

OUCH!

O boletim mensal de conscientização de segurança para você

Comprando Online com Segurança

Visão geral

A temporada de festas está chegando para muitos de nós e em breve milhões de pessoas estarão buscando comprar os presentes ideais. Muitos de irão comprar online em busca de ótimas ofertas e evitar multidões barulhentas. Infelizmente, os atacantes cibernéticos também estarão ativos, criando sites de compras falsos e utilizando outras táticas para enganar as pessoas. Neste boletim informativo, explicamos como você pode fazer compras online com segurança e evitar tornar-se uma vítima.

Lojas Online Falsas

Os atacantes cibernéticos criam lojas online falsas que imitam a aparência de sites reais ou usam os nomes de lojas ou marcas conhecidas. Ao buscar as melhores ofertas online, você pode se deparar com um desses sites falsos. Ao comprar nesses sites, você pode acabar com itens falsificados ou roubados e, em alguns casos, suas compras podem nunca ser entregues. Siga os passos a seguir para se proteger das lojas online falsas:



Sempre que possível, compre nas lojas online que você já conhece, confia e já comprou anteriormente. Adicione aos favoritos as lojas online que você já visitou e confia.



Fique atento a preços significativamente melhores do que aqueles que você vê nas principais lojas online. Se a oferta parecer boa demais para ser verdade, pode ser falsa.



Suspeite se o site se parece ao que você usou antes, mas o nome do domínio do site ou o nome da loja está um pouco diferente. Por exemplo, você pode estar acostumado a fazer compras na Amazon, cujo endereço do site é www.amazon.com, mas terminar comprando em um site falso com um endereço semelhante, onde a letra “o” foi substituída pelo número 0.



Digite o nome da loja online ou o endereço do site em um motor de pesquisa para conferir o que os outros disseram sobre isso. Procure termos como “fraude”, “golpe”, “nunca mais” e “falso”.



Use uma senha exclusiva para cada conta. Não consegue se lembrar de todas suas senhas? Considere armazenar todas elas em um gerenciador de senhas.

Golpistas em Sites Legítimos

Mantenha-se precavido, mesmo quando fizer compras em sites confiáveis. As grandes lojas online normalmente oferecem produtos vendidos por diferentes indivíduos ou empresas que podem ter intenções fraudulentas. Esses destinos online são como mercados do mundo real, em que alguns vendedores são mais confiáveis do que outros. Verifique a reputação de cada vendedor antes de fazer o pedido. Desconfie de vendedores que são novos na loja online ou que vendem itens a preços excepcionalmente baixos. Revise a política da loja online sobre compras de terceiros. Em caso de dúvida, compre os itens vendidos diretamente pela loja online, não pelos vendedores terceirizados que participam de seu mercado online.

Pagamentos Online por Compras

Revise periodicamente os extratos do seu cartão de crédito para identificar cobranças suspeitas. Se possível, ative a opção de notificação por e-mail, sms ou aplicativo sempre que for feita uma cobrança no seu cartão de crédito. Se você achar alguma atividade suspeita, ligue imediatamente para sua empresa do cartão de crédito e denuncie. Evite usar cartões de débito sempre que puder. Os cartões de débito retiram dinheiro diretamente de sua conta bancária; se a fraude for cometida, você terá muito mais dificuldade em recuperar seu dinheiro. Outra opção é usar serviços de pagamento conhecidos, como PayPal, para compras online, que não exigem a divulgação do número de seu cartão de crédito ao fornecedor. Por último, considere usar um cartão-presente para as compras online.

Só porque uma loja online tem uma aparência profissional muito bem feita, não significa que seja legítima. Se o site deixa você desconfortável, não o use. Em vez disso, acesse um site conhecido em que você pode confiar ou já usou com segurança anteriormente. Você pode não encontrar essa oferta incrível, mas é muito mais provável que acabe com um produto legítimo e evite ser enganado.

Editor convidado

Lenny Zeltser é Diretor de Segurança da Informação da Axonius e instrutor sênior e autor do Instituto SANS. Você pode segui-lo no Twitter [@lennyzeltser](https://twitter.com/lennyzeltser) e ler seu blog acessando zeltser.com.



Recursos

Engenharia Social: <https://www.sans.org/u/Uz7>

Enganando Você Através das Mídias Sociais: <http://www.sans.org/u/X7p>

Simplificando as senhas: <http://www.sans.org/u/Xu9>

OUCH! é publicado pela SANS Security Awareness e é distribuído sob [a licença Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Você é livre para distribuir este boletim informativo ou usá-lo em seu programa de conscientização, desde que você não modifique o boletim informativo. Para traduções ou mais informações, entre em contato com www.sans.org/security-awareness/ouch-newsletter. Conselho Editorial: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley