

HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

WEEKLY

Volume #4 - Issue #185

November 9th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Dangers of Letting Your Kids Shop Online



Online Shopping:

Online shopping is an activity that is increasing in popularity, thus the cyber criminals are also increasing their ways to take advantage of it. Here are a few the major dangers faced when you shop online:

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:

- 1) Verify that 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.
- 2) Look for obvious warning signs like poor grammar and spelling.
- 3) 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 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>.
- 4) 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.

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.

Protect Your Computer/Mobile Device while Shopping:

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:

1) 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.

2) Only connect to wireless networks you manage, such as your home network, or networks you know you can trust when making 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.

3) 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.

Protect 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 are technologies 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.

Thank you for subscribing to our email!



Copyright © 2015-2018 House of File Technologies