

A cibersegurança do indivíduo: ameaças, direitos e remédios

Ameaças, direitos e remédios para o consumidor

Como proteger o indivíduo no ambiente digital?

Proteger de quê? Quem tem o dever de proteger? O que fazer quando a proteção falha?



Cibersegurança é sobre pessoas

Organizações públicas e privadas têm programas de gestão de risco, equipes de resposta e política de conscientização de colaboradores. O usuário comum não tem nada disso. Na maioria das vezes, ela não sabe que está diante de uma ameaça digital e só descobre quando essa já se concretizou. Proteger o espaço digital é proteger o ser humano que o usa.

Como proteger o indivíduo no ambiente digital?

A pesquisa mapeou cinco grupos prioritários para políticas públicas

Três estão nomeados na Estratégia Nacional de Cibersegurança (Decreto nº 12.573/2025). Dois não estão, mas o direito brasileiro reconhece a sua vulnerabilidade por outras vias.

**Crianças e
adolescentes**

Pessoas idosas

**Pessoas
neurodivergentes**

Mulheres

Consumidores

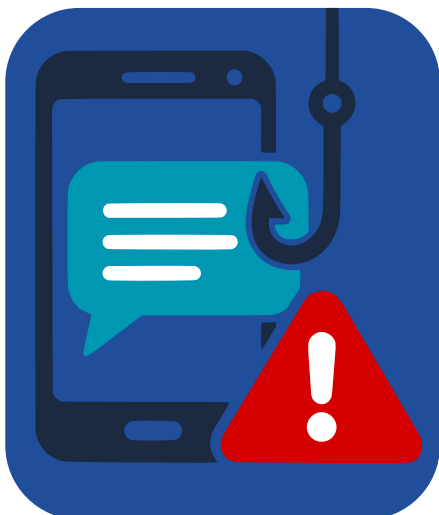
Todos nós, quando compramos, pagamos ou contratamos pela internet. A vulnerabilidade do consumidor é reconhecida desde 1990 (CDC, art. 4º, I), mas o consumidor não aparece na lista da Estratégia Nacional de Cibersegurança. Esta cartilha trata dele: é o grupo mais numeroso e o mais atingido pelas fraudes digitais.

Ameaças

Aqui estão algumas ciberameaças que oferecem perigo ao consumidor. Esse rol não é exaustivo.

1

Engenharia social



Sinal de alerta. O banco nunca liga pedindo que você transfira dinheiro, instale um programa ou informe senha.

O que é?

O criminoso manipula a confiança, a pressa ou o medo para que você mesmo entregue a senha, instale um programa ou faça a transferência.

Como aparece?

Phishing (e-mail ou site falso), smishing (SMS) e vishing (ligações). A forma mais comum no Brasil é a falsa central.

Por que ficou mais perigosa?

A mensagem não tem mais erro de português, a voz pode ser clonada e a ligação pode ser indistinguível da do banco, com o uso de IA

2

Uso indevido da sua identidade ou das suas senhas



O que é?

Alguém, de posse dos seus dados ou das suas credenciais faz operações em seu nome sem que você participe.

Como aparece?

Roubo de credenciais, clonagem de contas e falsidade de identidade

De onde vêm os dados?

De vazamentos, de programas maliciosos ou de uma engenharia social anterior. Por isso esta ameaça costuma ser o desfecho de outra.

3

Controle do seu celular ou computador



Sinal de alerta. Nenhuma instituição pede para instalar aplicativo de acesso remoto (AnyDesk, TeamViewer e similares) para resolver um problema de segurança.

O que é?

Um programa malicioso ou um aplicativo de acesso remoto permite que o criminoso controle o seu aparelho à distância.

Como aparece?

No golpe da mão fantasma, alguém liga dizendo ser técnico do banco, alerta sobre uma invasão e convence você a instalar um aplicativo de suporte. A partir daí, o criminoso opera o aplicativo do banco, faz transferências, contrata empréstimos e troca senhas.

4

Falha de segurança da empresa

**O que é?**

Aqui a ameaça não parte de uma abordagem a você. Parte do sistema da empresa que guarda os seus dados ou do produto que você usa. Um vazamento expõe seus dados.

Por que importa?

É a única das quatro em que a origem está na omissão do fornecedor, e não só no criminoso. Os dados bancários que o golpista usa na falsa central vieram de algum lugar.

As ameaças se encadeiam

ELO 1
O vazamento
expõe seus
dados

ELO 2
A engenharia
social usa os
dados para
convencer você

ELO 3
Você entrega a
senha ou instala
o programa

ELO 4
A operação é
feita sem você

Em cada elo há um responsável diferente.

Quem realizou a operação?

No caso de fraudes bancárias, é importante identificar como o golpe aconteceu. Existem duas situações:

Operação sem a sua participação

Alguém usou suas senhas ou seus dados e você não fez nada. É o que pode acontecer na invasão de contas, na contratação fraudulenta de empréstimos e em compras não autorizadas com cartão de crédito.

O banco, em regra, pode responder pelo prejuízo decorrentes de fraudes relacionadas aos riscos de sua atividade.

É a Súmula 479 do STJ. O banco pode, porém, afastar sua responsabilidade se demonstrar a existência de culpa exclusiva do consumidor ou de terceiro.

Operação realizada por você, enganado

A responsabilidade do banco dependerá das circunstâncias do golpe e da existência de falhas na prestação do serviço.

Entre alguns aspectos considerados, pode-se citar:

- 1 Uso indevido de dados: o golpista utilizou informações bancárias sigilosas obtidas em razão de falha de segurança?
- 2 Transações suspeitas: a operação era incompatível com seu perfil habitual e deveria ter despertado mecanismos de prevenção?
- 3 Segurança do serviço: ajuda a determinar se houve falha na prestação do serviço se a instituição financeira deve reparar os prejuízos.

A análise desses fatores ajuda a determinar se houve falha na prestação do serviço e se a instituição financeira deve reparar o prejuízo.

Em resumo

Cada situação precisa ser analisada considerando a forma como a fraude ocorreu e a segurança oferecida pela instituição. Por isso, adotar medidas de prevenção é fundamental.

Quem tem o dever de proteger?



As empresas

Segurança do serviço

As empresas devem garantir a segurança que o consumidor pode legitimamente esperar de seus produtos e serviços. Quando uma falha de segurança causa prejuízos, o fornecedor por ser responsabilizado.

Proteger dados pessoais

Quem trata dados pessoais deve adotar medidas de segurança desde a concepção do produto (LGPD, art. 46) e comunicar incidentes à ANPD e a você em três dias úteis (art. 48).

Prevenir fraudes no Pix

Contestação pelo aplicativo, bloqueio de valores suspeitos, rastreamento do dinheiro pelas contas por onde passou e compartilhamento dos indícios de fraude entre bancos (Regulamento do Pix; Res. BCB nº 493/2025; Res. Conjunta nº 6/2023).

Plataformas

Pelo que o STF decidiu em 2025, há presunção de responsabilidade por conteúdos ilícitos divulgados por anúncios pagos ou impulsionados, mesmo sem notificação prévia, mas a plataforma pode demonstrar que agiu com diligência necessária. Nas publicações fraudulentas comuns, a notificação pode fundamentar a responsabilização caso a plataforma deixa de agir. Aplica-se aos **marketplaces** o CDC.



O Estado

Fiscalizar e punir.

Procon e Senacon (CDC), ANPD (dados), Banco Central (bancos e Pix), Anatel (telefonia).

Investigar e processar.

Polícia e Ministério Público.

Conscientizar e combater fraudes.

Estratégia Nacional de Cibersegurança, art. 4º, X.

Aconteceu. E agora?

1 Conter o dano nas primeiras horas

Pix: conteste a transação no aplicativo do banco e solicite o Mecanismo Especial de Devolução (MED). Ele permite investigar a fraude e bloquear valores disponíveis na conta envolvida. **Cartão:** bloqueie e conteste a compra. **WhatsApp ou rede social:** use o canal oficial de recuperação, altere suas senhas e avise seus contatos. **Anúncio, perfil ou loja falsa:** denuncie na plataforma. **Registre o boletim de ocorrência:** registre a fraude reunindo comprovantes, conversas e informações do ocorrido.

2 Recuperar o dinheiro

Pelo MED, no Pix, se os valores foram bloqueados. Pelo cancelamento ou reembolso da compra junto ao cartão de crédito. Pela contestação do contrato eventualmente celebrado sem autorização do consumidor.

3 Indenização

Você tem direito à reparação dos danos materiais e morais (CDC, art. 6º, VI). Vale contra o seu banco, contra o banco que abriu a conta do golpista, mesmo que você não seja cliente dele (CDC, art. 17), e contra o marketplace ou intermediador, conforme o papel de cada um. Se a fraude usou dados vazados, a LGPD é um segundo fundamento (arts. 42 a 44).

4 Acionar os órgãos



SAC do
fornecedor ou da
plataforma



Banco Central.br
para reclamar de
banco ou do Pix



Procon/
Consumidor.gov



Juizado Especial
Cível ou Defensoria
Pública



ANPD, se envolver
dados pessoais

Quando a lesão atinge muita gente, o Ministério Público e a Defensoria podem propor ações coletivas.

A via penal

O registro de ocorrência ajuda a documentar a fraude e permite que as autoridades iniciem as providências cabíveis. Durante a investigação, a polícia poderá buscar os registros necessários à identificação dos responsáveis, observadas as exigências legais. No estelionato, a investigação, via de regra, depende da representação da vítima, isto é, da manifestação de sua vontade.

O que precisa mudar

Proteger o ser humano é redesenhar o sistema em volta dele. Cada ator tem a sua parte.

Governo

Incluir o consumidor expressamente na Estratégia Nacional de Cibersegurança. Criar uma estratégia nacional de conscientização, com nomenclatura única dos golpes, campanhas permanentes e avaliação de resultado, nos moldes do PNI e do combate ao tabagismo.

Publicar dados abertos sobre fraudes contra o consumidor.

Congresso

Prever no CDC o dever de segurança desde a concepção, para que a prevenção da fraude seja parte do projeto do serviço e não só uma consequência do dano.

Disciplinar a responsabilidade pela fraude de engenharia social em serviços de pagamento, com repartição clara entre o banco de origem, o banco de destino e o consumidor.

Justiça e órgãos de defesa

Aplicar de modo uniforme a distinção entre operação autorizada e não autorizada, com os critérios da origem dos dados, do perfil da operação e dos controles.

Procon e Senacon: fiscalizar o desenho dos serviços, e não só responder a reclamações.

Banco Central e ANPD: atuar em conjunto nos incidentes que ligam vazamento de dados a fraude.

Empresas

Bancos: alertas de risco antes de concluir a transferência, limites e tempo de espera para operações fora do perfil, canais de contestação simples.

Plataformas: verificação de anunciantes e perfis, resposta rápida à denúncia de loja ou perfil falso.

Telefonia: identificação da origem das chamadas, para que a falsa central não pareça o banco.

Todas: ensinar o consumidor sobre o golpe específico que atinge o seu serviço, com a mesma nomenclatura do governo.

Como proteger o ser humano?

Não é pedindo que ele não caia. É construindo serviços em que cair seja difícil, em que o dinheiro possa ser bloqueado em minutos, em que quem falhou responda, e em que a informação chegue a cada pessoa no formato que ela entende. A cibersegurança começa e termina em quem está do outro lado da tela.



Esta cartilha resume o policy paper **A cibersegurança do indivíduo: ameaças, direitos e remédios**, do Centro de Tecnologia e Sociedade da FGV Direito Rio. As referências legais e jurisprudenciais estão no documento completo.