OUCH! | Novembro de 2015

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

- Lojas Online Falsas
- Seu Computador / Dispositivo Móvel
- Seu Cartão de Crédito

Fazendo compras na Internet com Segurança

Época para ser Cauteloso

A época das férias está perto e em breve nós e milhões de pessoas ao redor do mundo estaremos procurando as lembranças perfeitas. Muitos de nós vamos escolher comprar pela Internet para tentar uma boa promoção e evitar longas filas e multidões impacientes. Infelizmente essa também é a época do ano favorita para os criminosos cometerem fraudes online ou financeiras. Nesse mês nós explicamos os perigos de fazer compras online e as formas de se proteger.

Editor Convidado

Jonathan Homer (**@JonathanLHomer**) é um líder reconhecido na indústria de conscientização de Segurança Cibernética e atuante tanto no governo quanto no setor privado. Jon é especialista em engajamento de audiência e técnicas de treinamento de ponta.

Lojas Online Falsas

Enquanto muitas lojas online são legítimas, algumas não são, elas são páginas falsas feitas por criminosos. Os criminosos criam essas páginas falsas copiando a aparência ou usando o mesmo nome de lojas famosas. Então eles as usam para enganar pessoas à procura do melhor negócio possível. Quando você procura na Internet o menor preço possível, você pode ser direcionado para uma dessas páginas falsas.

Ao selecionar uma loja virtual para comprar um produto, seja cauteloso com páginas de Internet promovendo preços muito mais baratos que os outros, ou produtos esgotados em todas as lojas do país. A razão do produto deles estar tão barato ou disponível é ele não ser legitimo, ser um item falsificado ou roubado ou ainda, em alguns casos, um golpe onde você nunca receberá nada. Proteja-se fazendo o seguinte:

- Verifique se a página de Internet tem um endereço de e-mail legítimo e um número de telefone para atendimento às vendas ou atendimento a questões técnicas. Se a página parecer suspeita, ligue e fale com uma pessoa;
- Procure por sinais óbvios de aviso como gramática e escrita pobres;
- Suspeite seriamente se uma página aparentar ser uma réplica exata de uma loja conhecida que tenha usado no passado, mas que tenha o endereço de Internet ou da loja ligeiramente diferente. Por exemplo, você pode ter utilizado a página https://amazon.com para compras online. Mas suspeite se de repente estiver utilizando uma página dizendo-se a Amazon, com o endereço http://store-amazon.com;
- Digite o nome da loja ou sua URL (endereço de Internet) em uma página de busca e veja o que outras pessoas disseram sobre esse endereço no passado. Procure termos como “golpe”, “nunca mais” ou “falso”. A falta de histórico ou

Fazendo compras na Internet com Segurança

testemunho também é um mal sinal pois indica que a página é muito nova;

Lembre-se: só por que um site parece profissional não significa que é legítimo. Se alguma coisa no site chamar sua atenção, dedique um tempo para investigar. Se não estiver confortável com o site, não utilize. Ao contrário, procure uma loja de nome, em que possa confiar ou onde tenha comprado com segurança no passado. Você pode não encontrar tantos grandes negócios ou aqueles super descontos mas terá mais chances de receber um produto legítimo e ter seu perfil de crédito intacto ao final.

Mantenha-se protegido online comprando somente de lojas conhecidas e de boa reputação.

Seu Computador / Dispositivo Móvel

Além de comprar em um website legitimo, certifique-se de ter seu computador ou dispositivo móvel seguro. Criminosos cibernéticos vão tentar infectar seus dispositivos para que possam obter suas informações bancárias, de cartão de crédito e senhas. Siga os seguintes passos para manter seus dispositivos seguros:

- Se você tem crianças em casa, considere a possibilidade de ter dois equipamentos, um para seus filhos e outro para os adultos. Crianças são curiosas e fuçadoras de tecnologia, por isso são mais propensas a infectar seus computadores. Ao utilizar um equipamento ou tablet separado e dedicado para transações de bancos e compras online, você reduz a chance de se infectar. Se os dispositivos dedicados não são uma opção, então tenha contas separadas no computador compartilhado e certifique-se de que seus filhos não têm privilégios administrativos;
- Só use redes wireless (Wi-Fi) que você gerencie, como sua rede residencial, ou redes em que você confie, quando precisar fazer transações bancárias. Utilizar redes Wi-Fi públicas como as de lanchonetes pode ser ótimo para ler notícias mas não para acessar sua conta bancária;
- Instale sempre as últimas atualizações e use um antivírus atualizado. Isso dificulta bastante o trabalho de um criminoso cibernético que queira infectar seu equipamento;

Seu Cartão de Crédito

Monitore o extrato do seu cartão de crédito para identificar contas suspeitas. É importante acompanhá-lo regularmente, no mínimo uma vez ao mês. Algumas operadoras de cartão de crédito oferecem a opção de informá-lo por e-mail ou mensagens de texto (Torpedos ou SMS) toda vez que uma compra é feita no cartão, ou quando elas excedem um determinado limite. Outra opção é ter um cartão de crédito dedicado para compras pela Internet pois se ele for comprometido você poderá trocá-lo facilmente sem gerar impacto às suas outras compras com cartão. Se você achar que houve uma fraude no seu cartão, ligue

Fazendo compras na Internet com Segurança

para sua operadora de cartão de crédito imediatamente e explique a situação. Essa é uma boa razão para utilizar cartões de crédito ao invés de débito, nas compras online. Cartões de débito sacam o dinheiro diretamente na sua conta bancária e se uma fraude for detectada, será muito mais difícil obter seu dinheiro de volta.

Por último, existe tecnologia que permite fazer um pagamento sem expor o número do seu cartão de crédito. Podem ser cartões de crédito que geram números de cartão únicos a cada compra online (verifique com sua operadora ou banco) ou use serviços de pagamento conhecidos como PayPal, que não requer a divulgação do seu número de cartão de crédito para o vendedor. No Brasil temos também a opção de utilizar cartões de crédito pré-pagos, que podem ser carregados com o valor exato da compra e evitar o comprometimento de valores acima daquele montante.

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em http://www.securingthehuman.org.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

Recursos

Cinco Passos Para Ficar Seguro:	https://www.securingthehuman.org/ouch/2014#october2014
Protegendo Sua Rede Domestica (de casa):	https://www.securingthehuman.org/ouch/2014#january2014
Protegendo seu novo Tablet:	https://www.securingthehuman.org/ouch/2013#december2013
Dica de Segurança do Dia do SANS (em Inglês):	https://www.sans.org/tip_of_the_day.php

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser