The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

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

Shopping Online Securely

'Tis the Season to Be Cautious

The holiday season is close upon 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 a great deal and avoid long lines and impatient crowds. Unfortunately, this is also a criminal's favorite time of the year to commit online or financial fraud. This month, we explain the dangers of shopping online and ways you can protect yourself.

Guest Editor

Jonathan Homer (**@JonathanLHomer**) is a recognized leader in the Cyber Security Awareness industry and is active within both the government and private sectors. Jon specializes in audience engagement and leading edge training techniques.

Fake Online Stores

While most online stores are legitimate, some are not; they are fake websites set up by criminals. Criminals create these fake websites by copying the look of or using the name of well-known stores. They then use these websites to prey on people who are looking for the best deal possible. When you search online for the absolute lowest prices, you may be directed to one of these fake websites.

When selecting a website to purchase a product, be wary of websites advertising prices dramatically cheaper than anywhere else or offering products sold out nationwide. The reason their products are so cheap or available is because what you will receive is not legitimate, is a counterfeit or stolen item or, in some cases, you never even receive anything. Protect yourself by doing the following:

- 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.
- Look for obvious warning signs like poor grammar and spelling.
- Be very suspicious if a website appears to be an exact replica of a well-known website you have used in the past, but the website domain name or the name of the store is slightly different. For example, you may be used to going to

© SANS Institute 2015

Shopping Online Securely

the website https://www.amazon.com for all of your Amazon shopping. But be very suspicious if you were to find yourself at a website pretending to be Amazon with the URL http://www.store-amazon.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 "scam," "never again" or "fake." A lack of reviews is also not a good sign, as it indicates that the website is very new.

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 something about the site sets off warning bells, take time to investigate. 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 quite as great a deal or find that hot ticket item, but you are much more likely to end up with a legitimate product and a clean credit report.

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. If separate devices are not an option, then have separate accounts on the shared computer and ensure your kids do not have administrative privileges.
- Only connect to wireless networks you manage, such as your home network, or networks you know you can trust when making financial transactions. Using public Wi-Fi networks, such as at your local coffee shop, may be great for reading the news, but not for accessing your bank account.

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

Keep an eye on your credit card statements to identify suspicious charges. You should review your statements regularly, at a minimum at least once per month. 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 and explain the situation. This is also why credit cards are better for online purchases than debit cards. Debit cards take money directly from your bank account, and if fraud has been committed, it can be far more difficult to get your money back.

Finally, there is new technology that enables you to pay without exposing your credit card number. Consider credit cards that generate a unique card number for every online purchase, or use well-known payment services, such as PayPal, which do not require you to disclose your credit card number to the vendor.

Video of the Month

Be sure to check out our free resources including posters, daily tips and Video of the Month. This month, we're covering Cloud Computing and Protected Health Information (PHI). View the video at https://www.securingthehuman.org/u/8x9.

Resources

Five Steps to Staying Secure:	https://www.securingthehuman.org/ouch/2014#october2014
Securing Your Home Network:	https://www.securingthehuman.org/ouch/2014#january2014
Securing Your Tablet:	https://www.securingthehuman.org/ouch/2013#december2013
SANS Security Tip of the Day:	https://www.sans.org/tip_of_the_day.php

License

OUCH! is published by SANS Securing The Human and is distributed under the Creative Commons BY-NC-ND 4.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit https://www.securingthehuman.org/ouch/archives. Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus