

# *Comércio via Internet*



Apoio de Divulgação:

**TRT-13ª REGIÃO**  
Secretaria de Governança  
e Gestão Estratégica  
Assessoria de Governança de SI  
e Proteção de Dados Pessoais

Contribuição:

**IDV** INSTITUTO PARA  
DESENVOLVIMENTO  
DO VAREJO

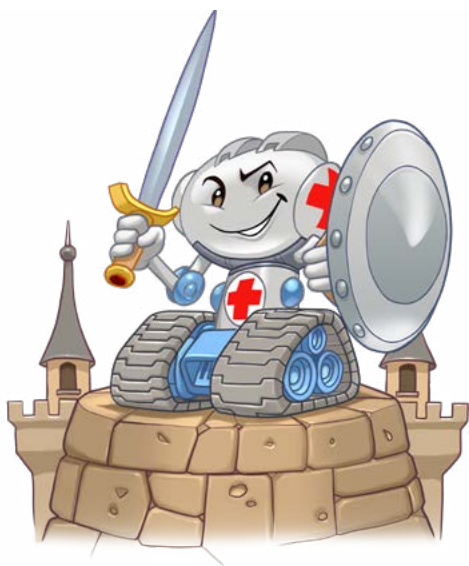
Produção:

**cert.br nic.br cgi.br**

# ***COMPRE E VENDA COM SEGURANÇA***

**A** Internet permite comprar ou vender, a qualquer tempo e lugar, produtos e serviços que nem sempre estão a nosso alcance no dia a dia. No entanto, com os fraudadores cada vez mais ardilosos, é importante tomar cuidado para não ser vítima de golpes.

Veja aqui dicas de segurança no Comércio via Internet.



## UTILIZE DISPOSITIVOS SEGUROS

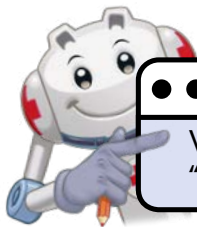
**O** uso de dispositivos com sistemas e aplicativos desatualizados, sem correções de segurança e mecanismos de proteção, facilita a ação de atacantes e de *malware* que visam furtar dados e praticar fraudes.

- » Utilize mecanismos de proteção, como antivírus e *firewall* pessoal
- » Mantenha sistemas e aplicativos atualizados
  - ative a atualização automática, sempre que possível
- » Evite usar dispositivos de terceiros
  - não há como ter certeza se estão seguros
  - seus dados podem ser indevidamente copiados

# USE SOMENTE SITES E APLICATIVOS OFICIAIS

**E**xistem páginas falsas e aplicativos maliciosos que tentam se passar por organizações conhecidas, como as de comércio eletrônico, para enganar você. É preciso ter cuidado para usar somente *sites* ou aplicativos legítimos.

- » Baixe o aplicativo legítimo da instituição a partir das lojas oficiais
- » Acesse o *site* digitando o endereço (URL) diretamente no navegador
  - use sempre conexão segura (https)
- » Se usar *sites* de busca, confirme se a URL apresentada é a correta
- » Salve a página nos “Favoritos” para facilitar futuros acessos



Veja mais dicas no fascículo  
“Celulares e Tablets”.

# INTERAJA SOMENTE COM O PERFIL OFICIAL DA EMPRESA NAS REDES SOCIAIS

**A**o contatar empresas via redes sociais, para efetuar compras ou acionar serviços de atendimento, é preciso ter certeza que o perfil é o legítimo para não entregar seus dados ou seu dinheiro a golpistas.

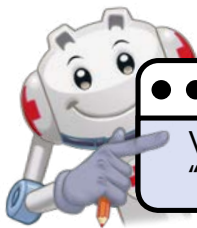


» Confira se o perfil é legítimo (oficial)

- procure pelo selo indicativo de conta comercial verificada, sempre que disponível
- observe se o *link* da descrição direciona para a loja oficial
- busque o perfil no *site* da empresa, se possível

» Desconfie se o perfil:

- cobrar taxas adicionais
- pedir informações como senhas ou dados de cartão

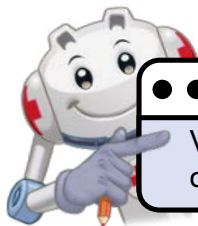
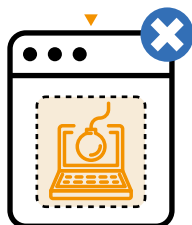


Veja mais dicas no fascículo  
"Phishing e Outros Golpes".

# ANTES DE COMPRAR, PESQUISE A REPUTAÇÃO DO SITE OU PLATAFORMA

É prática comum de golpistas criar páginas e anúncios fraudulentos em sites ou plataformas para atrair e enganar compradores. Eles vendem, mas não entregam a mercadoria e podem usar os dados coletados para cometer outras fraudes.

- » Consulte no Procon as empresas verificadas e as que devem ser evitadas
- » Busque por reclamações em redes sociais e sites especializados
- » Leia avaliações de outros compradores

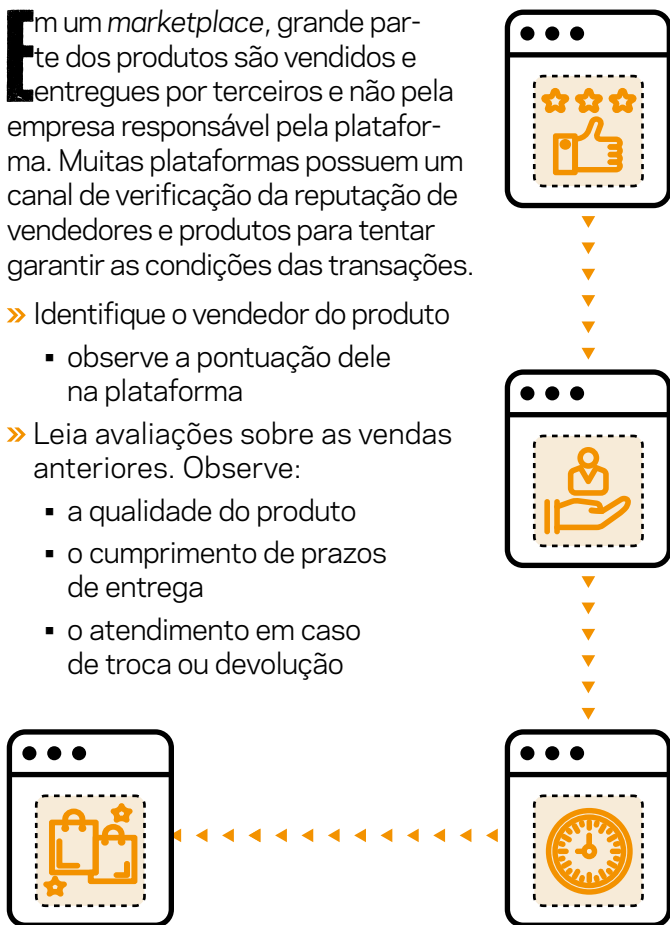


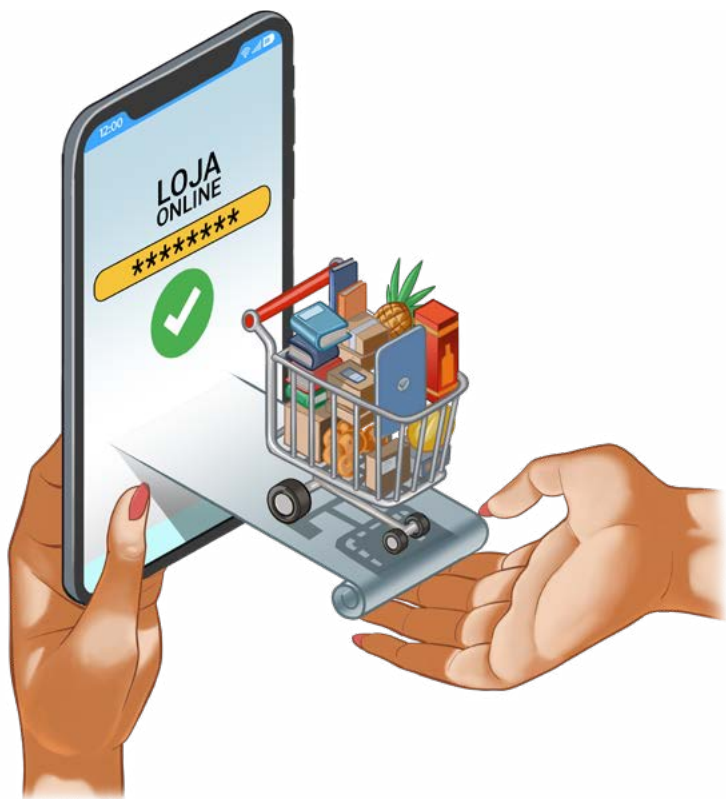
Veja mais dicas no guia “#Internet com Resposta Vai às Compras”.

# VERIFIQUE A REPUTAÇÃO DO VENDEDOR

**E**m um *marketplace*, grande parte dos produtos são vendidos e entregues por terceiros e não pela empresa responsável pela plataforma. Muitas plataformas possuem um canal de verificação da reputação de vendedores e produtos para tentar garantir as condições das transações.

- » Identifique o vendedor do produto
  - observe a pontuação dele na plataforma
- » Leia avaliações sobre as vendas anteriores. Observe:
  - a qualidade do produto
  - o cumprimento de prazos de entrega
  - o atendimento em caso de troca ou devolução





Marketplace é o termo usado quando diversos vendedores são reunidos numa mesma plataforma, mas os produtos podem ser vendidos e entregues pela própria plataforma ou por vendedores terceiros.

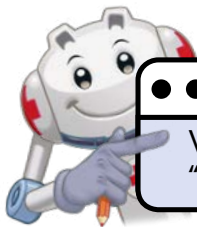


# FAÇA TODO O PROCESSO DE COMPRA E VENDA DENTRO DA PLATAFORMA

**G**olpistas alegam falha de sistema e pedem que o cliente pague ao entregador, ou desviam a conversa para outros canais nos quais apresentam falsos comprovantes ou cobram taxas extras. Se você negociar fora da plataforma, perderá os recursos de segurança que ela oferece.



- » Desconfie de pedidos de pagamento ou negociação fora da plataforma
  - na dúvida, contate a plataforma via canais oficiais
- » Ao fazer qualquer pagamento:
  - confira o valor antes de autorizar a cobrança
  - confirme o valor cobrado em sua conta e/ou cartão de crédito



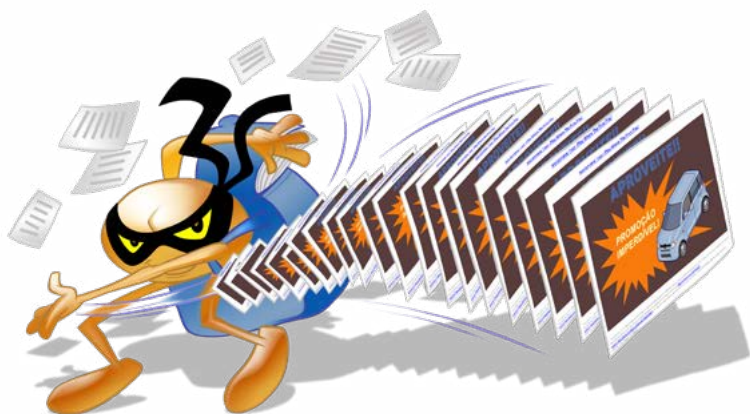
Veja mais dicas no fascículo  
"Phishing e Outros Golpes".



# NÃO SE DEIXE LEVAR POR MENSAGENS E E-MAILS ENGANOSOS

**A**lertas de compras no cartão de crédito, pedidos de confirmação de compra ou anúncios muito vantajosos são usados como iscas para fazê-lo clicar em *links* maliciosos ou telefonar para números falsos, pelos quais o golpista vai tentar efetivar o golpe.

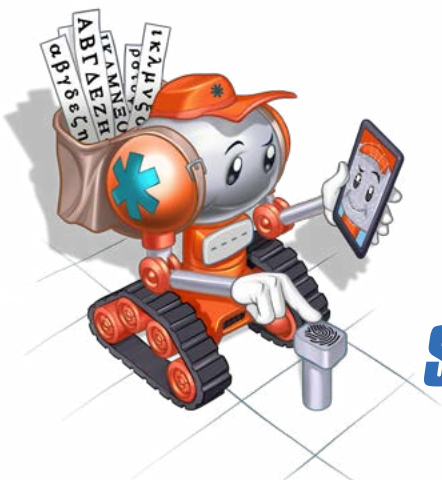
- » Não clique no *link* nem ligue para o número enviado na mensagem
  - verifique se a promoção realmente existe
  - na dúvida, contate a instituição via canais oficiais
- » Desconfie sempre!
  - questione se o conteúdo faz sentido
  - lembre-se: “quando a esmola é demais, o santo desconfia”



## VERIFIQUE SE O LINK OU A PUBLICAÇÃO PATROCINADA É LEGÍTIMA

**L**inks e publicações patrocinadas são recursos comerciais legítimos, usados para atrair visitantes para sites e perfis dos anunciantes, mas podem ser explorados por golpistas para aumentar os acessos a anúncios fraudulentos e páginas falsas ou com *malware*.

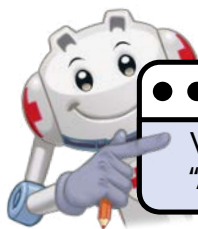
- » Fique atento a promoções ofertadas via publicações e *links* patrocinados
  - prefira acessar diretamente o site, aplicativo ou perfil, sem clicar em *links*



## **PROTEJA SUAS CONTAS E SENHAS**

**S**e conseguirem suas senhas e códigos de verificação, golpistas podem invadir suas contas, furtrar sua identidade e cometer fraudes em seu nome, causando prejuízos inclusive à sua reputação e pontuação de crédito.

- » Ative a verificação em duas etapas
- » Não compartilhe seu usuário e senha, nem códigos verificação
- » Não repita senhas
  - uma senha vazada pode dar acesso a várias contas e dispositivos



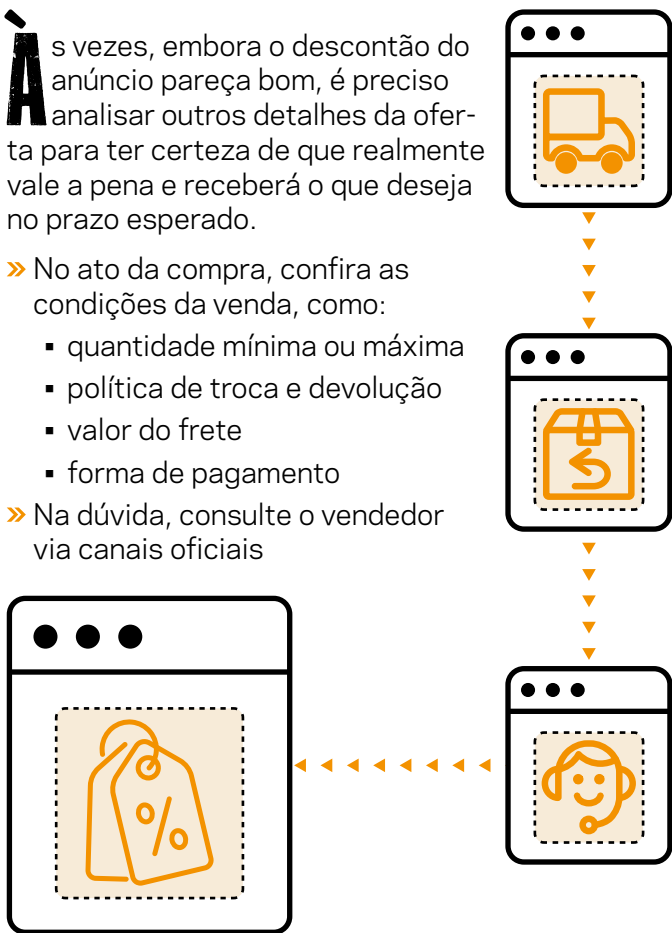
Veja mais dicas no fascículo  
"Autenticação".



# ANALISE AS CONDIÇÕES DE COMPRA E VENDA

**A**s vezes, embora o desconto do anúncio pareça bom, é preciso analisar outros detalhes da oferta para ter certeza de que realmente vale a pena e receberá o que deseja no prazo esperado.

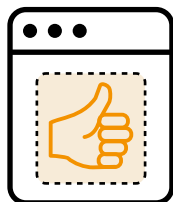
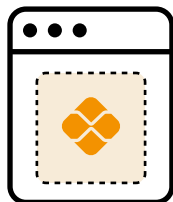
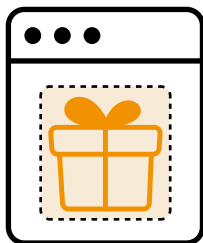
- » No ato da compra, confira as condições da venda, como:
  - quantidade mínima ou máxima
  - política de troca e devolução
  - valor do frete
  - forma de pagamento
- » Na dúvida, consulte o vendedor via canais oficiais



# PREPARE-SE PARA NÃO PERDER OFERTAS

**C**ampanhas como a *Black Friday* são bastante famosas e marcadas por ofertas que se esgotam rapidamente devido à alta procura e aos estoques limitados.

- » Tenha em mente que, para garantir o produto, não basta incluí-lo no carrinho
  - é necessária a confirmação do pagamento
- » Ofertas com pagamento via Pix costumam ter desconto
  - lembre-se de ajustar seus limites de transferência antes da compra





## ***SE USAR PIX, CONFIRA OS DADOS ANTES DE CONFIRMAR A OPERAÇÃO***

**A** pesar de pagamentos via Pix serem práticos e, muitas vezes, mais vantajosos, chaves falsas podem ser usadas por golpistas para induzir transações fraudulentas. Além disso, comprovantes falsos também são usados para confirmar a efetivação de uma transação não realizada.

- » Antes de transferir, confira os dados do destinatário
- » Para recebimentos via Pix, confira se o valor realmente caiu na sua conta antes de entregar o produto

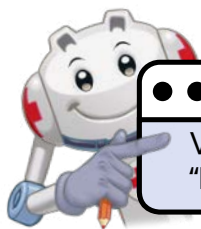




## **SE USAR CARTÃO, PREFIRA O VIRTUAL**

**A**lguns sites e aplicativos permitem gravar dados do cartão de crédito para compras recorrentes, como serviços de transporte. Para evitar que furem dados de seu cartão físico em caso de invasão de conta, prefira usar a opção virtual ou *online*.

- » Use cartão virtual, caso opte por gravar os dados de seu cartão
  - ele possui dados diferentes do cartão físico e pode ser alterado com frequência
- » Reduza o limite do cartão virtual, se possível
- » Habilite e acompanhe as notificações de uso
  - caso haja movimentações estranhas, fale com o seu banco



Veja mais dicas no fascículo  
"Banco via Internet".

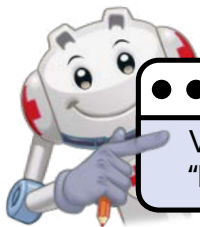
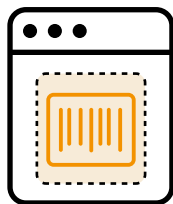
# SE USAR BOLETO, CONFIRA OS DADOS ANTES DE PAGAR

O boleto é uma forma prática de pagamento que pode ser usada mesmo por quem não tem conta bancária; entretanto, é preciso ficar atento para não pagar um documento adulterado.

» Antes de pagar, verifique, por exemplo:

- se os dados do beneficiário, como nome e CNPJ, correspondem aos do vendedor
- se os dígitos iniciais do código digitável são iguais ao código de identificação do banco emissor
- se os últimos dígitos do código digitável correspondem ao valor a ser pago

» Se desconfiar de algo, não pague o boleto e contate o vendedor via canais oficiais

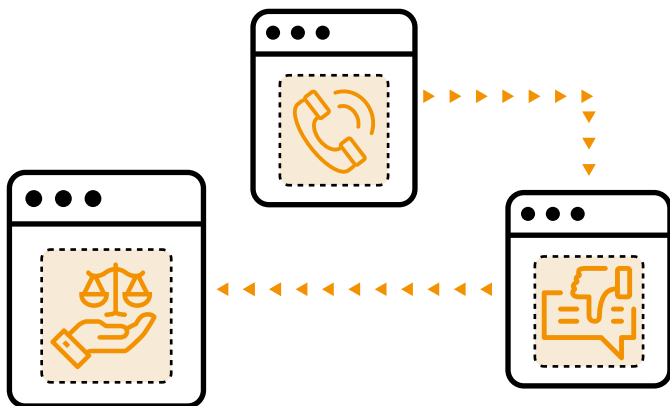


Veja mais dicas no fascículo  
"Banco via Internet".

# COMPROU OU VENDEU E NÃO RECEBEU? O QUE FAZER?

**A**s vezes, acontece de o comprador não receber o produto ou o vendedor não receber o valor correspondente à venda. É importante tentar os canais oficiais para resolver o problema.

- » Contate o site ou a plataforma responsável pela compra ou venda
- » Caso necessário, recorra ao Procon de sua região ou sites de reclamações
- » Se ainda não conseguir resolver o problema:
  - faça um boletim de ocorrência
  - considere procurar ajuda jurídica





## **SAIBA MAIS**

- » Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança para Internet, disponíveis em: **<https://cartilha.cert.br/>**
- » Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores. Confira em: **<https://internetsegura.br/>**

## cert.br

O CERT.br (<https://cert.br/>) é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional de último recurso, mantido pelo NIC.br. Além da gestão de incidentes, atua na conscientização sobre segurança, na consciência situacional e na transferência de conhecimento, em cooperação com outros CSIRTs.

## nic.br

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br (<https://nic.br/>) é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz diversas ações que trazem benefícios à Internet no Brasil.

## cgi.br

O Comitê Gestor da Internet no Brasil (<https://cgi.br/>), responsável por estabelecer diretrizes estratégicas para o uso e desenvolvimento da Internet no País, coordena e integra iniciativas de serviços Internet, promovendo qualidade e inovação.



O IDV - Instituto para Desenvolvimento do Varejo (<https://idv.org.br/>) nasceu em 2004 para fortalecer a representatividade de empresas varejistas formais de diferentes setores de atuação nacional, promovendo o desenvolvimento sustentável do varejo e contribuindo para a melhoria da vida das pessoas.



<https://cartilha.cert.br/cc/>