

Top 10 Cyber Monday Shopping Safety Tips

By Virtual World Computing



Top 10 Cyber Monday Shopping Safety Tips: Survival of the Smart & Savvy

Copyright © 2013 by Virtual World Computing

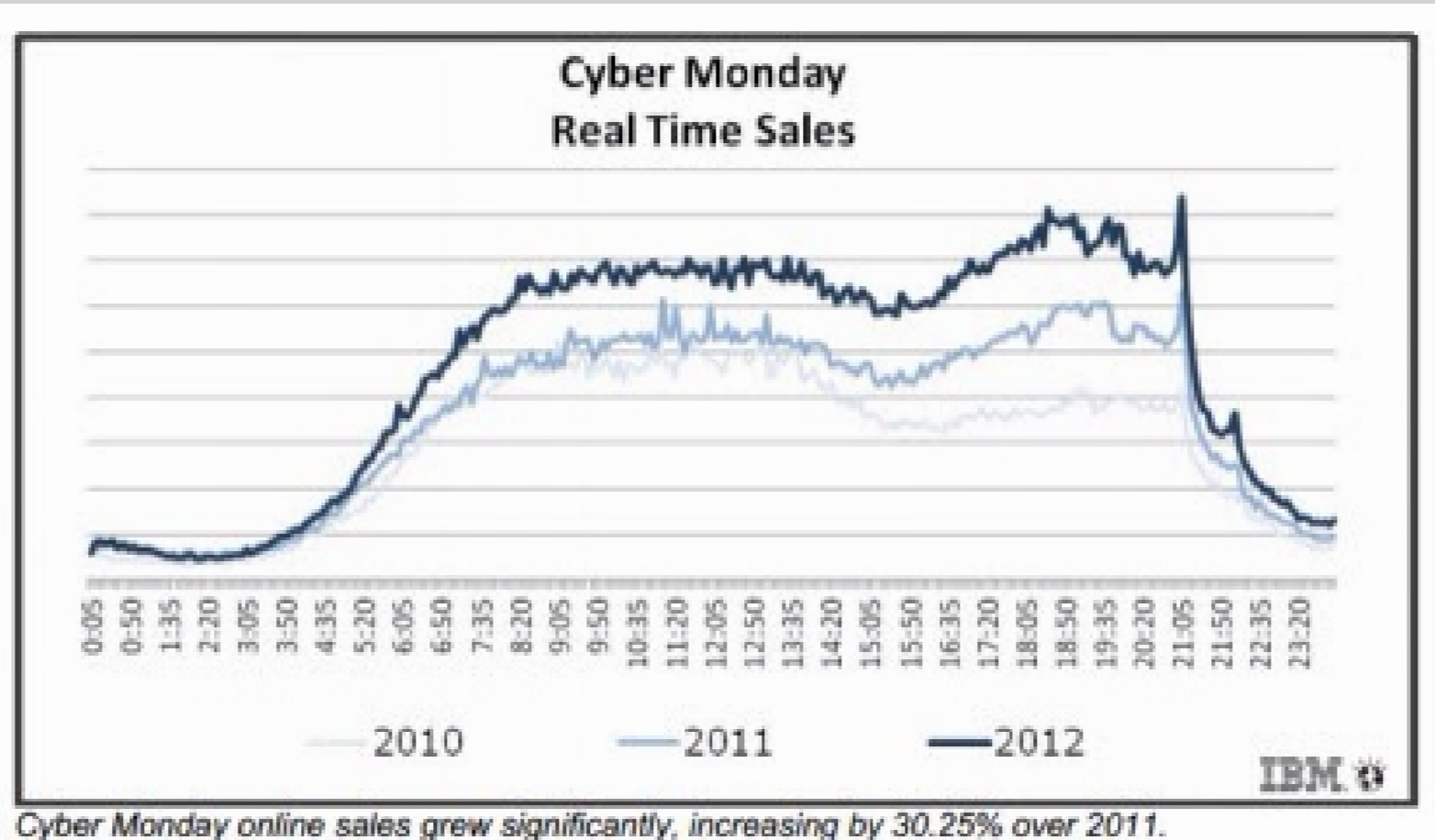
Bev Robb | Cocoon™ service

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means including storage and retrieval systems without permission in writing from Virtual World Computing

Powered By Bookemon. www.bookemon.com

Cyber Monday in the United States is the first Monday after Black Friday and is another major busy American shopping day. Cyber Monday follows hot on the heels of Black Friday and is also a time when cybercriminals, Identity thieves, malware writers, and online scam artists push their unsavory code and wares on unsuspecting online shoppers.

Cyber Monday was the biggest shopping day of the year in 2012, with an increase of 30 percent over Cyber Monday of the previous year.



Cyber Monday online sales grew significantly, increasing by 30.25% over 2011.

Prime Time For Cyber Gangs

The 2013 Norton Report states that cybercrime continues to be a growing global concern. Both the total global direct cost of cybercrime (US\$113 billion; up from \$110 billion) and the average cost per victim of cybercrime (\$298; up from \$197) increased this year. With approximately 378 million victims per year (more than 1 million each day and 12 per second) —there are plenty of online victims for cyber gangs to attack.

It is also interesting to note that the report also found that while nearly half of all smartphone users care enough about their devices to sleep with them, they are not taking the basic precautions of backing up, installing security software, or using passwords.

"If this was a test, mobile consumers would be failing," said Marian Merritt, Internet Safety Advocate, Symantec. "While consumers are protecting their computers, there is a general lack of awareness to safeguard their smartphones and tablets. It's as if they have alarm systems for their homes, but they're leaving their cars unlocked with the windows wide open."

Consumers Need To Be Proactive

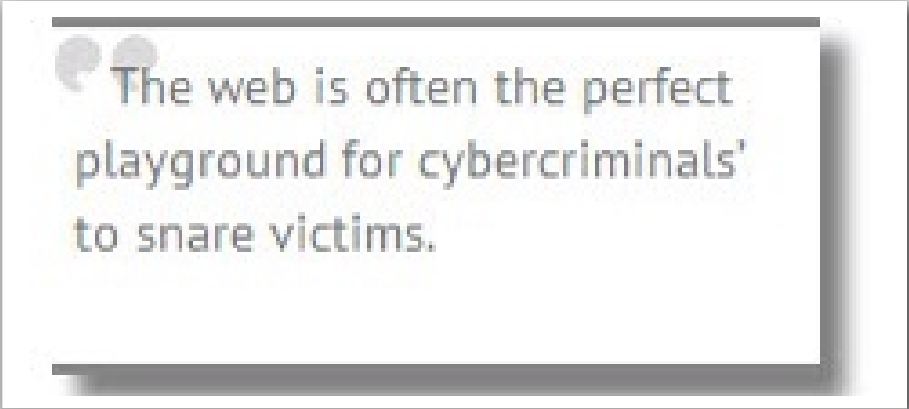
With the growing popularity of mobile devices combined with public Wi-Fi networks — more consumers are becoming vulnerable to identity theft and online fraud. Cyber gangs frequently operate highly sophisticated attacks that are geared toward the retrieval of quick money. Their attacks are often combined with the use of carefully crafted social engineering techniques.

When you shop online — it's alright to venture on the side of paranoia when it comes down to web security. But, if you have not taken the necessary steps to protect your computer or mobile device, it's only a matter of time before you feel the hackers scalpel sever a major artery in one or more of your financial accounts.

How Do You Become Proactive?

Do you remember that old German adage "knowledge is power"? With all the Internet threats that abound while web surfing — always expect the unexpected. The majority of Internet security risk factors for online shopping can be controlled with the right online tools, the right attitude (a willingness to learn and apply the necessary strategies), and the desire to become proactive versus reactive.

Knowledge Is Power



“The web is often the perfect playground for cybercriminals’ to snare victims.

The web is often the perfect playground for cybercriminals’ to snare victims. Social media houses the glitter with connections, apps, games and traps. Major search engines feed the curious, but can also circumvent legitimate searches and replace them with malicious links.

Using the same weak password across multiple sites gives a hacker an entrance to hijack all your online accounts; and has the potential to steal bank login information and potentially wipe your bank account out.

A weak password such as 123456, password, abc123, or using your first name or pet’s name as your password is the Achilles heel of online security.

Begin With The Basics

Backing up your computer and devices and using strong passwords is your first line of defense against cybercriminals.

Always set up a regular backup schedule. There is generally minimal effort involved in backing up your operating system (and data) and is well worth the slight inconvenience of the initial setup.

By creating complex passwords for each site (and not sharing the same password at multiple sites), you will reduce the chance of cyber miscreants hacking all of your accounts.

Your Entire Digital Life Could Be Wiped Out

in one hour. Such was the case of the epic hacking of Wired journalist, Mat Honan...

The hackers were not satisfied with simply hacking Mat's Gmail and Twitter accounts. Instead, they also hacked his Apple iCloud account to remotely wipe his MacBook, iPad, and iPhone too.

Mat learned a difficult lesson with this carefully crafted social engineering attack. Failure to back up his data and the hackers ability to convince an Apple technical support representative, gave them a temporary password to Mat's

.Me account. The hackers only needed two pieces of information:

his billing address and the last four digits of his credit card was all

that was needed to gain control of Honan's email account. Once they had access to his email account they were able to get the password reset to other online accounts.

Never Put All Your Eggs In One Basket



If Mat had used two-factor authentication with his Google account and backed up his devices on a regular basis — he would not have lost an entire year of his life in photos, documents, and email.

Fortunately Mat's wiped MacBook was recovered through DriveSavers. The cost of data retrieval can run several thousand dollars; while the price of a backup is dirt cheap in comparison.

Still, too many consumers remain indifferent to backing up their data until they are affected by a virus, a hack, or a failed hard drive. Backing up is like flossing your teeth — preventative maintenance will save you time, anguish, and prevent gum disease.



Top 10 Cyber Monday Shopping Safety Tips

Now that you know why it is important to regularly back up you data, it is also equally important to protect your computer and devices too.

Computers

You should always keep your operating system and firmware updated. Your operating system should include antivirus, anti-malware/spyware, and a firewall.

All software on your computer should be updated to the latest version, and this includes keeping the browsers that you shop with updated too.

Mobile Devices

Keep your operating system updated and install a trusted mobile antivirus protection app such as Bullguard, Lookout, McAfee, Kaspersky, or ESET. Make it a habit to only download apps from trusted companies or developers.

Note: Criminals also use QR codes to infect your device with malware or link you to a phishing site. Choose your QR code scanner carefully. Using a QR code scanner such as Norton Snap will block and warn you if the code is malicious.

I. Backup & Update

Palin's Hack

Who can forget Sarah Palin's hacked email account? What an easy hack that was! She had a password reset question that had the answer splashed all over the Internet. With personally identifiable information a keystroke away, the hacker was able to breach her account and gain access to all her private email.


Most people should know not to use passwords that are associated with something that can be traced directly back to them. With just a bit of search engine research: birth dates, names of pets, spouses name, etc. can all be figured out with some social engineering or access to public profiles on social media accounts.

Passwords

Use a minimum password length of eight characters composed of numerals, symbols, punctuation, and upper/lowercase letters. Change passwords every season and use a different password for each site.

2. Use Strong Passwords

Shop Securely

Always make sure that you are buying from a trusted and secure site. If you look at the top of your browser where the website address is displayed, you should see  <https://> indicating that the site encrypts the information between your computer to the e-tailer. Most browsers will also show a lock icon indicating that you are shopping on a secure website.

Use Trusted Sites

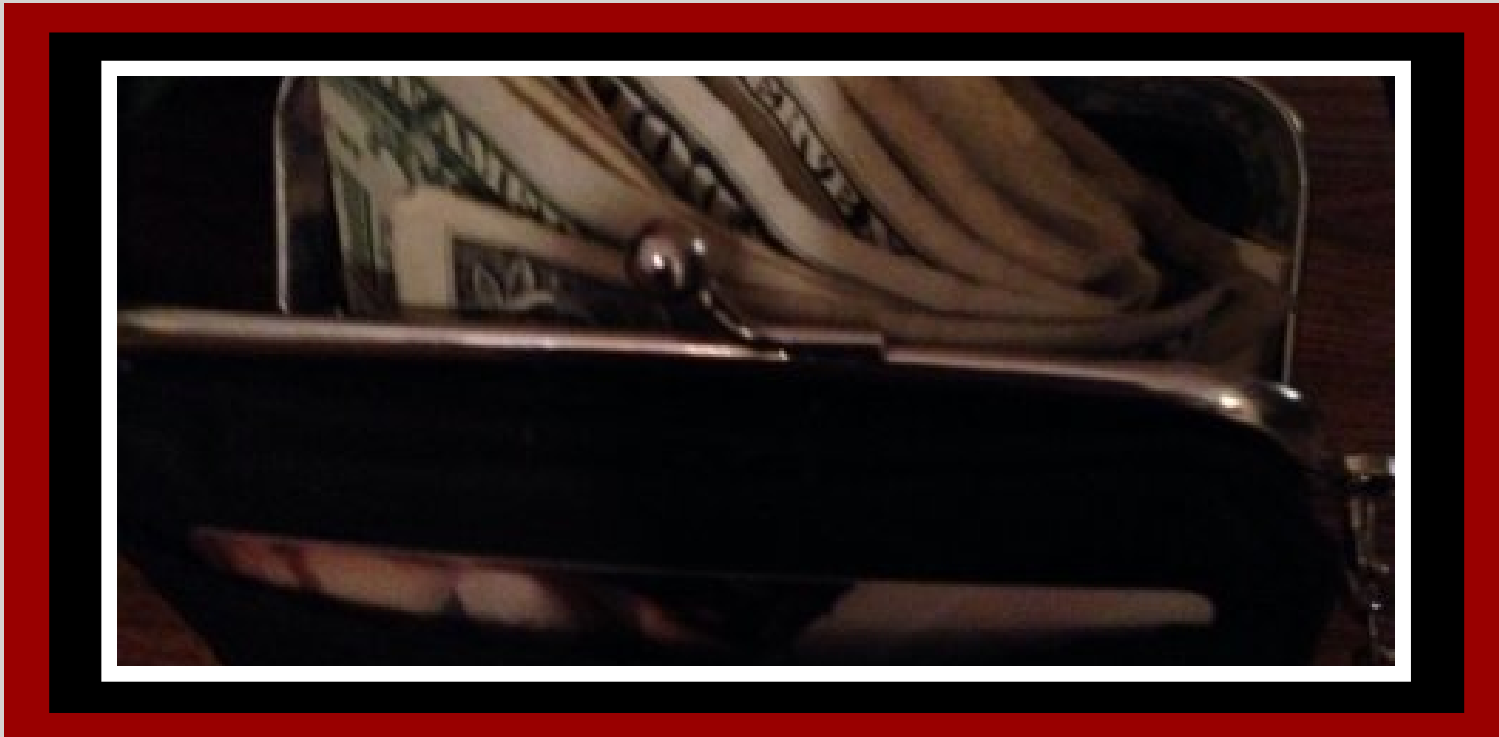
Stick to reputable and trustworthy sites and read customer reviews.

This is the time of year when fake websites pop up all over the Internet in an attempt to scam you out of your private information and rip you off.

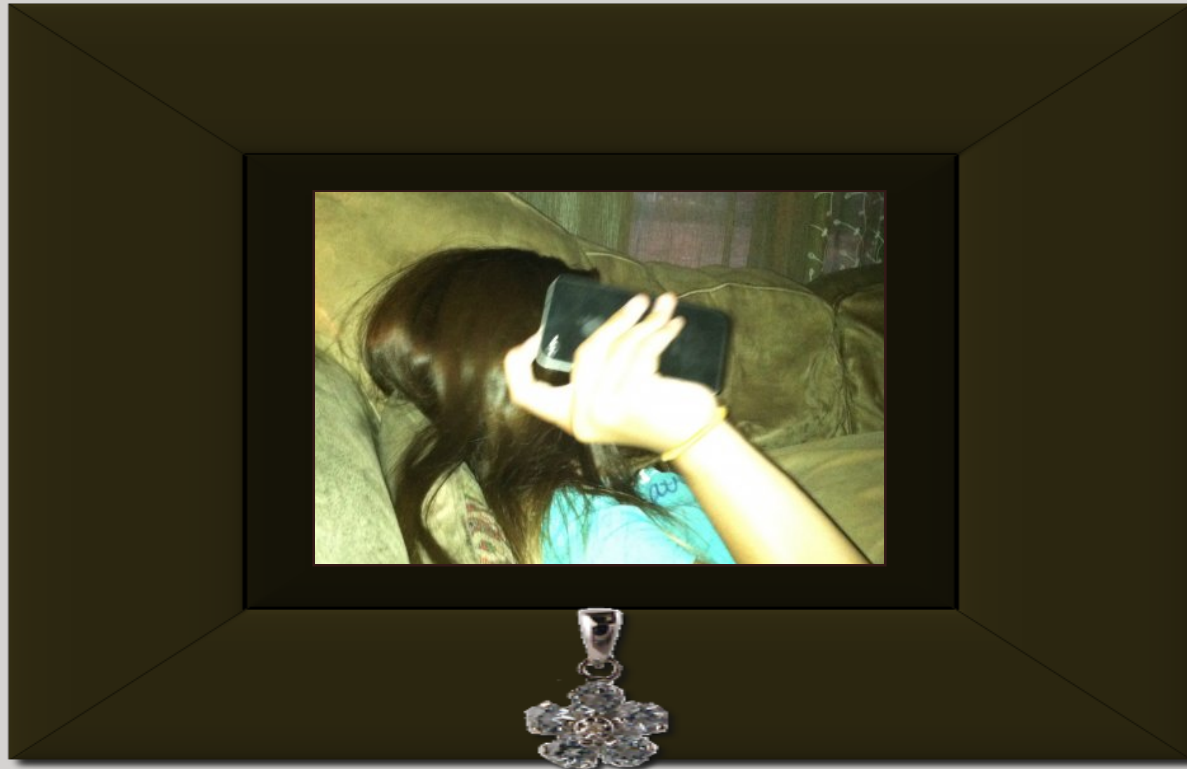
3. Shop At Secure & Trusted E-TAIL Sites

Phishing scams are hot this year. Whether it is a tweet on Twitter, a private message on Facebook, or an email with a malicious link or attachment — don't take the bait this Cyber Monday!

From fake e-cards to bogus delivery notifications, criminals hone their scams hoping to nab as many victims as possible, while pocketing quick cash.



4. Avoid Email & Social Media Phishing Scams



Scambook is warning that the the same type of gift card text message scam as last year, may reappear this year. Though the dollar amount and retailers may change —the scam is still the same.

5. Avoid Free \$1000 Gift Card Text Messages



Cyber Monday Deals

About 80,000,000 results (0.50 seconds)

According to Jovi Unawing of GFI Labs: "Black Friday and Cyber Monday are among the most targeted holidays for malicious scams. The volume of product searches and online transactions that take place during these few days creates an opportunity for cybercriminals to target online shoppers with SEO poisoning, malicious links on social media sites, phishing scams and other attack methods."

Be aware that searching for "Cyber Monday Deals" can become dangerous when utilizing a search engine to locate all those awesome deals.

6. Scrutinize Search Engine Results



Last year the government seized 150 domains due to fraudulent operations in the sales of online counterfeit goods. Professional sports jerseys, golf equipment, DVD sets, footwear, handbags, and sunglasses are some of the more popular items listed on the Department of Justices website.

7. Avoid Purchasing Counterfeit Goods

Always read the site privacy policy. Yes, I know most of them are pretty boring but it is better to know in advance if a site is going to share your private information with affiliates or other businesses, so that you can steer to a more privacy-friendly site.



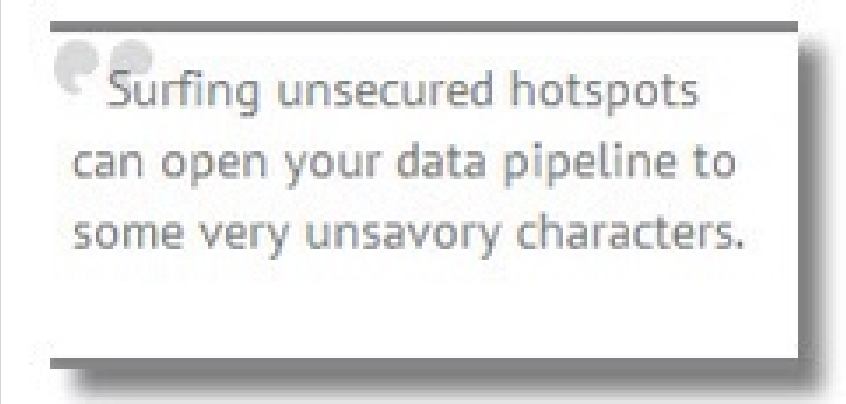
Using a debit card to shop online could open your checking account to a hacker. Since debit cards remove money directly from your account, if there is any type of fraud it will be difficult to get the charges reversed quickly since banks can take up to two weeks to investigate fraudulent activity.

Opt for using a dedicated credit card instead, and always keep a record of your online order. One card is easier to check up on and will reduce your risk to other accounts. Be sure to keep a close eye on your credit card statement too, and set up alerts so that you receive notifies when charges exceed a set amount.

8. Protect Your Private Information & Avoid Using Debit Cards

Whether you use public Wi-Fi for convenience or because you do not want to use your data plan — the bad guys still have all kinds of tools to gather and steal information from you.

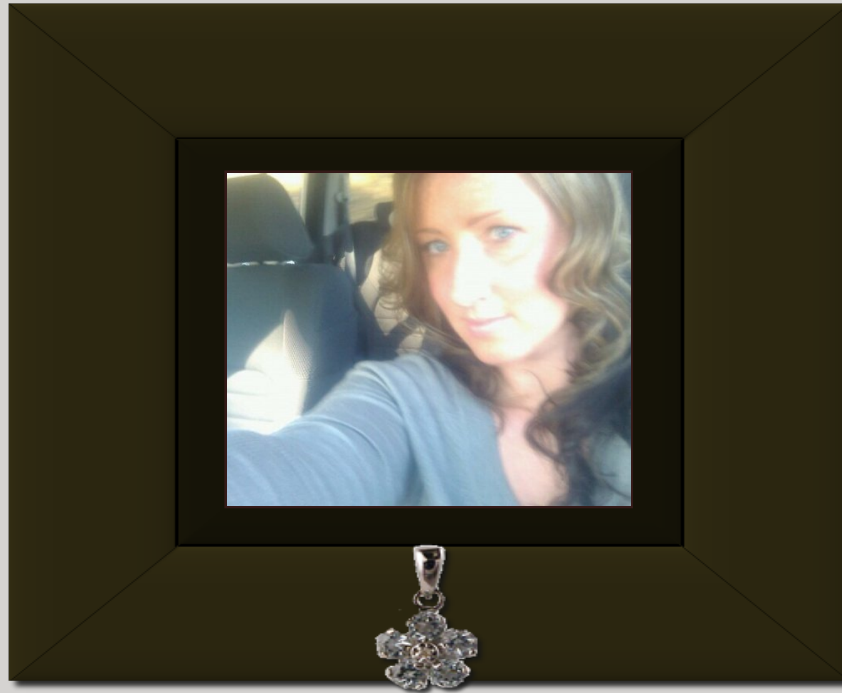
If you must use public Wi-Fi to shop, be sure to use a VPN or our free cloud-based Cocoon security software, so that all your browser activities become routed through a "secure tunnel" that will block the bad guys from getting into your shopping data.



Surfing unsecured hotspots
can open your data pipeline to
some very unsavory characters.

Secure your wireless network with a password (do not use the default).

9. Avoid Using Public Wifi & Secure Your Home Wifi



Don't believe everything that you see!
Before you buy that awesome \$75
iPad, it's probably too good to be true...

10. Be Wary Of Deals That Sound Too Good To Be True



Touching the internet is dangerous stuff. That's why Cocoon never lets our user's touch it directly. We keep the Internet at arms-length from our users. Users connect to us, and we touch the Internet for them.