer por falhas em servidores DNS ou por malware instalado no dispositivo da vítima.

“No caso do pharming, a atenção deve estar em três pontos: digitar manualmente o endereço de sites sensíveis, desconfiar de mudanças sutis na aparência das páginas e manter sempre os sistemas e antivírus atualizados. Esses cuidados reduzem bastante o risco de cair nesse tipo de armadilha”, orienta Tieppo.

Smishing: quando um simples SMS vira armadilha

O smishing é um golpe via SMS, em que mensagens falsas induzem a vítima a clicar em links maliciosos ou compartilhar informações pessoais. Normalmente, se passam por bancos, operadoras ou serviços de entrega.

“Nunca clique em links recebidos por SMS se você não solicitou aquele contato. Além disso, não compartilhe senhas ou códigos por mensagem e ative filtros de spam no celular. Esse simples hábito já evita grande parte das tentativas de fraude via smishing”, alerta o especialista.

Phishing: a isca digital mais comum da internet

O phishing é a forma mais comum de ataque digital. Utiliza e-mails, redes sociais ou aplicativos de mensagens para se passar por instituições confiáveis, induzindo a vítima a fornecer dados sigilosos, como logins, senhas e números de cartão.

“A dica principal contra o phishing é sempre checar o remetente antes de clicar em links ou abrir anexos. Também recomendo habilitar a autenticação em dois fatores e participar de treinamentos de conscientização digital, especialmente em ambientes corporativos. A informação continua sendo a melhor defesa contra esse tipo de golpe”, reforça o Diretor Executivo da HexaDigital.

Tieppo ressalta que o combate a esses crimes é uma responsabilidade compartilhada. “O usuário precisa adotar hábitos digitais mais seguros, enquanto empresas devem investir em políticas de conscientização e tecnologias de defesa. A combinação de educação e prevenção é a melhor estratégia contra golpes online”, conclui.

Foto: Divulgação