OUCH! | November 2013

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- Online Stores
- Your Computer
- Your Credit Card

# How to Shop Online Securely

## Tis the Season to be Cautious

The holiday season is close upon us and soon millions of people around world will be looking to buy the perfect gifts. Many people will choose to shop online in search of a great deal or to avoid long lines and crowds. Unfortunately, this is also the time unscrupulous websites may attempt to scam you by selling counterfeit products, stealing your credit card information or failing to deliver anything. In this newsletter we will cover some of the dangers of shopping online and ways to protect yourself.

### Guest Editor

Lenny Zeltser is the guest editor. Lenny focuses on safeguarding customers' IT operations at NCR Corp and teaches malware forensics at the SANS Institute. Lenny is active on Twitter as **@lennyzeltser** and writes a security blog at **blog.zeltser.com**.

## Online Stores

A scammer can easily set up a website that appears to be a legitimate store by simply copying the look of other, well-known stores. Once these fake websites are online, scammers prey on people who are looking for the lowest price possible. Shoppers often start by searching on Google or Bing for products they'd like to buy, and then add words such as "cheapest" or "lowest price." In return, the search engine will present many, even hundreds of websites selling the item. Some of these websites may be fake.

When selecting a website to purchase your desired item, be wary of online stores offering a price that is dramatically cheaper than anyone else. The reason they may be so cheap is because after you purchase your item, what you receive in the mail is a counterfeit or stolen item, or in some cases is simply never even shipped. Indicators of fraudulent websites include:

- There is no phone number to call for sales or support-related questions.
- The website domain name is different than the domain name it uses for email addresses or other contact information.
- The website uses poor grammar or spelling.

# How to Shop Online Securely

- The website is 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.

Remember, just because the site looks professional does not mean that it is legitimate. If some aspect of the site strikes you as odd, take the time to take a closer look at it. For instance, call the phone number listed in the "contact" section of the website to confirm that the number is valid. Also, type the store's name or URL into a search engine and see what other people have said about the website in the past. If you are still not sure if the website is legitimate, do not use it. Instead, use a well-known website that you can trust, preferably one you, your friends or family members have used in the past. The prices may not be quite as good, but you will receive a more reliable product and be less likely to get ripped off.

*The best way to protect yourself online is to shop at trusted online stores that have an established reputation.*

## Your Computer

In addition to shopping at legitimate websites, you want to ensure the computer you are using for online purchases is secure. If your computer is infected, a cyber criminal somewhere in the world can capture your keystrokes and files. This could allow the criminal to steal your username and password for online stores, credit card and banking information and other sensitive details. Make sure the computer you are using is one you control and connected to a trusted network. This means at least ensuring that you've installed the latest security updates and run up-to-date anti-virus software.

If you have children in your house, consider having two computers, one for your kids and one just for the adults. Kids are very curious and interactive with technology, and as a result they are more likely to infect their own computer. By using a separate computer just for online transactions, such as online banking and shopping, you reduce the risk of your computer being infected. If two computers is not an option, then at least have separate accounts on the shared computer, and ensure your kids do not have administrative privileges.

# How to Shop Online Securely

## Your Credit Card

Be smart with your credit card. This involves keeping an eye on your credit card statements to identify suspicious charges. You should review your statements at least once per month. Some credit card providers even give you the option of being notified by email or a smartphone alert when charges are made to your card, or when charges exceed a set amount. If you believe fraud has been committed, such as never receiving your package even though you have tried to contact the store multiple times, or you see odd charges to your credit card, call your credit card company right away and explain the situation. This is why credit cards are far better for online purchases than debit cards. Debit cards take money directly from your bank account, and if fraud has been committed it is far more difficult to get your money back. Finally, several credit cards give you the option of generating unique card number for every online purchase, or perhaps consider a service like PayPal where you do not have to expose your credit card with every online purchase. Check your credit card company to see what additional services they offer for online purchases.

## Cyber Defense Initiative (CDI) 2013

Join SANS Institute in Washington, DC from December 12-19 for CDI 2013! Featuring more than 25 courses, SANS' most interesting and challenging educational programs, to meet the needs of the sophisticated cyber security community in the nation. As a special bonus, CDI is powered by NetWars-Tournament Play, and will include our second annual Tournament of Champions. Learn more and sign-up at https://www.sans.org/event/cyber-defense-initiative-2013.

## Resources

Stay Safe Online:

http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/online-shopping

Common Security Terms:

http://www.securingthehuman.org/resources/security-terms

SANS Security Tip of the Day:

https://www.sans.org/tip_of_the_day.php



Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis