

cartilha de  
**compras**  
seguras  
na **Internet**



RNP



CAIS

quais as  
vantagens de  
se **comprar**  
pela **Internet?**

3

**sumário**

antes,  
**durante** e  
**depois** das  
**compras**

5



A comodidade de realizar compras pela Internet é uma realidade atualmente, fazendo cada vez mais parte do dia a dia das pessoas. Leia nesta cartilha como realizar operações de compra de forma segura.

quais as vantagens  
de se **comprar** pela **Internet**?

## 1 **Comodidade:**

Não há filas ou multidões, o serviço fica disponível 24 horas por dia e você pode comprar sem sair de casa.

## 2 **Pesquisa de preço:** A Internet é o limite. Você pode

pesquisar preços em diversos sites ou utilizar serviços específicos para isso, optando pela melhor oferta.



## 4 **Formas de paga-**

**mento:** Comprar pela internet geralmente possibilita muitas outras formas de pagamento além das encontradas em lojas convencionais.

## 3 **Descontos:** Geralmente as lojas online oferecem muito mais produtos em promoção que as lojas físicas – isso sem falar nos sites de compras coletivas, que apresentam descontos de até 90%.



## 5 **Personalização:** Nada de vendedores empurrando compras – na Internet, você consulta e escolhe o que quiser.

## ▶ **fique ligado**

**Itens com mais risco:** Tenha cuidado especial ao comprar itens populares, como *smartphones*, TVs LCD, *notebooks* e *tablets*. Itens mais desejados são mais explorados, o que pode tornar a compra mais arriscada. Desconfie se vir muitos itens difíceis de serem encontrados em um mesmo *site* ou descontos que parecem bons demais para serem verdade.



antes, durante  
e **depois** das **compras**

# antes das compras

► **Antes de comprar, você precisa estar atento(a) ao seu computador.** Seu programa antivírus está atualizado? As atualizações são importantes porque a cada dia milhares de novas ameaças surgem na Internet e um programa desatualizado pode não identificá-las, deixando seu computador desprotegido. Se existir algum vírus, não é seguro fazer compras online a partir dele. Então, faça a verificação!

► **Se não souber como reforçar a segurança do seu computador, peça ajuda.** Vulnerabilidades em *softwares* ajudam os fraudadores. É fundamental manter um antivírus, *firewall* pessoal, *anti-spyware* e *anti-spam*. No caso de ambiente Windows, utilize a opção **Microsoft Update** para atualizações. Tanto o sistema operacional quanto os aplicativos (exemplo: Microsoft Office) serão atualizados.

► **Da mesma forma, tenha sempre as versões mais recentes de seu navegador de acesso à Internet.** Todos os principais navegadores têm atualizações automáticas, alguns por meio das atualizações do sistema operacional (exemplos: Microsoft Internet Explorer, Apple Safari), outros por meio da própria aplicação (exemplos: Mozilla Firefox e Google Chrome). Nesse último caso, às vezes é necessário fechar o navegador para que o processo de atualização seja concluído. Esse simples cuidado oferece muito mais proteção adicional contra golpes de *phishing* e vírus.





► **Mantenha atualizados também o Adobe Flash Player, Oracle, Java e Adobe Reader** (para documentos *.pdf*). Há inúmeras vulnerabilidades que afetam essas aplicações. Uma vez que eles têm integração com os navegadores, basta abrir uma página maliciosa para comprometer seu computador.



► **Apesar de tentadores, desconfie dos preços muito abaixo da média do mercado.** Se não for um *site* de compras coletivas, onde geralmente os descontos chegam a até 90%, pode tratar-se de uma fraude. Pesquise o preço médio do produto em *Já Cotei* (<http://www.jacotei.com.br>) ou Buscapé (<http://www.buscape.com.br>). Conhece a velha história de que “o barato pode sair caro”? Encaixa-se perfeitamente aqui. Tenha bom senso.



► **Confira sempre os Termos de Uso e a Política de Privacidade da loja para ver se concorda com eles antes de efetuar a sua compra.** Também é importante estar ciente da política de trocas e devoluções para saber como a loja reage a esse tipo de ocorrência.



► **Seja cuidadoso com os links patrocinados do Google e do Facebook.** Já aconteceram diversos ca-



tos em que fraudadores pagaram pelo serviço para destacar suas páginas falsas ou páginas de distribuição de *software* malicioso (*malware*). Utilize sites de busca alternativos para verificar o endereço correto da loja, como Microsoft Bing e DuckDuckGo (<https://duckduckgo.com>).

► **Telefone para tirar dúvidas.** Se o site não oferecer um telefone para contato, desconfie.

► **Não deixe suas compras para a última hora, como no caso de aniversários e datas comerciais.** Atrasos eventuais podem ocorrer em época de grande demanda. Organize-se para comprar com antecedência, pois assim você poderá evitar contratempos.

► **Troque a senha de seu usuário PagSeguro ou PayPal com frequência.**



## » mais algumas dicas para proteger seu computador

▶ **Instrua todas as pessoas que usam o seu computador para que elas façam bom uso dele e não baixem arquivos desconhecidos.** Se possível, tenha um computador exclusivamente para compras e uso de banco por Internet.

▶ **Crie um usuário sem privilégios de administrador para uso da família.** O usuário “*Administrador*” (sistemas Microsoft Windows) tem acesso total ao sistema, o que permite ao atacante comprometer ainda mais o sistema com “*keyloggers*” (Trojan ou cavalos de Tróia).

▶ **Senhas ainda são muito importantes.** Não utilize senhas óbvias, como palavras encontradas em um dicionário. Use no mínimo 8 caracteres, incluindo números, letras em maiúsculo e minúsculo e caracteres especiais (exemplo: %\$#\*&). Outra dica importantíssima é não repetir a mesma senha em vários *sites* diferentes.

▶ **Nunca baixe conteúdo ilegal** (isto é, que viola direitos autorais) **ou de origem desconhecida**, pois isso pode comprometer a integridade do seu computador.

▶ **Mensagens de e-mail com remetente desconhecido, que solicitem dados confidenciais, possuam links camuflados ou ofereçam prêmios aos quais você nunca concorreu são exemplos de mensagens consideradas suspeitas.** Desconfie!

▶ **O CAIS mantém um catálogo com as principais fraudes em circulação na Internet que pode lhe ser útil para identificar ações maliciosas.** Visite:

<http://www.rnp.br/cais/fraudes.php>

## ► como saber se uma loja *online* é confiável?

### ◉ Aproveite o trabalho que organizações de defesa

**do consumidor já fez.** O PROCON-SP mantém uma lista de *websites* de compras que devem ser evitados. Atualmente a lista conta com mais de 200 entradas, com dados adicionais como Razão Social e CNPJ. Consulte a lista em [http://www.procon.sp.gov.br/pdf/acs\\_site-naorecomendados.pdf](http://www.procon.sp.gov.br/pdf/acs_site-naorecomendados.pdf) (arquivo PDF).

### ◉ Não visite *sites* sugeridos em spam que você rece-

**be por e-mail.** Você pode ser levado a *sites* falsos cujo objetivo seja coletar seus dados financeiros ou instalar programas maliciosos.

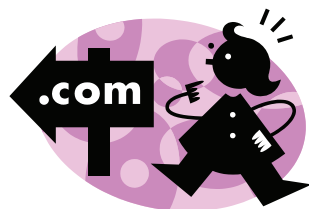
### ◉ Todos os principais navegadores têm um recurso

**que verifica se cada página que você abre foi denunciada como *phishing*.** Você também pode instalar o *AntiFraude UOL*

(Barra UOL – <http://barrauol.uol.com.br/antifraude.jhtm>), que oferece proteção adicional.

### ◉ Faça uma consulta sobre a empresa no site **Reclame**

**Aqui** ([www.reclameaqui.com.br](http://www.reclameaqui.com.br)). Uma busca rápida pode revelar resultados sobre atrasos na entrega, problemas com trocas, produtos danificados, entre outros



problemas. Confirme se a empresa existe realmente.

● **Procure o CNPJ no site Registro.br** (<https://registro.br/cgi-bin/whois>) e faça uma busca simples na Receita Federal ([www.receita.fazenda.gov.br](http://www.receita.fazenda.gov.br)) e na junta Comercial de seu estado (JUICSP no caso de São Paulo – <http://www.juicsp.fazenda.sp.gov.br>). Desconfie do site se não encontrar um CNPJ associado.

● **Pesquise sobre a empresa nos sites de busca.** Você pode encontrar tanto reclamações quanto boas indicações.

● **Peça opinião de outras pessoas em suas redes sociais ou mesmo pessoalmente.** Sempre é mais confiável comprar em uma loja onde outras pessoas compraram sem problemas.



# durante as compras

► **Prefira fazer suas compras *online* a partir de seu computador pessoal, pois você tem mais controle do que foi acessado através dele.**

Se utilizar computadores públicos, de LAN *houses*, do trabalho ou mesmo de amigos, tome cuidados adicionais, como não usar cartão de crédito como forma de pagamento ou trocar suas senhas posteriormente.

► **Verifique se o *site* oferece comunicação segura entre seu computador e o servidor.** O nome técnico deste protocolo é *SSL* ou *TLS* (*Secure Socket Layer / Transport Layer Security*) e pode ser verificado em seu navegador pela presença do endereço no formato *https://www. exemplo.com* (em vez de *http://...*) e da figura de um cadeado na interface gráfica de seu navegador.

► **Usar o cartão de crédito em compras *online* é tão seguro quanto usá-lo em um restaurante.** Tanto compras no mundo real quanto *online* estão sujeitas a fraudes ou problemas na manipulação de seus dados (armazenamento inadequado e vazamento dos dados de seu cartão, por exemplo). Se preferir,





use UOL PagSeguro ou PayPal. Essas duas formas de pagamento são muito seguras e você não precisa fornecer os dados de seu cartão de crédito à loja.

► **O PROCON de várias cidades recomenda que não se realize depósito bancário em nome de pessoas físicas.**

► **Se ainda assim você não se sentir muito seguro(a), escolha o pagamento via boleto bancário ou SEDEX a cobrar.** Evite informar sua conta bancária e CPF – prefira um depósito não identificado.

## » dicas essenciais para fazer compras coletivas seguras

► **Há muitos sites de compra coletiva na Internet.** Segundo uma matéria da revista *Exame* de Novembro de 2012, no auge desse tipo de serviço existiram 1.050 sites. É difícil de separar os sites confiáveis dos fraudulentos. Groupon, Peixe Urbano, SaveMe (BuscaPé Company) e clickOn são os principais – prefira perder promoções mas comprar em sites com melhor reputação. O PROCON São Paulo registrou um aumento de 400% nas reclamações contra esse tipo de site no primeiro semestre de 2012.

► **Desconfie de descontos muito grandes para itens de grande procura, como produtos de grife, smartphones, tablets e laptops.** Não há milagre que faça com que o preço de um desses itens, original e com impostos devidamente pagos, seja mais de 30% menor.

► **Mesmo sites confiáveis têm ofertas de empresas de maior ou menor confian-**

**ça.** O Groupon concede um “Selo de Aprovação” às lojas que passaram por um cuidadoso processo de seleção. Saiba mais em

<http://www.groupon.com.br/sello-de-aprovacao>.



► **Pergunte aos seus amigos se eles já compraram pelo site em questão.** Sempre é melhor contar com a indicação de alguém conhecido.

► **Pesquise sobre o site nas redes sociais.** Veja o que estão falando dele, se existe algum elogio ou reclamação.

► **Verifique a abrangência geográfica do site.** Os sites melhor estruturados oferecem promoções em muitas cidades diferentes.

► **Veja se você conhece as marcas que estão anunciando.** Nomes conhecidos passam uma segurança maior.

► **Observe quantas ofertas já foram vendidas.** Será que uma loja ou serviço pequeno conseguirá atender a demanda? Atente para esta questão.

► **Confira no box “Como saber se uma loja é confiável” outras dicas que também se aplicam às compras coletivas.**







## » dicas de segurança para compras em *sites* internacionais

► **Verifique se o vendedor ou loja entrega os produtos no Brasil.**

► **Verifique também a reputação do vendedor.**

► **Alguns produtos podem ser taxados e retidos pela alfândega.** Verifique as taxas de envio internacional antes de comprar, assim como a política de entrega da loja. Procure referências.

► **Sempre é melhor comprar de algum vendedor ou loja indicado por alguém que já tenha recebido seu pedido sem problemas.**

► **Faça uma busca na Internet para conferir o que foi dito sobre a loja.**



## ► fique ligado

**Cadeado no navegador não é garantia de segurança!** O cadeado significa apenas que um protocolo chamado *TLS* (também chamado de *SSL*) está fazendo com que a conexão entre seu computador e o servidor que hospeda o *website* seja protegida por criptografia.

**Certos ataques permitem que um atacante se coloque no meio da conexão *TLS* e capture seus dados.**

Outros ataques envolvem a instalação de progra-

mas maliciosos, que direcionam seu computador para *websites* falsos mesmo que o endereço seja o correto. É possível também alterar a configuração de seu roteador Wi-Fi ou *cable* modem (do provedor de Internet) de forma que a tradução de nomes (*site.exemplo.com*) para endereços IP – o protocolo DNS – leve seu computador a se conectar com um *site* falso, mas que tem um endereço correto. Existem ainda ataques muito avançados que envolvem os chamados “*exploit kits*” e que infectam sua máquina pela simples abertura da página com um computador desatualizado.

**Mantenha seu computador totalmente atualizado** – sistema operacional, *plug-ins* de navegador como Adobe Flash e Java, Adobe Reader e principalmente navegadores. Fique atento aos alertas relacionados a certificados digitais e *websites* perigosos (páginas falsas ou que já hospedaram programas maliciosos) que seu navegador exibe.

**Essas boas práticas, aliadas a um comportamento seguro** (como não abrir mensagens e *links* enviados por desconhecidos), **são muito eficazes contra ataques atuais e futuros.**

# depois das compras

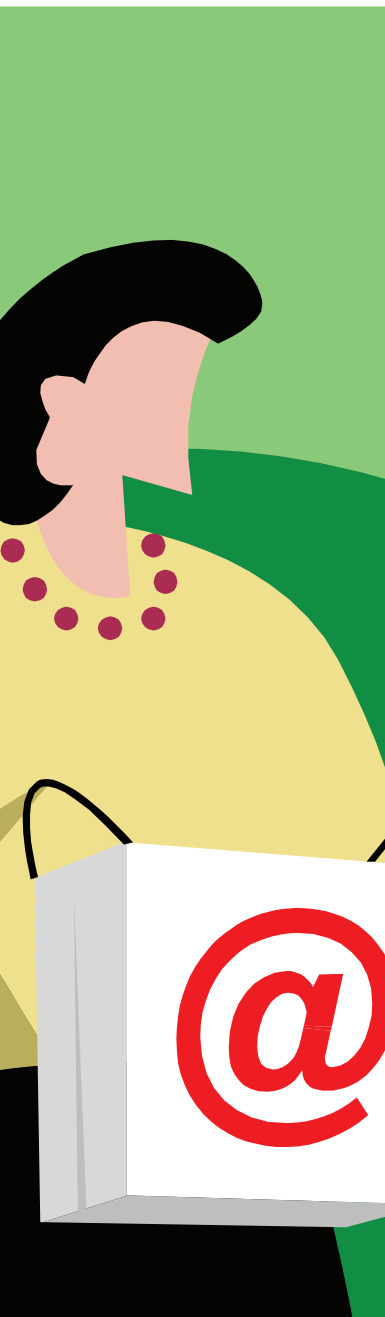
**No caso de compras pela Internet, o PROCON informa que o consumidor pode fazer uso do direito de arrependimento.** Desistir da compra é possível dentro de sete dias contados a partir da data de entrega do produto.

**Caso tenha efetuado cadastro com seus dados, faça logoff do site.** Faça o mesmo depois de efetuar a compra. O raciocínio é o seguinte: quando você tira dinheiro do banco, você não encerra a sessão antes de deixar o caixa eletrônico? Sim, pois desta forma você está protegendo a sua conta, evitando que outros a acessem. A lógica é a mesma ao fazer *logoff*.

**Sempre salve comprovantes de compras.** Se você tiver problemas mais tarde, poderá precisar deles. Você pode salvá-los em seu computador ou enviá-los para o seu *e-mail* a fim de arquivá-los.

**Erros e atrasos podem ocorrer mesmo com as melhores e mais confiáveis empresas online, por diversas razões.** Veja o que você pode fazer se isso acontecer com você:





## » o que fazer caso não receba o produto na data prevista

► **Entre em contato com a loja cobrando a entrega e aguarde uma resposta.** Caso não consiga resolver o problema diretamente com a empresa, você pode postar uma reclamação no *site Reclame Aqui* ([www.reclameaqui.com.br](http://www.reclameaqui.com.br)), onde se costuma dar bastante atenção às ocorrências. Lembre-se de que esse site é apenas um registro público de reclamações, que também auxilia na interação entre consumidor reclamante e empresas reclamadas. Não há garantia de resolução do problema. Esse site é mais útil no processo de escolha da empresa.

► **Se não tiver sucesso no contato com a empresa, procure uma unidade do PROCON** (<http://www.portaldoconsumidor.gov.br/procon.asp?acao=buscar>) **para registrar uma reclamação.** Você também pode procurar um *Juizado Especial Cível* (Pequenas Causas) e ingressar com uma ação.

Para obter a razão social e CNPJ, ou CPF associado ao domínio consulte o *Registro.br* (<https://registro.br/cgi->



*bin/whois*). Essa dica vale somente para *websites* cujo domínio seja *.br*.

▶ **Reclamar de compras e produtos por meio de redes sociais é muito popular.** Embora a maioria das empresas monitorem sua marca nas principais redes sociais, reclamar por meio delas é pouco efetivo. Além disso, muitos dos amigos que o seguem podem considerar essas reclamações inapropriadas e inconvenientes. Use as redes sociais para divulgar e propagar sua reclamação em último caso.

## ► fique ligado

**Confira com muita atenção as faturas de seus cartões de crédito.** O

ideal é conferir assim que ela chegar. Se identificar uma compra irregular, informe a sua operadora. Operadoras sérias costumam apoiar o processo de investigação e ressarcir, quando comprovada a fraude. A maioria dos cartões oferece fatura parcial – a movimentação atualizada antes do fechamento. Verifique se seu cartão oferece o serviço de notificação de transações via SMS (torpedo). Este recurso não impede fraudes, mas permite que você reaja o mais rápido possível.



## » compras em sites de leilão

► **Os sites de leilões** (<http://www.bomnegocio.com/>, <http://www.olx.com.br/>, <http://www.mercadolivre.com.br> entre outros) são uma modalidade de compra diferente da convencional, principalmente pelo fato de intermediar a compra com lojas e pessoas físicas. Sendo que o intermediador, o site de leilão, não se responsabiliza pelas negociações que são realizadas, é preciso ter um cuidado redobrado quando da compra por este meio.

► **Conheça o sistema de qualificação de vendedores do seu site de leilões preferido.** Você pode saber mais sobre a reputação do vendedor a partir da avaliação de vendas anteriores feitas por outros compradores.

► **Leia os comentários que os compradores anteriores fizeram com relação ao vendedor.** Embora este tipo de indicador esteja sujeito a fraude, a reputação é uma boa maneira de avaliar o vendedor.

► **Leia atentamente a descrição dos produtos, política de compra e de entrega do produto.**

► **Pergunte sobre o produto no espaço destinado a este fim.** Esse tipo de recurso normalmente é aberto a qualquer pessoa que consulte o produto, podendo ser útil para identificar características que não condizem com a descrição ou mesmo para conhecer compradores insatisfeitos. Se você se sentiu lesado por algum vendedor, informe a administração e possíveis futuros compradores (por meio de qualificação) o mais breve possível.

Confira as iniciativas e projetos de segurança da  
informação promovidos pela RNP em:

<http://www.rnp.br/servicos/seguranca>