**Os riscos de comprar online e como se proteger**

Nos últimos anos, o volume de compras online aumentou absurdamente. As principais lojas virtuais agora oferecem mais opções e seleções de produtos aos consumidores, enquanto as lojas físicas tradicionais oferecem seus próprios incentivos online para permanecer competitivas e capturar uma fatia do mercado online. Além disso, com o despertar da pandemia de COVID-19, [muitas pessoas passaram a comprar online](https://news.un.org/en/story/2021/05/1091182) o que elas costumavam obter nas lojas da vizinhança. Infelizmente, assim como a atividade online dos consumidores, os crimes cibernéticos também aumentaram – gerando prejuízos financeiros para as vítimas.

Mas não é porque existem golpes na Internet e crimes cibernéticos que você deve evitar fazer compras online. Comprar online com segurança é perfeitamente possível, desde que você conheça os riscos potenciais e tome as precauções adequadas.

## Quais são os riscos de fazer compras online?

Os riscos de segurança potenciais representados pelas compras online incluem:

### Roubo de identidade

Normalmente, envolve a invasão dos sites de comércio eletrônico por criminosos que roubam os detalhes de login e cartão de crédito dos usuários para aplicar [golpes financeiros](https://www.kaspersky.com.br/resource-center/threats/online-banking-theft) posteriormente. Esse tipo de roubo permite que os criminosos personifiquem os usuários para fazer compras fraudulentas ou vender detalhes pessoais para outros criminosos.

### Lojas online falsas

Infelizmente, nem todos os sites de comércio eletrônico são autênticos. Os golpistas podem criar sites falsos que se parecem muito com lojas virtuais reais. Eles copiam o design, layouts e roubam logotipos para fazer com que usuários desavisados pensem que estão visitando um site confiável.

Eles podem oferecer marcas populares de roupas, joias e eletrônicos a preços baixos. Algumas vezes, quem compra até mesmo recebe os itens pelos quais pagaram, mas normalmente eles são falsificados. Outras vezes, simplesmente não recebe nada.

### Dados não criptografados

Alguns sites não criptografam dados. Sites que não têm [certificados SSL](https://www.kaspersky.com.br/resource-center/definitions/what-is-a-ssl-certificate) atualizados são mais vulneráveis a ataques. Os sites cujos URLs começam por HTTP em vez de HTTPS não são protegidos – o que é um risco para os compradores que compartilham detalhes de cartões de crédito e outras informações sensiveis.

### Violações de dados

Ao comprar na internet, você compartilha informações sensíveis com os lojistas, incluindo detalhes bancários ou de cartão de crédito, informações de contato e endereço. Se hackers obtiverem acesso não autorizado a um site de comércio eletrônico, haverá o risco de suas informações serem expostas em caso de violação de dados.

### Análises falsas

Muitos compradores leem reviews de produtos antes de comprar. Mas saiba que nem todas as análises são autênticas. Se uma loja específica apresentar um padrão de análises que parece muito bom para ser verdade, ou que não contém muitos detalhes, experimente verificar a fonte e procurar reviews em outros sites.

### Aplicativos falsos

Muitas lojas online autênticas têm aplicativos exclusivos. Algumas vezes, os criminosos cibernéticos tentam imitá-los criando [versões falsas](https://www.kaspersky.com.br/resource-center/preemptive-safety/identifying-and-avoiding-fake-apps). O objetivo é obter suas informações pessoais, como detalhes bancários ou de cartões de crédito, além de nomes de usuário e senhas.

### Wi-Fi sem proteção

Redes Wi-Fi sem proteção em locais públicos podem ser um risco à segurança. Entre eles há o risco de hackers se posicionarem entre você e o ponto de conexão. Se você realizar transações de compras online em uma rede Wi-Fi desprptegida, haverá o risco de hackers obterem as informações pessoais enviadas por você, como detalhes de cartões de crédito e informações pessoais.

### Adware

[Adware](https://www.kaspersky.com.br/resource-center/threats/adware) são anúncios indesejados que aparecem na tela enquanto você navega na Internet. Em inglês, adware é uma contração de "software de publicidade" (advertising software). Seu objetivo é gerar receita para seu dono. O adware pode ser legítimo, mas também pode ser usado por criminosos cibernéticos para fins fraudulentos – por exemplo, direcionar você para sites mal-intencionados que tentam obter suas informações pessoais. Algumas vezes, fechar o anúncio pop-up clicando no símbolo "X" é o suficiente para causar uma infecção.

### Phishing

Envolve o envio por golpistas de emails falsos que aparentam ser de um lojista autêntico. Os emails normalmente contêm um anexo ou link desenvolvido para enganar o destinatário e fazer com que ele clique no link – em geral, isso inicia uma infecção por [malware](https://www.kaspersky.com.br/resource-center/threats/types-of-malware).

## Comprar online é seguro?

Considerando esses riscos, é justo perguntar: comprar online é seguro? Para a maior parte, sim: comprar online é uma atividade segura. Os indivíduos em si e seus hábitos de navegar na Internet e comprar online que podem torná-la insegura. E é exatamente isso que os criminosos cibernéticos estão esperando.

Eles dependem de você não saber como identificar e evitar [emails de phishing](https://www.kaspersky.com.br/resource-center/threats/spam-phishing). Eles precisam que você use senhas fracas ou os mesmos nome de usuário e senha em todas as suas contas online. Eles querem que você use Wi-Fi pública para fazer login em contas privadas. Essencialmente eles dependem de você, o consumidor, não seguir as práticas recomendadas de segurança cibernética.

Se você for vítima de criminosos cibernéticos, isso poderá potencialmente custar muito mais que seu saldo no banco – pode custar sua identidade, o que levará a uma série de problemas financeiros e pessoais.

Há muitas histórias sobre fraudadores e hackers, mas a verdade é que há uma probabilidade muito menor dos criminosos cibernéticos obterem os detalhes do seu cartão de crédito via Internet do que por telefone, email ou mesmo em um restaurante. Ainda assim, comprar online com segurança requer uma medida adicional de vigilância.

## Como verificar se é seguro comprar em um site

Então, como é possível diferenciar sites de comércio eletrônico seguros de sites fraudulentos? Aqui estão alguns sinais que você deve observar:

**Verifique o certificado SSL**

SSL significa "Secure Sockets Layer" e é uma indicação que é seguro comprar em um site. Essencialmente, é um método de [criptografia](https://www.kaspersky.com.br/resource-center/definitions/encryption) que os sites que solicitam informações sensíveis ou pessoais – como detalhes de cartões de crédito – deveriam ter. Para verificar se um site de compras online tem um certificado SSL atualizado, procure um ícone de cadeado na barra de URL do navegador ou verifique se o URL começa com HTTPS, e não HTTP ("S" significa "seguro").

**Procure uma declaração de privacidade**

Uma política de privacidade explica como a empresa coleta, usa e armazena dados confidenciais dos clientes. Embora as leis e regulamentações variem muito no mundo inteiro, lojistas online autênticos deveriam ter uma declaração de privacidade explícita. Se não tiverem, isso poderá ser uma bandeira vermelha.

**Fique longe de negócios que parecem muito bons para ser verdade**

Se um site estiver vendendo roupas de grife, joias ou eletrônicos por preços consideravelmente menores que o preço de varejo usual, pergunte a si mesmo se não é bom demais para ser verdade. Você poderá estar comprando falsificações ou réplicas.

**Procure um endereço e um número de telefone**

Lojistas legítimos normalmente terão um número de telefone e o endereço físico visíveis no cabeçalho ou no rodapé. Se não tiver certeza de que uma loja online é autêntica, uma forma de verificar é copiando e colando os detalhes do endereço em um mecanismo de pesquisa para verificar se a localização é válida. Vendedores fajutos não fornecerão endereço ou usarão um endereço falso.

**Procure erros de ortografia e gramática**

Marcas de reputação normalmente procuram garantir que o texto e a imagem em seus sites seja de boa qualidade. Se um site estiver mal escrito e contiver muitos erros de ortografia ou gramática, isso poderá indicar que o vendedor não é legítimo. Outras bandeiras vermelhas podem incluir imagens de baixa qualidade, políticas de não devolução e a impossibilidade de fazer comentários e análises.

**Verifique se o site aceita cartões de crédito**

Os cartões de crédito estão entre as formas mais seguras de fazer transações online, já que é fácil para os emissores dos cartões reembolsar o dinheiro perdido em fraudes. Sites que não aceitam pagamentos em cartão de crédito podem ser preocupantes, pois é mais difícil que sites fraudulentos sejam certificados pelas empresas de cartões de crédito.

**Veja as análises online**

Ainda que as análises possam ser falsas, continua sendo útil olhar o padrão geral das análises dos clientes ao fazer compras online. Os sites de análises confiáveis podem ajudar a determinar o quanto legítimo é um lojista e o que outros clientes acham antes de você realizar a compra.

## Dicas de segurança para comprar online

Aqui estão algumas dicas para comprar online de forma seguraa:

**Digite o URL diretamente na barra de endereços**

Golpistas que enviam emails de phishing dependem de você clicar no link no email par ser levado para o "site de uma loja" – e o mesmo para links em resultados de pesquisa "envenenados". Esses links podem levar você até sites falsificados cuidadosamente preparados. Assim, quando você acha que está fornecendo seu nome de usuário e demais detalhes no site da Amazon, na verdade está enviando tudo para um criminoso.

Para ter certeza de que está visitando o site real e autêntico da loja, é muito mais seguro digitar o URL na barra de endereço do navegador. Pode demorar um pouco mais, mas essa ação tão simples pode evitar que você acesse um [site falso ou malicioso](https://www.kaspersky.com.br/resource-center/preemptive-safety/scam-websites).

**Obtenha um cartão de crédito temporário**

Os criminosos cibernéticos desenvolveram técnicas e malware muito sofisticados que, algumas vezes, podem frustrar seus melhores esforços de fazer compras online em segurança. Como nível adicional de segurança, você pode usar um cartão de crédito temporário para fazer compras online, em vez de usar seu cartão usual. Consulte o emissor do seu cartão de crédito para saber se é possível emitir um número de cartão de crédito temporário.

Muitas empresas de cartão de crédito fazem isso, permitindo a você realizar uma única compra. Isso impede que qualquer golpista que roube o número do cartão de crédito faça compras fraudulentas adicionais. No entanto, evite usar esses tipos de cartões de crédito em compras que necessitam de pagamentos recorrentes ou renovação automática.

Alguns bancos também oferecem cartões de crédito virtuais. Eles são semelhantes ao seu cartão convencional, mas um número de conta aleatório é gerado para cada compra, o que impede que o número seja reutilizado por hackers.

**Dedique um computador para usar bancos e fazer compras online**

Se você tiver mais de um computador, talvez seja interessante dedicar um deles apenas para usar bancos e fazer compras online. Ao evitar usar o computador para qualquer outro tipo de navegação na Internet, download, leitura de emails, navegação nas redes sociais e outras atividades online, você cria efetivamente um computador "limpo" [livre de vírus de computador e outras infecções](https://www.kaspersky.com.br/resource-center/preemptive-safety/antivirus-choices).

**Use um endereço de e-mail exclusivo**

Semelhante a criar um computador "limpo", você pode fazer o mesmo com um endereço de email. Crie um endereço de email para usar apenas em compras online. Isso limitará o número de mensagens de spam que você receberá e reduzirá o risco de abrir emails potencialmente mal-intencionados disfarçados de promoções de vendas ou outras notificações.

Por exemplo, se você usa seu email dedicado para compras online na Amazon, mas recebe uma mensagem da Amazon em sua conta de email principal informando sobre um problema com um pedido ou na conta da Amazon, você saberá que essa provavelmente é uma mensagem falsa ou mal-intencionada enviada por criminosos.

**Gerencie e proteja suas senhas online**

Usar [senhas fortes](https://www.kaspersky.com.br/resource-center/threats/how-to-create-a-strong-password) e senhas diferentes para cada conta online é uma das medidas mais importantes que você pode adotar para comprar online com segurança. Pode ser desafiador lembrar de muitas senhas diferentes, especialmente quando elas contêm várias letras, números e caracteres especiais. Mas você pode usar um [gerenciador de senhas](https://www.kaspersky.com.br/password-manager) para ajudar. Um bom gerenciador de senhas também criptografa senhas que, do contrário, seriam armazenadas como texto sem formatação. Alguns softwares antivírus e de segurança de Internet incluem o gerenciamento de senhas e recursos de segurança para senhas.

**Evite usar redes Wi-Fi públicas para fazer login em contas online**

Cafés, hotéis, restaurantes e outras áreas públicas muitas vezes oferecem Wi-Fi grátis. Isso pode ser útil para acessar o email, navegar na Internet e realizar outras atividades online. Mas [usar a Wi-Fi pública para entrar em uma conta privada é um risco de segurança.](https://www.kaspersky.com.br/resource-center/preemptive-safety/public-wifi-risks) Hackers inteligentes poderiam estar sequestrando o sinal de Wi-Fi ou até mesmo configurando sua própria rede para enganar você. E eles podem ver tudo o que você faz em seu dispositivo móvel ou laptop. Isso significa que, se você fizer login em uma conta bancária ou em um site de loja, o hacker conseguirá obter seu nome de usuário e a senha.

Também é muito importante ter cuidado ao usar a Wi-Fi pública em lojas físicas tradicionais. Por exemplo, ao fazer compras em um shopping center — prestes a fechar negócio — compreensivelmente talvez você queira consultar os sites online para ver se eles oferecem preços melhores. Mas os criminosos cibernéticos estão contando com isso e podem interceptar seus dados e capturar suas senhas, detalhes de login e informações financeiras. Se precisar acessar a Internet enquanto faz compras, use a rede do celular.

**Use uma VPN**

Se for absolutamente necessário fazer compras online enquanto usa uma rede Wi-Fi pública, instale primeiro uma [VPN (rede privada virtual).](https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn) Uma VPN criptografa todos os dados transferidos entre seu computador ou dispositivo móvel e o [servidor de VPN](https://www.kaspersky.com.br/vpn-secure-connection/vpn-server). Isso significa que os hackers não poderão interceptá-los, mesmo que conheçam a senha da rede Wi-Fi que você está usando. Uma rede VPN pode ser útil para fornecer a você uma maneira segura de comprar online em uma Wi-Fi pública.

**Atenha-se a marcas conhecidas ou das quais já ouviu falar**

Sempre que possível, procure comprar de lojas das quais já ouviu falar, especialmente daquelas com boa reputação. Mas mesmo assim é muito importante ter cuidado – os criminosos muitas vezes escrevem incorretamente os nomes dos sites falsos de propósito para que se assemelhem a uma empresa conhecida. Se você está procurando um item especializado que só está disponível em um site independente, pesquise cuidadosamente antes de enviar quaisquer informações financeiras.

**Ao comprar de um novo fornecedor, pesquise-o cuidadosamente**

Um bom teste é ver se é possível contatar o vendedor em caso de problemas com o pedido – procure um email, número de telefone ou endereço, além de uma política de devoluções. O histórico de feedback de um fornecedor é outra indicação de confiabilidade e integridade. As análises online podem ser úteis para sugerir o quanto fidedigno é um vendedor.

**Preste atenção aos tipos de informações que são solicitados**

Não divulgue mais informações do que o necessário para concluir sua compra. Nunca compartilhe informações pessoais por telefone, a menos que você seja o autor da chamada, e nunca responda a pedidos não solicitados de informações pessoais (especialmente senhas, cartões de crédito ou números de contas bancárias).

**Somente faça pagamentos online usando métodos de pagamento seguros e confiáveis**

Sempre que possível, use cartões de crédito – em geral, suas compras serão garantidas. Se você inserir acidentalmente suas informações de cartão de crédito ou débito em um site mal-intencionado ou responder a um email suspeito com essas informações, entre em contato imediatamente com o emissor do cartão de crédito para alertá-los. Nunca envie dinheiro pelo correio.

**Tenha muito cuidado ao usar seu dispositivo móvel para fazer compras online**

URLs encurtados, muitas vezes utilizados porque são mais fáceis de digitar em telefones, podem enganar e fazer com que você visite sites perigosos.

**Sempre faça logoff após fazer compras online**

Ao concluir uma sessão de compras online, sempre faça logoff, especialmente se você compartilha um computador com alguém ou se usou um computador (como em uma lan house) ou uma rede Wi-Fi públicos

**Acompanhe as faturas dos seus cartões de crédito**

Ao receber as faturas dos cartões de crédito, leia-as cuidadosamente e procure quaisquer cobranças indevidas. Se houver algo fora do normal, comunique imediatamente ao emissor do cartão. Certifique-se de que seus filhos não tenham acesso a suas contas online e limite o acesso às suas informações bancárias e de cartões de crédito.

**Instale software antivírus ou antimalware**

Usar um antivírus abrangente ajudará a proteger você contra ameaças à segurança das compras online.