Cartilha de Segurança para Internet

FASCÍCULO

COMÉRCIO ELETRÔNICO

cert.br nic.br cgi.br

ATUALMENTE, GRAÇAS À INTERNET, É POSSÍVEL COMPRAR PRODUTOS SEM SAIR DE CASA OU DO TRABALHO, SEM SE PREOCUPAR COM HORÁRIOS E SEM ENFRENTAR FILAS

E ainda receber tudo em casa ou pedir para entregar diretamente onde desejar.

Infelizmente há golpistas que se aproveitam das facilidades do comércio eletrônico para cometer fraudes. Assim como existem lojas, *sites* e vendedores confiáveis, também existem aqueles cujo objetivo é lesar os consumidores, causar prejuízos e obter vantagens financeiras.

Os golpes envolvendo comércio eletrônico são aqueles que procuram explorar a relação de confiança existente entre as partes envolvidas na transação comercial.

Alguns exemplos de golpes deste tipo são:

- **Golpe do site falso (*phishing*):** um golpista pode criar um *site* falso, similar ao *site* original, e induzir os clientes a fornecerem dados pessoais e financeiros, achando que estão no *site* verdadeiro
- **Golpe do *site* de comércio eletrônico fraudulento:** um golpista pode criar um *site* fraudulento, com o objetivo de enganar os clientes que, após efetuarem os pagamentos, não recebem as mercadorias. Também pode anunciar promoções em *sites* de compras coletivas e, assim, conseguir grande quantidade de vítimas em um curto intervalo de tempo
- **Golpe do *site* de leilão e venda de produtos:** um golpista pode usar um *site* deste tipo para vender produtos que nunca serão entregues. Também pode usar os dados pessoais e financeiros envolvidos na transação para outros fins.

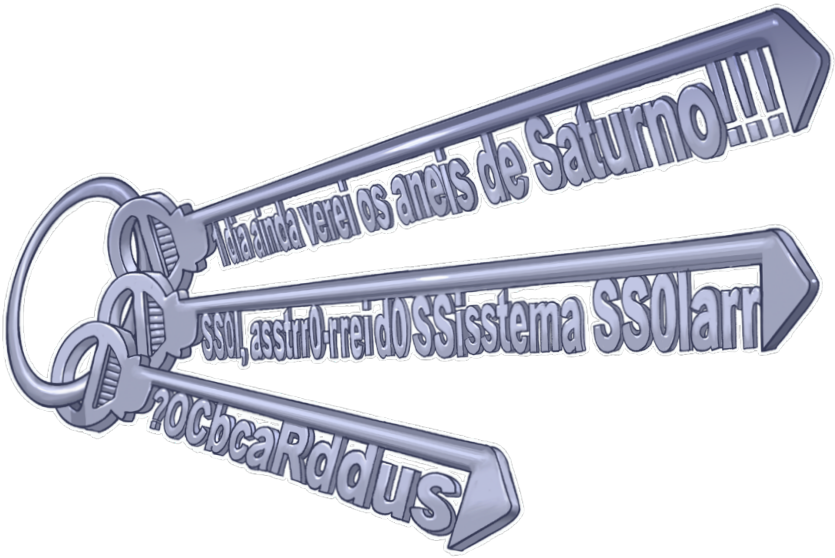
COMÉRCIO ELETRÔNICO: COMPRE COM SEGURANÇA

RISCOS PRINCIPAIS

Para aproveitar todo o conforto e as facilidades do comércio eletrônico de forma segura é importante, além de conhecer os golpes que são aplicados, estar ciente dos riscos que eles podem representar.

Alguns dos riscos que você pode enfrentar ao comprar pela Internet são:

- Não receber o produto
- Receber o produto, porém:
  - com atraso
  - totalmente ou parcialmente danificado
  - com características ou especificações diferentes do esperado
  - de origem ilícita ou criminosa, como contrabando ou roubo de carga
- Enfrentar dificuldades de contato com o *site*/loja, a fim de resolver problemas
- Ficar insatisfeito com a compra (“não era bem isso que eu imaginava”)
- Ter os dados pessoais e financeiros indevidamente obtidos, por meio:
  - do uso de computadores invadidos ou infectados
  - do acesso a *sites* fraudulentos e falsos
  - da interceptação de tráfego, caso o *site*/loja não use conexão segura
- Ter a privacidade invadida, via o compartilhamento indevido de dados pessoais
- Ter os dados financeiros repassados para outras empresas e indevidamente usados para outros fins
- Recebimento de *spam*



CUIDADOS A SEREM TOMADOS

ANTES DE COMPRAR

» Utilize sempre um computador seguro
- com a versão mais recente de todos os programas instalados
- com todas as atualizações aplicadas
- com mecanismos de segurança instalados e atualizados, como *antimalware*, *antispam*, e *firewall* pessoal

» Evite usar computadores de terceiros

» Acesse o *site*/loja digitando o endereço diretamente no navegador *web*
- evite seguir ou clicar em *links* recebidos em mensagens
- não utilize *sites* de busca para localizar o *site*/loja de comércio eletrônico

» Seja cuidadoso ao elaborar suas senhas
- utilize
  - números aleatórios
  - grande quantidade de caracteres
  - diferentes tipos de caracteres
- não utilize
  - sequências de teclado
  - qualquer tipo de dado pessoal
  - a sua própria conta de usuário
  - palavras que façam parte de listas

» Verifique se o *site*/loja é confiável
- pesquise na Internet para ver a opinião de outros clientes
  - principalmente em redes sociais e *sites* de reclamações
- escolha *sites*/lojas que você conheça pessoalmente e/ou que tenha boas referências
- observe:
  - se há reclamações referentes à empresa e se elas foram tratadas adequadamente
  - se são disponibilizados canais de atendimento, como *e-mail*, *chat* e telefone

- se a empresa disponibiliza informações, como endereço, telefone e CNPJ
- as políticas de privacidade, garantia, troca, cancelamento, arrependimento e devolução

- procure validar os dados de cadastro da empresa no *site* da Receita Federal

» Verifique as condições de compra

- faça uma pesquisa de mercado e desconfie se o produto estiver muito barato
- observe:
  - as condições do produto (novo, usado, defeituoso)
  - a descrição detalhada ou especificação técnica
  - o prazo de entrega

» Verifique, quando disponível, a reputação/qualificação do vendedor

» Fique atento ao comprar em *sites* de compras coletivas

- procure não comprar por impulso
- seja cauteloso e faça pesquisas prévias
- verifique atentamente as condições da compra

» Não compre caso desconfie de algo

AO REALIZAR A COMPRA

» Verifique as opções de pagamento oferecidas e escolha aquela que considerar mais segura

» Ao fornecer dados sensíveis via *e-mail* certifique-se de criptografar a mensagem

» Guarde as informações da compra, como comprovantes e número de pedido

- documente também outros contatos que você venha a ter
- essas informações podem ser muito importantes caso haja problemas futuros

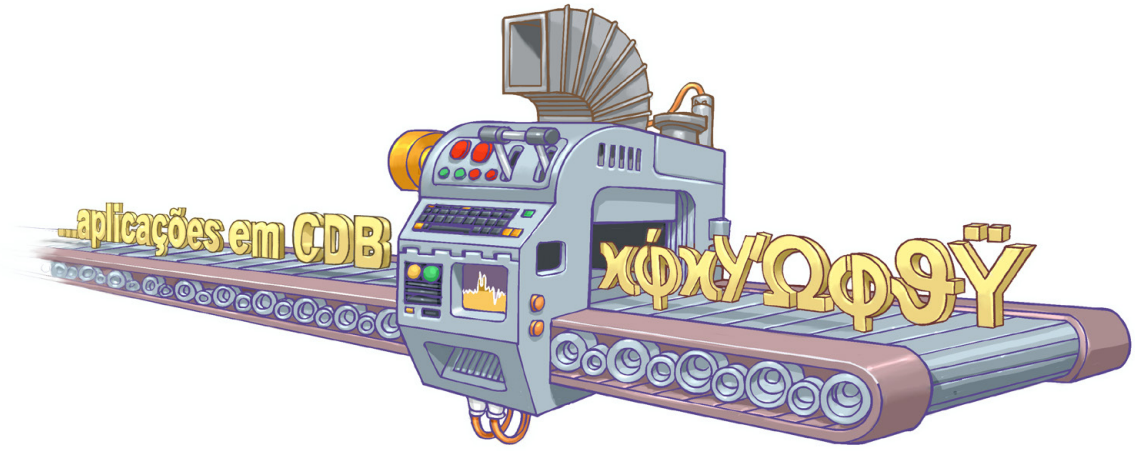
» Utilize sistemas de gerenciamento de pagamentos

- além de dificultarem a aplicação dos golpes, também podem impedir que seus dados pessoais e financeiros sejam enviados aos golpistas

» Certifique-se de usar conexões seguras. Alguns indícios são:

- o endereço do *site* começa com "https://"
- o desenho de um "cadeado fechado" é mostrado na barra de endereço
  - ao clicar sobre ele, são exibidos detalhes sobre a conexão/certificado digital em uso
- um recorte colorido (branco ou azul) com o nome do domínio do *site* é mostrado ao lado da barra de endereço (à esquerda ou à direita)
  - ao passar o *mouse* ou clicar sobre ele, são exibidos detalhes sobre a conexão/certificado digital em uso
- a barra de endereço e/ou o recorte são apresentados na cor verde e no recorte é colocado o nome da instituição dona do *site*

» Se tiver dúvidas entre em contato com a central de relacionamento da empresa



AO RECEBER O PRODUTO

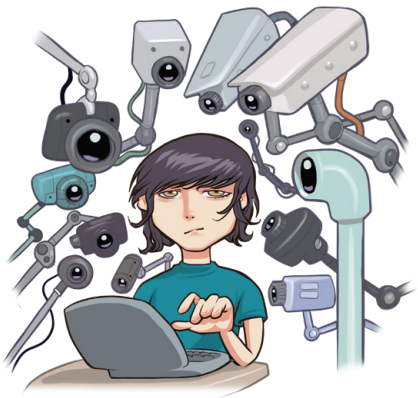
- Marque encontros em locais públicos caso a entrega seja feita pessoalmente
- Mesmo que o vendedor lhe envie o código de rastreamento fornecido pelos Correios, não use esta informação para comprovar o envio e liberar o pagamento
  - até ter o produto em mãos não há nenhuma garantia de que ele foi realmente enviado
- Antes de abrir a embalagem verifique se ela não está danificada
- Certifique-se de que o produto está de acordo com o que foi comprado
- Comente sobre a compra no *site*

EM CASO DE PROBLEMAS

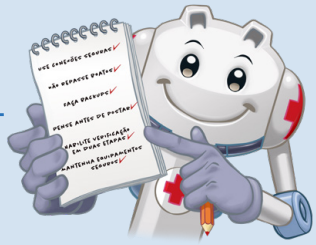
- Entre em contato com a empresa e verifique o ocorrido
- Se houver problemas de contato com o *site*/loja utilize *sites* de reclamações
- Utilize o Código de Defesa do Consumidor
  - denuncie o ocorrido ao PROCON da sua cidade, que poderá orientá-lo sobre a forma correta de agir

PROTEJA SEUS DADOS

- Cuidado com telefonemas solicitando informações pessoais
- Não responda mensagens de instituições com as quais você não se relacione
- Procure reduzir a quantidade de informações que possam ser obtidas sobre você
  - isso pode impedir, por exemplo, a criação de contas fantasma em seu nome
- Verifique periodicamente seu extrato bancário e do seu cartão de crédito
  - entre em contato imediatamente com o seu banco ou com a operadora do seu cartão de crédito caso detecte algum lançamento suspeito



SAIBA MAIS



» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **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: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

outubro / 2020