SANS SECURITY AWARENESS

OUCH! | November 2017

The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- Fake Online Stores
- Your Computer/Mobile Device
- Your Credit Card

Shopping Online Securely

Overview

The holiday season is nearing for many of us, and soon millions of people around the world will be looking to buy the perfect gifts. Many of us will choose to shop online in search of great deals and to avoid long lines and impatient crowds. Unfortunately, this is also the time of year many cyber criminals create fake shopping websites to scam and steal from others. Below, we explain the risks of shopping online and how to get that amazing deal safely.

Guest Editor

Lenny Zeltser builds security products at Minerva Labs and teaches malware combat at SANS Institute. Lenny is active on Twitter as **@lennyzeltser** and writes a security blog at **zeltser.com**.

Fake Online Stores

While many online stores are legitimate, there are some fake websites set up by cyber criminals. Criminals create these fake websites by replicating the look of real sites or using the names of well-known stores or brands. They then use these fraudulent websites to prey on people who are looking for the best deal possible. When you search online for the absolute lowest prices, you may find yourself directed to one of these fake websites. When selecting a website to make a purchase, be wary of websites advertising prices dramatically cheaper than anywhere else or offering products that are sold out nationwide. The reason their products are so cheap or available is because what you will receive is not legitimate, may be counterfeit or stolen, or may never even be delivered. Protect yourself by doing the following:

- When possible, purchase from websites that you already know, trust, and have done business with previously.
- Verify the website has a legitimate mailing address and a phone number for sales or support-related questions. If the site looks suspicious, call and speak to a human. If you can't get a hold of someone to talk to, that is the first big sign you are dealing with a fake website.
- Look for obvious warning signs, like deals that are obviously too good to be true or poor grammar and spelling.

Shopping Online Securely

- Be very suspicious if a website appears to be an exact replica of a well-known website you have used in the past, but its domain name or the name of the store is slightly different. For example, you may be used to shopping online at Amazon, whose website is https://www.amazon.com. But be very suspicious if you find yourself at websites pretending to be Amazon, such as http://store-amazoncom.com.
- Type the store's name or URL into a search engine and see what other people have said about the website in the past. Look for terms like "fraud," "scam," "never again," or "fake." A lack of reviews can also be a sign indicating that the website is very new and might not be trustworthy.
- Before purchasing any items, make sure your connection to the website is encrypted. Most browsers show a connection is encrypted by having a lock and/or the letters HTTPS in green right before the website's name.

Protect yourself online by shopping only at trusted websites with an established reputation.

Remember, just because the site looks professional does not mean it's legitimate. If you aren't comfortable with the website, don't use it. Instead, find a well-known website you can trust or have safely used in the past. You may not find that absolutely amazing deal, but you are much more likely to end up with a legitimate product and avoid having your personal and financial data stolen.

Your Computer/Mobile Device

In addition to shopping at legitimate websites, you want to ensure your computer or mobile device is secure. Cyber criminals will try to infect your devices so they can harvest your bank accounts, credit card information, and passwords. Take the following steps to keep your devices secured:

- If you have children in your house, consider having two devices, one for your kids and one for the adults. Kids are curious and interactive with technology; as a result, they are more likely to infect their own device. By using a separate computer or tablet just for online transactions, such as online banking and shopping, you reduce the chance of becoming infected.

Shopping Online Securely

- Always install the latest updates and run up-to-date anti-virus software. This makes it much harder for a cyber criminal to infect your device.

Your Credit Card

Regularly review your credit card statements to identify suspicious charges, especially after you used your cards to make many online purchases or used a new site. Some credit card providers give you the option of notifying you by email or text messages every time a charge is made to your card or when charges exceed a set amount. Another option is to have one credit card just for online purchases. That way, if it is compromised, you can easily change the card without impacting any of your other payment activities. If you believe fraud has been committed, call your credit card company right away. This is also why you want to use credit cards for all online purchases and avoid using debit cards whenever possible. Debit cards take money directly from your bank account, so if fraud has been committed, it can be far more difficult to get your money back. Finally, consider using credit cards that generate a unique card number for every online purchase, gift cards, or well-known payment services, such as PayPal, which do not require you to disclose your credit card number to the vendor.

Subscribe to OUCH!

Get the OUCH! security awareness newsletter every month for free, in the language of your choice. Simply subscribe at https://securingthehuman.sans.org/ouch.

Resources

Social Engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Four Steps to Staying Secure:	https://securingthehuman.sans.org/ouch/2016#october2016
Securing Your Home Network:	https://securingthehuman.sans.org/ouch/2016#february2016
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

License