OUCH! Novembro de 2021

Compras online com segurança

A época de festas está chegando. Em breve, milhões de pessoas estarão procurando os presentes perfeitos e muitos de nós farão compras online. Infelizmente, os cibercriminosos também estarão ativos, criando sites de compras falsos e outros golpes de compras online para roubar suas informações ou dinheiro. Aprenda como você pode encontrar boas ofertas sem se tornar uma vítima.

Lojas online falsas

Os criminosos criam lojas online falsas que imitam a aparência de sites reais ou usam nomes de lojas ou marcas famosas. Ao pesquisar as melhores ofertas online, você pode se deparar com algum desses sites falsos. Ao comprar nesses sites, você pode acabar com itens falsificados ou roubados, ou suas compras podem nunca ser entregues. Execute as seguintes etapas para se proteger:

- Quando possível, compre em lojas online que já conhece, confia e com as quais já é cliente. Marque essas lojas online nos seus favoritos.
- Suspeite de anúncios ou promoções em mecanismos de pesquisa ou redes sociais que sejam significativamente inferiores aos que você vê nas principais lojas online. Se uma oferta parecer boa demais para ser verdade, pode ser um golpe.
- Tenha cuidado com sites que não têm como contatá-los, formulários de contato quebrados, ou use endereços de e-mail pessoais.
- Desconfie se um site se parecer com um que você já usou, mas o nome de domínio do site ou o nome da loja for diferente. Por exemplo, você pode estar acostumado a fazer compras na Amazon, cujo endereço do site é www.amazon.com, mas acaba em um site falso que parece semelhante, mas tem o endereço do site www.amazonshoppers.com.
- Digite o nome da loja online ou seu endereço da web em um mecanismo de busca para verificar o que outras pessoas comentaram sobre ela. Procure termos como "fraude", "golpe", "nunca mais" e "falso".
- Proteja suas contas online usando uma senha forte e exclusiva para cada uma delas. Não consegue se lembrar de todas suas senhas? Considere amazená-las todas elas em um gerenciador de senhas.

Golpistas em sites legítimos

Mantenha-se alerta, mesmo ao fazer compras em sites confiáveis. As lojas online normalmente oferecem produtos vendidos por terceiros- diferentes indivíduos ou empresas- que podem ter intenções fraudulentas. Esses destinos online são como os mercados do mundo real, nos quais alguns vendedores são mais confiáveis do que outros.

- Verifique a reputação de cada vendedor antes de fazer o pedido, lendo suas avaliações.
- Desconfie de vendedores que são novos na loja online, não têm avaliações ou que vendem itens a preços incrivelmente baixos.

- Consulte a política da loja online sobre compras de terceiros.
- Em caso de dúvida, compre itens vendidos diretamente pela loja online, não por terceiros que participam de seu mercado online.
- Mesmo com fornecedores legítimos, certifique-se de entender a garantia do vendedor e as políticas de devolução antes de fazer sua compra.

Pagamentos online para compras

Consulte frequentemente os extratos do seu cartão de crédito para identificar cobranças suspeitas. Se possível, ative a opção de notificá-lo por e-mail, texto ou aplicativo quando uma cobrança for feita. Se você encontrar qualquer atividade suspeita, informe a sua empresa de cartão de crédito imediatamente. Use cartões de crédito em vez de cartões de débito para pagamentos online. Cartões de débito tiram dinheiro diretamente da sua conta bancária; se uma fraude for cometida, você terá muito mais dificuldade em conseguir seu dinheiro de volta. Os serviços de pagamento eletrônico ou e-wallets, como o PayPal, também são uma opção mais segura para compras online, pois não exigem que você divulgue o número do cartão de crédito ao fornecedor. Evite sites que só aceitam pagamentos em criptomoedas ou exigem métodos de pagamento desconhecidos.

Só porque uma loja online tem uma aparência profissional não significa que ela seja legítima. Se o site não parecer confiável, não o use. Em vez disso, acesse um site conhecido no qual pode confiar ou que já usou com segurança. Você pode não encontrar essa oferta incrível, mas é muito mais provável que evite ser enganado.

Editor convidado

Mark Orlando é um líder de segurança que defendeu redes no Pentágono, na Casa Branca e em vários clientes do setor privado. Hoje ele é o CEO e co-fundador da empresa de segurança cibernética Bionic, e é instrutor e autor de cursos no SANS Institute. [Twitter: @markaorlando]

Recursos

Simplificando as senhas: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Engenharia Social: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Mensagens/Ataques de Smishing: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
Golpes por meio das redes sociais: https://www.sans.org/newsletters/ouch/scamming-you-through-social-media/

Traduzido para a Comunidade por: David Boldrin