ENJOY SAFER TECHNOLOGY™

12 Dicas para realizar compras online com Segurança

As compras online chegaram no mercado há muito tempo e, pelo visto, para ficar. Com elas também despertaram os desejos dos cibercriminosos de se apropriarem do dinheiro das transações online. Devido aos ataques de phishing às redes abertas de WiFi é importante conhecer os riscos a que estamos expostos. A ESET preparou estes conselhos para manter sua segurança, da compra até a confirmação de seu pedido.

1 TENHA CUIDADO COM LOJAS DESCONHECIDAS

Pode ser que ao navegar na internet uma boa oferta apareça em um site de viagens ou uma promoção relâmpago em lojas online. Mas antes de aproveitar as oportunidades devemos nos fazer uma pregunta "Confio neste negócio? ".

Por que devemos nos questionar? A resposta é simples, existe uma grande quantidade de sites web sem segurança ou inclusive maliciosos, portanto, compras só devem ser efetuadas quando realmente estamos confiantes em compartilhar dados como cartão de crédito ou débito. Por exemplo, no passado houveram vendedores online que receberam pagamentos mas nunca entregaram as mercadorias ou enviaram produtos com defeito e sem nenhuma garantia.

Existem casos em que o negócio pode ser respeitado porém seu site web pode ser vulnerável, vários sites de e-commerce têm sido infectados com malware nos últimos anos. Não é incomum que alguns destes sites tenham um certificado SSL inválido, aumentando as chances de que um terceiro se faça passar por um site legítimo.

Assim mesmo, alguns destes sites podem guardar as senhas dos clientes em texto simples ao invés de criptografá-las como recomendado. Esta é a má notícia, se ocorrer um ataque, os cibercriminosos podem conseguir acesso as bases de dados da empresa, e dessa forma, ingressar nas contas dos usuários sem a necessidade de romper a criptografia ou ter que adivinhar as senhas.

Portanto é muito importante que preste atenção, revise as políticas de privacidade e os termos e condições de vendas antes de comprar algo em uma loja que não conhece. Caso não tenha se convencido da veracidade da loja visitada sempre é possível comprar em outro lugar.

---

2 PREPARE-SE PARA OFERTAS DE PHISHING

Os atacantes de Phishing sempre tentam atrair as vítimas desprevenidas com um email ou um link atrativo, especialmente, nas épocas de festas em que os compradores estão em busca de boas ofertas.

Os cibercriminosos poderiam, por exemplo, enviar um email prometendo um desconto em uma loja conhecida ou para um pacote especial de férias. Além disso, também podem tentar com links chamativos no Twitter ou Facebook.

Para evitar cair em um golpe de phishing, preste atenção quando receber e-mails ou mensagens de pessoas que não conhece, revise o conteúdo cuidadosamente para observar alguma inconsistência. E ainda, se tiver dúvidas, busque a oferta ou a loja procurando em um navegador conhecido.

3 UTILIZE RESPEITADOS MÉTODOS DE PAGAMENTO (E SEGUROS)

Onde quer que efetue suas compras online, preste atenção as formas de pagamento e como são seguro é, se irá pagar com cartão de crédito, o ideal é buscar lojas que usam plataformas de pagamentos reconhecidas e confiáveis.

---

4 UTILIZE HTTPS

Verifique se a loja possui conexão de segurança nas páginas em que são informados dados pessoais do cliente como nome, documentos, número do cartão de crédito e endereço, geralmente essas páginas são iniciadas por https:// e o cadeado é ativado (ícone amarelo em uma das extremidades da página). Clique no cadeado e observe se a informação do certificado corresponde ao endereço na barra de navegação do computador.

---

5 CUIDADO NO FACEBOOK

Facebook está se tornando uma ferramenta de transações e negociações de bens e serviços, não significando que está livre de perigos. Esta rede social às vezes apresenta anúncios de sites web desconhecidos ou suspeitos, oferecendo links a outros sites que não possuem certificados digitais ou que são inválidos. Devemos evitar compartilhar dados de Faturamento através de mensagens direta, já que não sabemos quem terá acesso as contas do Facebook do outro usuário.

---

6 COMPRE SEMPRE CONECTADO A REDES CONFIÁVEIS E EVITE WI-FI ABERTO

Devemos pensar cuidadosamente não só na forma como comprar online, mas também, onde efetuará a aquisição: em sua residência ou em uma rede Wi-Fi pública sem segurança?

É surpreendente a quantidade de pessoas que compartilham qualquer tipo de informação através de conexões desprotegidas como em um café ou um hotel. Isto é perigoso pois os cybecriminosos poderiam fazer um ataque do tipo Man-in-the-Middle, revisando o tráfego dos usuários desprevenidos e assim roubar seus dados pessoais.

Ao comprar em sua residência você não estará totalmente imune a um ataque, porém os riscos são menores se tiver uma solução de segurança, atualização de aplicativos e sistema operacional de seu equipamento. Além disso, você poderá melhorar sua segurança ao desabilitar os complementos e pluggins antes de fazer suas compras, já que isto reduz as possibilidades de acessos não autorizados aos dados de seu pedido.

7 UTILIZE SENHAS FORTES OU UM ADMINISTRADOR DE SENHAS

Estudos mostram que as pessoas com mais de 20 contas online, muito ativas na internet, têm mais chances de reutilizar senhas. Isto, de acordo a um relatório de Javelin Strategy and Research, torna-as 37% mais propensas a ter alguma de suas contas invadidas.

Ao utilizarmos senhas fortes, que incluem letras maiúsculas e minúsculas, números e símbolos nos mantemos mais seguros. Além disso, devemos mudar as senhas para cada uma das contas, evitando utilizar senhas iguais duas vezes. Parece difícil esta tarefa e, por isso, talvez sugerimos o uso de um gerenciador de senhas.

---

8 SEJA INTELIGENTE COM SEU TELEFONE

Se está efetuando compras de um smartphone ou tablet, você pode pensar que está imune a qualquer ataque, o que é um equivoco. Os cibercriminosos estão constantemente direcionando ataques em dispositivos móveis, por isso é necessário que sua segurança nestes equipamentos seja tão boa como em seu PC ou seu Mac.

Faça algumas coisas para reduzir as possibilidades de que seja atacado. Para começar, as compras devem ser realizadas somente de apps baixados de repositórios de aplicações oficiais. As lojas de terceiros são menos comuns , todavia, podem conter aplicações maliciosas desenvolvidas para roubar seus dados pessoais.

Também é possível remover as aplicações que não usa e desligar as redes sem fio quando está comprando em locais públicos, utilizando somente a conexão de dados do celular. Este último é para prevenir um ataque, que poderia fazer com que os cibercriminosos o encaminhem a se conectar em falsos pontos de Wi-Fi , com um nome forte e conhecido, roubando assim suas credenciais e seus dados bancários.

Também desative o Bluetooth e o Wi-Fi para minimizar as chances de que um local de vendas envie um spam.

---

9 NÃO GUARDE AS INFORMAÇÕES DE SEU CARTÃO DE CRÉDITO PARA COMPRAS FUTURAS

Para comprar on-line você deve usar seus cartões de crédito, que não está apenas desconectado de suas contas bancárias, mas também, estão assegurados contra cobranças fraudulentas. Você também vai correr menos risco de ser vítima de roubo de identidade e têm mais chance de conseguir um reembolso, caso seja comprovada atividades suspeitas ou ilícitas.

Também, deverá considerar ter um cartão de crédito somente para usar em compras online. A maioria dos bancos oferecem cartões de crédito com limites de dinheiro e período de tempos ajustáveis que facilitam a proteção contra cibercriminosos.

10 APRENDA OS CONCEITOS BÁSICOS

Pode parecer muito repetitivo mas antes de comprar on-line você deve se certificar de que você está seguro.

Isso envolve uma série de ações básicas, como instalar uma solução de segurança e atualizar regularmente seus programas e aplicações. Além disso, deve garantir que senhas sejam adicionadas a suas telas de bloqueio inicial, assim como um PIN em seu smartphone. Considere a ideia de ter um gerenciador de senhas, implementar um duplo fator de autenticação e talvez uma VPN para navegar com mais privacidade.

11 UM PC OU DOIS

Quanto mais computadores, tablets e dispositivos móveis tiverem acesso a informação de seu cartão de crédito mais estará exposto, correndo o risco de ser vítima de uma fraude. Tente limitar suas compras online para um ou dois dispositivos.

12 SALVE DADOS DO PEDIDO

Salve ou imprima todos os passos da compra, inclusive e-mails de confirmação.