ENTREVISTA — JOSÉ ROBERTO RUIZ, advogado especialista em direito digital

Saiba quais são os crimes mais comuns na internet e como agir

Ana Maria Campos

Os crimes digitais estão cada vez mais sofisticados e afetam milhões de pessoas em todo o mundo. Pesquisa do Datafolha mostrou que, nos últimos 15 meses, cerca de 33,4% dos brasileiros sofreram algum tipo de golpe virtual com prejuízo financeiro. O advogado José Roberto Ruiz, especialista em direito digital, explica quais são os cuidados para evitar golpes e os direitos de quem teve problemas na internet.

Divulgação

"Decisões judiciais têm determinado que bancos e instituições financeiras indenizem o consumidor, quando comprovada falha na segurança ou ausência de mecanismos eficazes de bloqueio"

Os crimes digitais estão cada vez mais sofisticados e ligados a operações corriqueiras do dia a dia. Quais são os cinco mais comuns?

Hoje, os golpes mais recorrentes envolvem engenharia social e exploração da confiança das vítimas. Entre os principais estão: Golpe do falso link ou phishing, em que o criminoso cria páginas idênticas às de bancos, lojas ou aplicativos para capturar senhas e dados pessoais; clonagem de WhatsApp, usada para pedir dinheiro a contatos da vítima; golpe do Pix, em que o golpista induz a vítima a transferir valores com urgência ou sob pretexto de erro de pagamento; golpes em marketplaces, envolvendo falsas vendas ou anúncios de produtos que não existem; roubo de dados em redes públicas de Wi-Fi, quando o usuário acessa contas bancárias ou preenche cadastros sem segurança.

Como a pessoa pode saber que está diante de um golpe se a maioria das transações hoje em dia são eletrônicas?

Existem sinais de alerta que devem ser observados. Mensagens com urgência, erros de português, links encurtados e promessas de ofertas irreais são indícios clássicos. Outro ponto é verificar se o endereço eletrônico começa com "https" e se há o cadeado de segurança. No caso de ligações, nenhum banco ou empresa confiável pede senhas, códigos ou transferências de valores por telefone.

Se alguém cair em um golpe, o que deve fazer imediatamente?

O primeiro passo é bloquear o meio de pagamento utilizado, principalmente contas bancárias e aplicativos. Em seguida, registrar um Boletim de Ocorrência detalhando todas as informações possíveis, inclusive, prints e comprovantes. Também é importante comunicar o banco ou a instituição financeira e registrar reclamação no Procon e no site *consumidor.gov.br*.

Quais órgãos ou instituições devem ser acionados?

A vítima deve procurar a Delegacia de Repressão a Crimes Cibernéticos, quando houver na região, ou uma delegacia comum, que encaminhará o caso à especializada. Além disso, é essencial registrar o caso junto ao banco, ao Procon, ao *consumidor.gov.br*, e, se envolver grandes plataformas, também junto às próprias empresas (como marketplaces ou redes sociais).

Existe alguma forma de recuperar o dinheiro perdido em transferências fraudulentas?

Em alguns casos, sim. O Banco Central instituiu o Mecanismo Especial de Devolução (MED), que permite o bloqueio e possível restituição de valores transferidos via Pix, desde que o golpe seja comunicado rapidamente. Além disso, decisões judiciais têm determinado que bancos e instituições financeiras indenizem o consumidor, quando comprovada falha na segurança ou ausência de mecanismos eficazes de bloqueio.

Quais erros as pessoas costumam cometer após perceber que foram enganadas?

O erro mais comum é não agir de imediato. Quanto mais tempo passa, menor a chance de rastrear o dinheiro. Outro equívoco é não registrar Boletim de Ocorrência, acreditando que o valor é pequeno, o que dificulta o rastreamento de grupos criminosos. Também é importante não apagar conversas ou prints, pois eles são provas fundamentais.

A própria tecnologia cria essa facilidade de ocorrência de crimes porque muitas vezes o consumidor não tem contato pessoal com as empresas. O que o consumidor pode exigir dos bancos e operadoras, por exemplo?

O consumidor pode e deve exigir mecanismos de segurança eficazes, como autenticação em dois fatores, confirmação por biometria e bloqueios temporários de transferências suspeitas. Também tem direito a informação clara e canal de atendimento rápido para contestar transações. O Código de Defesa do Consumidor garante a responsabilidade objetiva das instituições financeiras por falhas na prestação de serviço.

Se o consumidor recebe uma ligação com uma pessoa se passando por um funcionário de um banco, com a chamada de um telefone clonado, e acaba caindo no golpe, qual é o seu direito?

Mesmo que a ligação pareça autêntica, o banco tem dever de segurança. Se houver indício de clonagem, falha de autenticação ou ausência de travas que impediriam a transação, o consumidor pode exigir ressarcimento integral. A jurisprudência reconhece que a vítima não deve arcar com o prejuízo quando o golpe é consequência de falha sistêmica ou omissão do banco em prevenir fraudes previsíveis.

Como os tribunais têm decidido nesses casos?

O entendimento predominante é o de responsabilidade solidária entre bancos, intermediadores e plataformas. Os tribunais têm reforçado que as instituições financeiras devem adotar medidas proativas de segurança e indenizar o consumidor em caso de fraude que decorra de vulnerabilidade do sistema. O Superior Tribunal de Justiça já consolidou o entendimento de que, mesmo em fraudes praticadas por terceiros, há dever de indenizar quando há falha no serviço (Súmula 479 do STJ).