Online Safety Tips for Black Friday and Cyber Monday Shoppers

Ken Foster
KMBL Security (www.kmbl.us)
11/24/2011

The rush is on to get that great deal before they run out! Web sites post countdown timer, quantities remaining counters, and offer last minute special deals on shipping; all designed to increase your urgency to buy now, click here, hurry! Each year more people opt for online shopping as a way to avoid the malls, parking hassles, and cold weather. At this point the merits of online shopping are understood by most; however there are cyber-safety issues one must consider as well. Here are the 10 things you should do prior to shopping online the holiday season:

Use Secure Payment Methods:

1. Before you consider looking for those great online bargains, stop and make sure your computer is updated and has a working anti-virus program with current signatures. You might think why is this in the payment section? Thousands of new computers are infected each day by info-stealers, click hijackers, and Trojans because this simple step is not taken. For users on Windows (98.9% of all users) go to your windows update. It's pretty simple, but if you don't know how, just click on the Windows Start button and type "*Windows Update"* in the search box. Mac users, you are not exempt from malware either despite what you have been lead to believe. You are actually more susceptible because you are less likely to update your 3rd party apps (e.g. Adobe Reader, Java, etc…) and most likely do not have anti-malware software running. This makes you susceptible to cross-platform exploits. For more on mac exploits, visit The X Lab (http://www.thexlab.com/faqs/malspyware.html). What about your Anti-Virus program? Launch the app and check the date of your last updated signatures. Many people buy a new computer and it comes with 90 days of free Anti-virus; never renewing the subscription. Did you know many drive-by malware exploits are delivered by 3rd party Advertisements on legitimate websites? Be smart, patch your operating system and perform a virus scan before you shop!

2. If you don't have a PayPal account, get one. Many online retailers offer this as a method of payment. It allows you to securely use your credit card through PayPal who acts as a proxy. The vender gets their money without ever knowing your card number. Any company can look big and legitimate on the internet. Paypal is free, check them out at: www.paypal.com

3. Consider Single-Use Credit Card Numbers. This service issues the user a unique credit card number that allows for a single transaction against their account. This number is completely different and only

the bank can associate the single-use number to the accountholder. If someone get this unique number its useless since you already used it for the life of the single transaction. According to an article by Jerry Brito (Time Techland, 5/3/2011) Citibank, Discover, and Bank of America still offer this service. The article provides links to each provider's content. Read the article directly at: http://techland.time.com/2011/05/03/disposable-credit-card-numbers-can-protect-you-from-hacks/

4. Never provide a user name, password, or your credit card information if the web site is not secure. Today there are still web sites that don't use SSL (the little lock icon) to secure their online sensitive transactions. This is the same as the retailer asking you to shout your information across a crowded room; online it arrives unencrypted (plain-text) and readable by anyone who cares to listen. If your browser provides you any warnings about the SSL certificate (e.g. red address bar, pop-up alert, etc…) then under no circumstances trust the web site. If you have to buy that item from the site, look up their customer service number using the Online Yellow pages and call them directly. If you can't do that then use a Single use Credit Card Number. It's just not worth the risk to do it any other way.

5. Never use your Smartphone to Purchase items. Here is the reality; you should never directly purchase items from your smartphone. Instead, use apps like Amazon Price Check, Red Laser, etc… to find the absolutely best deal on your purchase. Once you find that item, add it to a wish list, bookmark the pages, etc… and then purchase the item from your home computer. This may seem like the long way home, but you have no idea who made the apps your downloaded, what they are doing, and if they are securely protecting your sensitive information on your smartphone. Furthermore you probably don't have a decent anti-malware app on your smartphone. If you are storing your credit card information on the device, you are just asking for someone to steal it. Iphone users don't think your apps are any more secure than the Android guys, there just more restrictive in what they put in the marketplace, not more diligent (http://www.pcworld.com/article/243407/iphone_security_flaw_shows_potential_for_app_store_malware.html).

Passwords, Passwords, Passwords:

6. Most people use the same 3 or 4 passwords on every site they visit. This practice is incredibly unsafe. Websites get hacked all the time; consumers may or may not ever be notified. Simply put, it doesn't take a rocket scientist to guess if you use your email address and a password on one site, that you probably use the same combination on others (e.g. bank, other online retailers, etc…). Consider using unique passwords for each site. There are several ways to manage this. The easiest method is to download LastPass. LastPass integrates into your browser and stored securely logon and password information. It offers a secure password generator guaranteed to give the craftiest cybercriminal nightmares. One of the nicest features is it can be set to automatically log you onto sites (your choice), reducing the complexity for remembering the password. Visit: www.lastpass.com and sign up. It's free and secure. Just remember, keep your LastPass password in a safe place. If you lose it you're as out of luck as the thieves you're trying to defeat.

7. Password Rules. If you are going to set your own passwords take a minute to understand what makes a password secure. If you go to https://www.grc.com/haystack.htm you can test the strength of some of your current passwords. You may be shocked to see how weak they are, motivating you to change them. This page also discusses a concept called haystacks, which is worth reading if you are truly concerned. If not and you just want to fix the issue, go to the PCtools online password generator (https://secure.pctools.com/guides/password/?length=8&phonetic=on&alpha=on&mixedcase=on&numeric=on&punctuation=on&nosimilar=on&quantity=10&generate=true) . Just make you choose all the options the site will allow (e.g. Special characters, more than minimum length, etc…). I recommend you set the total passwords generated to 10 and then randomly select one from the list. If you are going to store them on your system, consider a password protected store or at a minimum a password protected Excel spreadsheet.

Shipping and delivery

8. Buy early to avoid high-cost delivery charges. Most online retailers provide free or reduced rate shipping if you order prior to mid-December. Regardless of the shipper, only choose methods that provide online tracking. Most shippers allow you to subscribe to delivery status update and delivery notices for your packages. Know where your package is and when it was delivered. The less time is sits on your doorstep, the better. If you use FedEx, consider having high dollar packages rerouted and held at your local Kinko's Printers office. They are open 24/7 in most locations.

9. Understand if your package is insured prior to purchase. Most commercial shippers insure packages for a set amount. If you are buying a high dollar item, consider it's more likely to be stolen than a pair of wool socks and insure accordingly.

10. If you can't be there to pick-up your package when it arrives, consider asking if a trusted neighbor might be willing to get it for you. Something as simple as a text to them after it arrives. This is especially important in high-density living areas such as condominiums and apartments. If you are going to ask them to pick up several packages, consider giving the neighbor a nice gift card at the end of the season as thanks.

The Holiday season is stressful enough. Identity theft, stolen packages, and infected computers are unwelcome additions. If you take a few minutes to prepare today, your chances of these issues happening is far less. Have a happy holiday.

Please feel free to re-tweet or share the link to this article with friends, family, co-workers, etc…