

Cartão de crédito online

SETE DICAS PRÁTICAS PARA PROTEGER SEU CARTÃO

Especialista explica sobre riscos e medidas de proteção para realizar compras pela internet

Embora o Pix tenha se tornado o método de pagamento preferencial da maioria dos brasileiros (84%) que fazem compras online, o cartão de crédito continua sendo um meio importante para o consumo na internet, sendo utilizado por 67% dos consumidores do país, segundo a pesquisa TIC Domicílios, do Cetic.br. Contudo, junto a toda essa praticidade, tam-

bém traz uma série de riscos, como golpes, fraudes e clonagens de cartão. Entre 2023 e 2024, o volume de dinheiro perdido com golpes no Brasil aumentou 17%, saltando de R\$ 8,6 bilhões para R\$ 10,1 bilhões (dados Febraban).

“A popularização do comércio online exige que o consumidor esteja cada vez mais atento à segurança digital”,

diz Camila Poltronieri Flaquer, diretora de uma startup especializada em cobrança digital. “A maioria dos golpes acontece em momentos de distração ou por falta de medidas simples de proteção que fazem toda a diferença na hora da compra.”

A seguir, confira seis dicas para reforçar a segurança em compras online com cartão de crédito.



1 - COMPRE APENAS EM SITES CONFIÁVEIS

Desconfie de ofertas boas demais e verifique sempre se o site exibe o cadeado de segurança na barra de endereço e o prefixo https://. Além disso, procure por sinais adicionais de confiabilidade: dados de contato claros (endereço físico e telefone), política de trocas e devoluções explícita, CNPJ visível e selo de certificação quando houver (por exemplo, programas de segurança de grandes marketplaces). Consulte comentários recentes de outros consumidores em mais de uma fonte — não se limite apenas às avaliações exibidas pelo próprio site, pois estas podem ser moderadas. Pesquise no Reclame Aqui, redes sociais, fóruns e em grupos locais; leia as reclamações e veja se a empresa responde e resolve problemas.

Analise com atenção as políticas de privacidade e as condições de frete e prazos. Observe se o site fornece rastreamento do pedido e informação clara sobre garantia e assistência técnica. Outra alternativa é dar preferência a marketplaces consolidados (Amazon, Mercado Livre, grandes varejistas que você conheça), sempre comprando apenas de vendedores com boa reputação dentro dessas plataformas — verifique a nota do vendedor, percentual de entregas no prazo e número de vendas realizadas. Em compras internacionais, use lojas oficiais das marcas ou revendedores autorizados.

Dica prática: antes de finalizar a compra, pesquise o nome do site seguido de “fraude”, “reclame” ou “golpe” — se aparecerem muitos relatos negativos, procure outra loja.

2 - USE UMA REDE DE INTERNET SEGURA

Evite fazer compras usando Wi-Fi público (cafés, aeroportos, shoppings). Redes abertas permitem que invasores façam “sniffing” — interceptem dados transmitidos pelo seu aparelho. Priorize o uso de redes domésticas protegidas com senha forte (WPA2/WPA3). Se precisar usar uma rede pública, prefira conectar-se por dados móveis (4G/5G) do seu plano, que são mais seguras que redes Wi-Fi abertas.

Considere usar uma VPN (Rede Virtual Privada) ao efetuar compras — ela cria um túnel criptografado entre seu dispositivo e o servidor da VPN, dificultando que terceiros interceptem seu tráfego. Escolha provedores de VPN com boa reputação, sem logging (sem registro das atividades) e preferencialmente pagos — os serviços gratuitos frequentemente têm limitações e riscos.

No computador, mantenha o sistema operacional, navegador e antivírus atualizados. Instale extensões confiáveis que bloqueiem scripts maliciosos e pop-ups (por exemplo, bloqueadores de anúncios respeitáveis) e desconfie de downloads oferecidos por sites desconhecidos. No celular, atualize o sistema e só instale aplicativos por lojas oficiais (Google Play, App Store).

PEQUENA CHECKLIST DE SEGURANÇA DE REDE:

- Usar WPA2/WPA3 no Wi-Fi doméstico; trocar a senha periodicamente.
- Desabilitar compartilhamento de arquivos em redes públicas.
- Preferir dados móveis ou VPN em redes desconhecidas.
- Verificar certificado de segurança do site (cadeado + https://).

3 - DÊ PREFERÊNCIA AO CARTÃO VIRTUAL

Cartões virtuais (emitidos por bancos e fintechs) são números temporários gerados exclusivamente para compras online. Eles têm validade curta ou são de uso único — isso reduz drasticamente o risco em caso de vazamento. Muitos serviços permitem criar cartões com limite definido, desativá-los a qualquer momento ou restringir o uso a uma única transação.

Quando o site pedir para salvar os dados do cartão (para compras futuras), prefira não salvar. Em vez disso, gere um cartão virtual para a compra e descarte após o uso. Se o banco permitir, crie um cartão virtual para cada loja importante; assim, se houver problema com um vendedor, você bloqueia apenas aquele cartão.

Exemplo de uso: quero comprar na loja X gero um cartão virtual com limite exato do valor da compra concluo a transação o cartão expira automaticamente.

4 - TENHA UM CARTÃO EXCLUSIVO PARA COMPRAS NA INTERNET

Se puder, mantenha um cartão físico ou virtual apenas para compras online. Isso facilita o controle dos gastos e limita a exposição do seu cartão principal. Algumas pessoas deixam um limite baixo nesse cartão exclusivo; outras preferem usá-lo somente em sites que já testaram. Em caso de fraude, só um cartão — com limite controlado — será afetado, não toda a sua conta.

Se usar um cartão dedicado, monitore sua fatura frequentemente e ajuste o limite conforme necessidade. Mantenha o cartão em instituições financeiras confiáveis e ative bloqueios rápidos (via app) para desativar temporariamente o uso caso notifique algo suspeito.

5 - ATIVE A AUTENTICAÇÃO POR DOIS FATORES

Sempre que possível, opte por cartões e contas que exijam autenticação adicional para autorizar compras: SMS com código, app de autenticação (TOTP), biometria (impressão digital/face) ou confirmação por aplicativo do banco. A autenticação por dois fatores (2FA) adiciona uma barreira que impede que criminosos concluam compras mesmo com dados do cartão.

PARA MAIOR SEGURANÇA:

- Prefira apps de autenticação (Google Authenticator, Authy) ao SMS, já que SMS pode ser alvo de clonagem (SIM swap).
- Ative 2FA nas contas de e-mail, lojas online e carteira digital.
- Use biometria quando disponível — é prática e mais difícil de replicar.

6 - ACOMPANHE OS GASTOS COM FREQUÊNCIA

Monitore a fatura do cartão e o extrato bancário com regularidade. Ative notificações em tempo real para cada compra (push ou SMS) — isso facilita detectar cobranças indevidas imediatamente. Se notar uma transação desconhecida, bloqueie o cartão pelo app e entre em contato com o banco para contestar a cobrança.

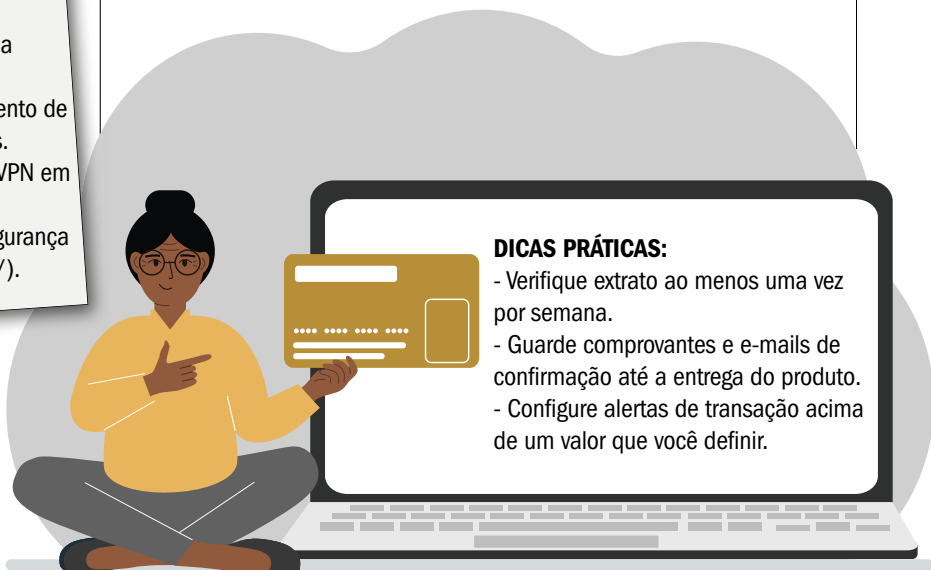
7 - NÃO SALVE OS DADOS DO SEU CARTÃO DE CRÉDITO EM SITES E APLICATIVOS

Evite deixar número, validade e CVC salvos em lojas e apps. Quando salvar, você aumenta o risco em caso de invasão ou vazamento. Prefira digitar os dados sempre que comprar e, quando possível, use métodos de pagamento por token (o próprio site ou gateway transforma seus dados em um token seguro) ou serviços de checkout de terceiros confiáveis (PayPal, Google Pay, Apple Pay, etc.) — estes ocultam o número real do seu cartão.

Se o banco oferece cartões virtuais temporários, use-os em vez de salvar os dados. Caso opte por deixar dados salvos, revise periodicamente os locais onde suas informações estão guardadas e exclua o que for desnecessário.

Seguindo essas práticas, você aproveita a comodidade das compras online com mais tranquilidade e segurança.

“Fazer compras online com mais segurança também contribui para um uso mais consciente do cartão de crédito, o que ajuda na saúde financeira das famílias”, conclui Camila.



DICAS PRÁTICAS:

- Verifique extrato ao menos uma vez por semana.
- Guarde comprovantes e e-mails de confirmação até a entrega do produto.
- Configure alertas de transação acima de um valor que você definir.