camara-e.net
Câmara Brasileira de Comércio Eletrônico

CARTILHA ANTIFRAUDE

CONSUMIDORES

CARTILHA ANTIFRAUDE PARA CONSUMIDORES

SUMÁRIO EXECUTIVO

CARTILHA ANTIFRAUDE PARA CONSUMIDORES

INTRODUÇÃO

BOAS PRÁTICAS CONTRA A FRAUDE ONLINE

Comprar via Internet é cômodo e prático, pois além da facilidade de pesquisar e comparar preços, aproveitar ofertas instantâneas e sazonais, produto é entregue diretamente no endereço escolhido.

Porém a compra online requer alguma precaução e certos cuidados, como:

- **Sem Contato, nem pensar**: Quanto mais fácil a localização de telefones, endereços e e-mail para entrar em contato com o comércio eletrônico, tirar dúvidas ou encaminhar problemas, mais confiável o site.
- **Meios de Pagamento na Internet**: Comprar apenas em Lojas Virtuais que disponibilizem serviços de Pagamento Online conhecidos. E evitar pagar a compra por meio de depósito ou boleto se a loja virtual tiver pouco tempo de mercado.
- **Bom Senso Futebol Clube**: Usar o Bom Senso! Ofertas milagrosas ou muito diferentes dos preços praticados no mercado podem trazer armadilhas para o comprador. Como sempre, o barato sai caro!
- **Lojas Idôneas**: Pesquisar sobre a loja e verifique se ela tem Razão Social e CNPJ ativos na Receita Federal - https://goo.gl/YpbRnc, além de endereço físico e formas de contato. Também vale pesquisar a empresa no Reclame Aqui e no Procon.
- **Segurança de Dados**: Verificar se a loja possui conexão de segurança nas páginas em que são informados os dados pessoais do cliente como nome, endereço, documentos, número do cartão de crédito, geralmente essas páginas são iniciadas por https:// e o cadeado ativado (ícone visualizado em uma das extremidades da página).
- **Dispositivos Seguros**: Utilizar wifi, computador ou smartphone seguros. Nunca faça compras virtuais por meio de computadores de outras pessoas ou usando redes públicas de wifi.
- **Recibo da Compra**: Salvar todos os passos da compra, inclusive o e-mail de confirmação.
-

OBSERVATÓRIO DE GESTÃO DE FRAUDE (OBSERVATORE.ORG)

CIÊNCIA EM CONSTRUÇÃO

Projeto capitaneado pelos comitês de Meios de Pagamento, Varejo Online e Gestão de Riscos da camara-e.net

Estudar a fraude é um processo de construção e desconstrução de saberes e conhecimentos científicos, simultaneamente disciplinar e interdisciplinar, contribuindo para a consolidação de um objeto científico de uma ciência ainda em construção: Gestão da Fraude. Observatório de Gestão de Fraude tem os seguintes objetivos:

- Agregar cidadãos e instituições interessadas em conhecerem a gestão de riscos na economia digital;
- Promover as boas práticas e cartilhas sobre a prevenção à fraude online;
- Contribuir para uma opinião pública esclarecida sobre as gestão de riscos;
- Constituir uma memória das práticas fraudulentas, enquanto instrumento para uma mais eficaz prevenção e detecção da fraude, uma regulação eficiente;
- Apoiar as organizações na prevenção da fraude;

  Promover o comércio eletrônico seguro no Brasil por meio do desenvolvimento dos meios de pagamento;
- Apresentar os principais golpes aplicados na Internet;
- Informar sobre os cuidados que consumidores devem tomar para proteger vida online;
- Fomentar o comércio eletrônico com transparência, ética e responsabilidade.

camara-e.net
Câmara Brasileira de Comércio Eletrônico

O PORQUÊ DA FRAUDE ONLINE

"Uma vez que atacar e fraudar serviços online de instituições bancárias ou comerciais é cada vez mais difícil, golpistas vêm concentrando esforços na exploração de fragilidades dos usuários, no caso, as lojas online"

IDENTIFICAR A FRAUDE ONLINE

Utilizando técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.

De posse dos dados das vítimas, os golpistas costumam efetuar transações financeiras, acessar sites, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas, entre outras atividades maliciosas.

Muitos dos golpes aplicados na Internet podem ser considerados crimes contra o patrimônio, tipificados como estelionato. Dessa forma, o golpista pode ser considerado um estelionatário.

A seguir são apresentados alguns dos principais golpes aplicados na Internet e alguns cuidados que o consumidor online deve tomar para se proteger.

CARTILHA ANTIFRAUDE

O Furto de Identidade, ou *identity theft*, é o ato pelo qual uma pessoa tenta se passar por outra, atribuindo-se uma falsa identidade, com o objetivo de obter vantagens indevidas.

Alguns casos de furto de identidade podem ser considerados como crime contra a fé pública, tipificados como falsa identidade.

Na Internet uma identidade pode ser furtada, caso alguém crie um perfil em seu nome em uma rede social, acesse sua conta de e-mail e envie mensagens se passando por você ou falsifique os campos de e-mail, fazendo parecer que ele foi enviado por você.

POSSÍVEIS DANOS

Caso a sua identidade seja furtada, você poderá arcar com consequências como perdas financeiras, perda de reputação e falta de crédito. Além disto, pode levar muito tempo e ser bastante desgastante até que você consiga reverter todos os problemas causados pelo impostor.

COMO SE PREVINIR?

A forma de impedir que sua identidade seja furtada é evitar que o impostor tenha acesso aos seus dados e às suas contas de usuário e senhas. É muito importante ser cuidadoso com as senhas, tanto ao usá-las quanto ao elaborá-las.

CARTILHA ANTIFRAUDE

A Fraude de Antecipação de Recursos, ou *Advance Fee Fraud*, é aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

A FRAUDE DO "ALMOÇO GRÁTIS"

Por meio do recebimento de mensagens eletrônicas ou do acesso a sites fraudulentos, a pessoa é envolvida em alguma situação ou história mirabolante, que justifique a necessidade de envio de informações pessoais ou a realização de algum pagamento adiantado, para a obtenção de um benefício futuro.

O **Golpe da Nigéria** é um dos tipos de fraude de antecipação de recursos mais conhecidos e é aplicado.

Recebe-se um e-mail convite para atuar como intermediário em uma transferência internacional de fundos, mas que para receber o valor absurdamente alto a que terá direito, precisa-se antecipar uma quantia para arcar com os custos;

O valor antecipado será perdido e os dados clonamos.

A fraude de antecipação de recursos possui diversas variações que, apesar de apresentarem diferentes discursos, assemelham-se pela forma como são aplicadas e pelos danos causados. Algumas destas variações são:

Loteria internacional: e-mail informando o sorteio de uma loteria internacional, mas que para receber o prêmio a que tem direito, precisa-se fornecer dados pessoais e informações bancárias.

Crédito fácil: e-mail contendo uma oferta de empréstimo ou financiamento com taxas de juros muito inferiores às praticadas no mercado.

Como se Previnir?

Uma mensagem relativa a este golpe, geralmente, possui características como:

- Oferece quantias astronômicas de dinheiro;
- Solicita sigilo nas transações;
- Solicita que você a responda rapidamente;
- Apresenta palavras como "urgente" e "confidencial" no campo de assunto;
- Apresenta erros gramaticais e de ortografia
- Deve-se sempre desconfiar de propostas muito tentadoras, pois não existe almoço grátis!

Phishing, phishing-scam ou phishing/scam, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social. Exemplo:

- Tenta-se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular;
- Tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, da instalação de programas maliciosos; e do preenchimento de formulários contidos na mensagem ou em páginas Web.

Como se Previnir?

- Ficar atento a mensagens, recebidas em nome de alguma instituição, que tentem induzir o fornecimento de informações, instalar/executar programas ou clicar em links;
- Evitar responder mensagens que apelem demasiadamente pela atenção e que, de alguma forma, façam ameaças caso não se execute os procedimentos descritos;
- Ser cuidadoso ao acessar links. Procurar digitar o endereço diretamente no navegador Web;
- Utilizar mecanismos de segurança, como programas antimalware, firewall pessoal e filtros anti-phishing.

Pharming é um tipo específico de phishing que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço de DNS (Domain Name System). Neste caso, quando você tenta acessar um site legítimo, o seu navegador Web é redirecionado, de forma transparente, para uma página falsa.

Não acessar o site de comércio eletrônico ou Internet Banking se o mesmo não utilizar conexão segura. Sites confiáveis de comércio eletrônico e Internet Banking sempre usam conexões seguras quando dados pessoais e financeiros são solicitados;

Sair do site caso, ao digitar uma URL, for redirecionado para outro site, o qual tenta realizar alguma ação suspeita, como abrir um arquivo ou tentar instalar um programa;

Sair do site caso o certificado apresentado não corresponda ao do site verdadeiro.

COMO SE PREVINIR?

Não acessar o site de comércio eletrônico ou Internet Banking se o mesmo não utilizar conexão segura. Sites confiáveis de comércio eletrônico e Internet Banking sempre usam conexões seguras quando dados pessoais e financeiros são solicitados;

Sair do site caso, ao digitar uma URL, for redirecionado para outro site, o qual tenta realizar alguma ação suspeita, como abrir um arquivo ou tentar instalar um programa;

Sair do site caso o certificado apresentado não corresponda ao do site verdadeiro.

CARTILHA ANTIFRAUDE

Um boato, *hoax*, ou simplesmente Fake News, consistem em uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental.

Por meio de uma leitura minuciosa de seu conteúdo, normalmente, é possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides.

Boatos podem trazer diversos problemas, tanto para aqueles que os recebem e os distribuem, como para aqueles que são citados em seus conteúdos.

Como se previnir?

Normalmente, os boatos se propagam pela boa vontade e solidariedade de quem os recebe, pois há uma grande tendência das pessoas em confiar no remetente, não verificar a procedência e não conferir a veracidade do conteúdo da mensagem. Para que você possa evitar a distribuição de boatos é muito importante conferir a procedência dos e-mails e, mesmo que tenham como remetente alguém conhecido, é preciso certificar-se de que a mensagem não é um boato.

Site falso de e-commerce

O QUE É?

- O golpista cria um site fraudulento, com o objetivo específico de enganar os possíveis clientes que, após efetuarem os pagamentos, não recebem as mercadorias.
- Para aumentar as chances de sucesso, o golpista costuma utilizar artifícios como: enviar spam, fazer propaganda via links patrocinados, anunciar descontos em sites de compras coletivas e ofertar produtos muito procurados e com preços abaixo dos praticados pelo mercado.

Como se previnir?

Fazer uma pesquisa de mercado, comparando o preço do produto exposto no site com os valores obtidos na pesquisa e desconfie caso ele seja muito abaixo dos praticados pelo mercado;

Pesquisar na Internet sobre o site, antes de efetuar a compra, para ver a opinião de outros clientes;

Acessar sites especializados em tratar reclamações de consumidores insatisfeitos, para verificar se há reclamações referentes a esta empresa.

CARTILHA ANTIFRAUDE

Pesquisa de reputação das Lojas Online - eficiente ferramenta para se evitar o risco, ao invés de mitigá-lo…

Conheça a reputação da empresa

Pesquisar o que as pessoas andam falando sobre a empresa. Sempre que se estiver com o pé atrás com algum comércio eletrônico, deve-se consultar a idoneidade do site nos órgãos de proteção ao consumidor como o Reclame Aqui. O Procon, por exemplo, mantém uma lista das empresas que recomenda evitar.

As redes sociais também são ótimas ferramentas para descobrir se existem reclamações em torno destes serviços e conhecer a opinião de outros consumidores. Nas fan pages das empresas no Facebook você encontra comentários de clientes e avaliações com estrelas. Além disso, você pode ver se a empresa responde os comentários deixados pelo público e se ela se importa em resolver os problemas que são relatados.

Boas e Más Indicações - Boca a Boca

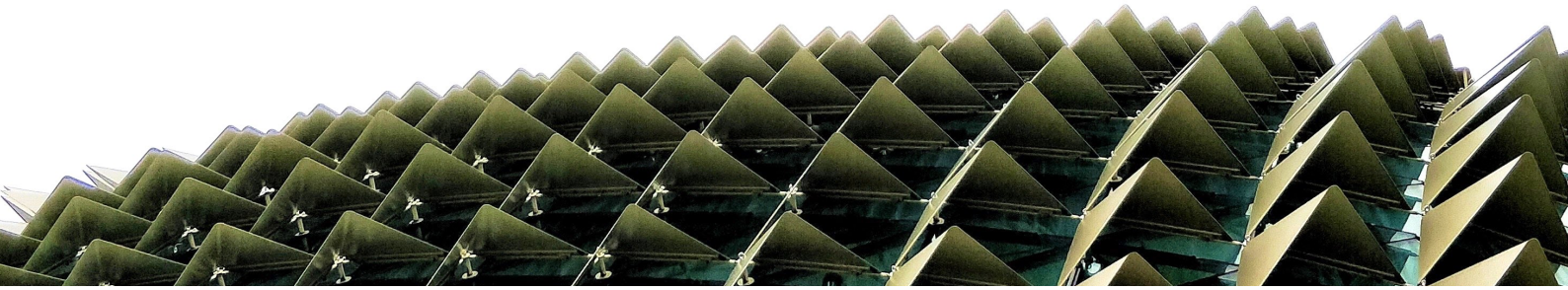
Não se deve pensar duas vezes antes de pedir indicações de parentes e amigos sobre um site específico, sobretudo daqueles que já têm o hábito de comprar pela internet.

Ler a Política do Site

A Política do Site deve esclarecer não só suas medidas de segurança como também seu sistema de trocas e devolução. Quanto mais confiante o consumidor estiver, melhor será sua compra e mais protegido estará o seu CPF.

Qualidade dos Textos do Site

Deve-se sempre procurar por pistas de golpes nos sites. Erros de português e fotos de má qualidade são bons indícios de sites que não são idôneos, construídos de forma amadora e com a finalidade exclusiva de tirar dinheiro das pessoas.



CARTILHA ANTIFRAUDE

NAVEGUE PROTEGIDO

Ferramentas de proteção da estação de trabalho e do navegador contra programas maliciosos e ameaças invasivas.

Os fraudadores farão de tudo para obter informações pessoais e os dados de cartões de crédito. Os golpes podem ser inteligentes e engenhosos, mas nunca o suficiente se soubermos como evitá-los. A proteção da estação de trabalho e do navegador contra programas maliciosos e ameaças invasivas exigem o seguinte:

Manter sempre Atualizado o Software de Proteção e Antivírus

A instalação de um bom antivírus está no topo da lista dos principais cuidados a serem tomados para proteger dispositivos, como computadores e smartphones, de ameaças virtuais.

Contudo, engana-se quem pensa que basta instalar o *software* de proteção e nunca mais atualizá-lo, acreditando que estará em segurança para sempre!

Ao contrário do que muitos pensam, a atualização do antivírus não serve deixar o computador mais lento, obrigando sua troca com maior frequência. Mas sim, para a aplicação de melhorias aperfeiçoadas pelos desenvolvedores. Nos *softwares* de proteção, a atualização é responsável por trazer defesas às novas ameaças que vão surgindo no mercado.

Criar Senhas Difíceis de Serem Descobertas

Muita gente coloca datas como senhas e isso é um tremendo erro. Pois datas são fáceis de serem descobertas por programas porque tem opções muito limitadas. Também não se deve usar palavras simples. O ideal é usar letras, números e caracteres especiais. Mas como vou lembrar da senha depois?

Basta, por exemplo, usar uma palavra conhecida e utilizar uma troca de letras por números ou símbolos. Veja os exemplos abaixo:

A = 4 ou @

E = 3 ou &

I = 1 ou !

O = 0 (zero)

S = 5 ou $

T = 7

CARTILHA ANTIFRAUDE

CONTINUE A NAVEGAR PROTEGIDO...

Ignorar e-Mails de Remetentes Desconhecidos e Evitar Clicar em Links Recebidos via e-Mail

Estes procedimentos ajudam a evitar a fraude baseada no Phishing.

Usar Bloqueador de Pop-ups

O Pop-Up, ou janela adicional que se abre junto ao site visitado, pode ser uma armadilha fraudulenta.

Assim, é melhor evitarmos os Pop-Ups.

Fazer Download de Arquivos Apenas de Sites Conhecidos

Arquivos baixados de origens desconhecidas podem trazer vírus e programas maliciosos junto aos mesmos.

Solicitar "Alertas de Transação Financeira"

Uma excelente forma de estar sempre informado sobre a utilização, autorizada ou não, do cartão de crédito é a solicitação de "Alertas de Transação Financeira" do banco. Assim, torna-se possível acompanhar as compras efetuadas com o cartão por email ou SMS.

Aviso de Viagem

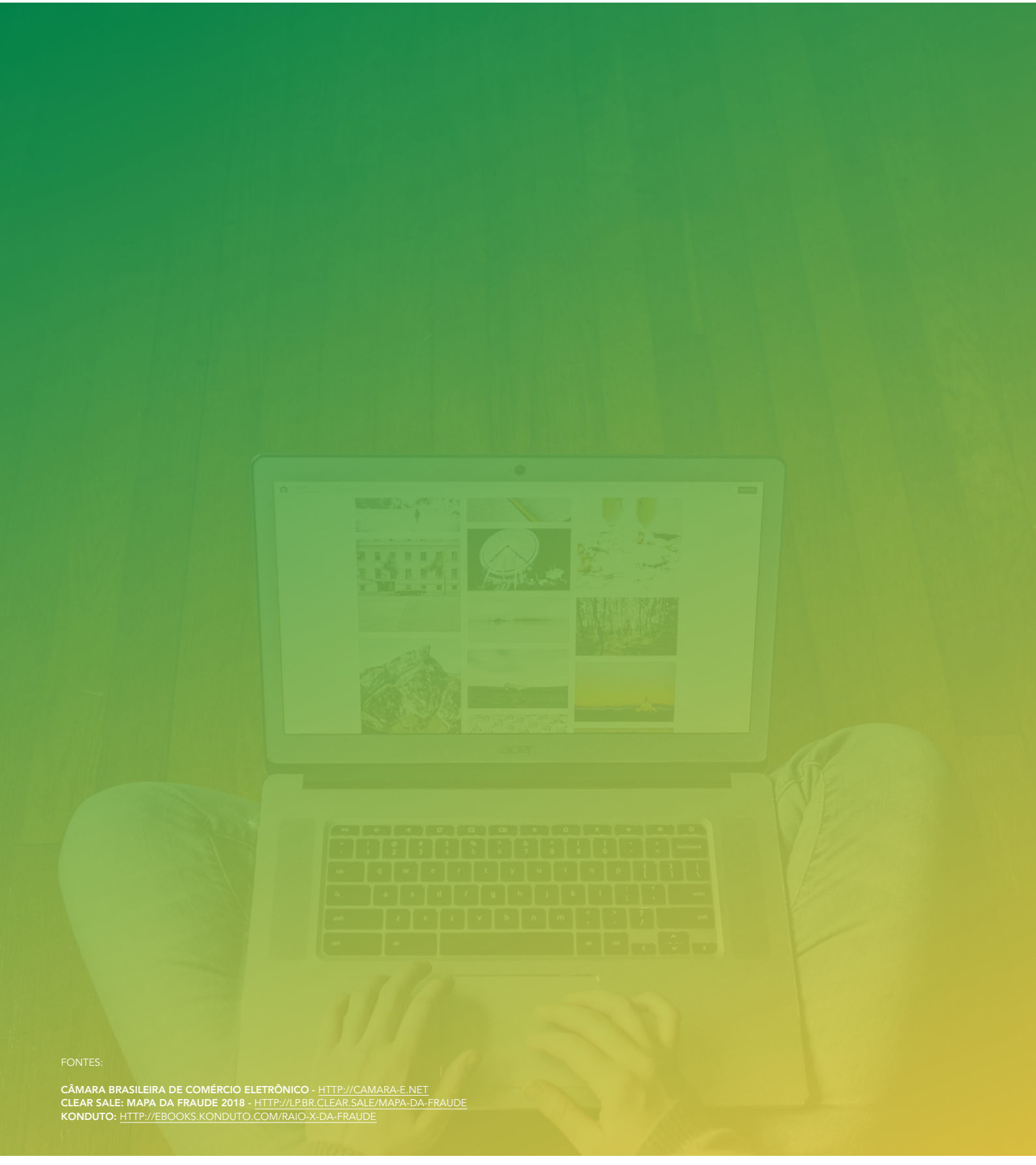
É de extrema importância a informação, ao banco emissor do seu cartão, sobre os países de destino e por quanto tempo se pretende viajar.

Assim, o banco saberá que uma transação efetuada no exterior pode ou não ser fraudulenta.

camara-e.net
Câmara Brasileira de Comércio Eletrônico

AV. ANGÉLICA, 2.503 – 5° ANDAR, SALA 56
SÃO PAULO/SP

T 55 (11) 3237-1102
W CAMARA-E.NET



FONTES:

CÂMARA BRASILEIRA DE COMÉRCIO ELETRÔNICO - HTTP://CAMARA-E.NET
CLEAR SALE: MAPA DA FRAUDE 2018 - HTTP://LP.BR.CLEAR.SALE/MAPA-DA-FRAUDE
KONDUTO: HTTP://EBOOKS.KONDUTO.COM/RAIO-X-DA-FRAUDE