Halting Hackers For the Holidays

12 Tips Before Christmas

By Gary S. Miliefsky,
Cyber Security Expert, Consumer Advocate and CEO of SnoopWall, Inc

October was National Cyber Security Awareness month and during that time, millions of online identities were stolen in America with over 200 published breaches (see: http://www.privacyrights.org).

We're getting close to one billion records of identity theft – more than 3x our entire population in the USA. America has proven herself to be not only one of the greatest nations on earth when it comes to size of economy, innovations, financial and retail markets leadership but also the number one target for cyber criminals.

According to StopThinkConnect.org, nearly two-thirds of the American public have heard, read or seen something about online safety and security issues recently. However, most of what they remember is negative: identity theft, privacy loss, and increased frequency of attacks. In a recent survey, published at http://stopthinkconnect.org/research-surveys/research-findings/, consumers were asked why they don't do the things they can or should do to stay safe online. Americans said they simply lacked the information or knowledge.

So if you want to enjoy Black Friday, CyberMonday and the Christmas Shopping experience without losing your privacy and identity or putting your children's safety at risk, here's the information you need.

Here are my best tips you should follow to Halting Hackers on the Holidays:

1. Defend Yourself Against Porch Pirates

Criminals known as "porch pirates" are thieves who sneak onto properties and steal packages left on doorsteps. There are free and paid apps that track packages such as Slice, iDelivery, DeliveryStatus and MyPackage. If you know your tracking ID, then you know where your delivery is and when it should arrive. However, if a Porch Pirate guesses a valid tracking number, they can also know when and where packages are going.

If you are going to ship packages to your home, you might consider getting a Land Port device from http://www.thelandport.com to protect package deliveries or try Doorman at http://www.doorman.co/ who holds packages for you until you are home.

Better yet, see if you can get permission to ship packages to work. If, however, you can't have packages delivered to work, ask a neighbor or friend to receive your packages for you. If you are still going to have packages arrive at home, when you aren't there, you might want to setup a live recording video camera aimed at your porch such as a Foscam or Grandstream: Foscam - http://foscam.us/ Grandstream - http://www.grandstream.com/. Don't tip off criminals by knowing when you are not home. Disable geolocation on your smartphone so your location can't be tracked. You can also cleanup your location history at the Apple iCloud/iTunes and at http://history.google.com.

A more sophisticated Porch Pirate is also a cyber-criminal that might send you an SMS message or email with malware to gain remote access to your PC or smartphone and install a RAT (Remote Access Trojan - see our threat report entitled Year of the RAT for more information on this subject matter, located here: http://www.snoopwall.com/reports/).

Then they can eavesdrop on your orders and deliveries. If they get your password to http://history.google.com for example, they can geolocate you, to see when you are home and when you are away from home. If they know you are not home and a package is scheduled for delivery, they can easily steal it if they are in your location.

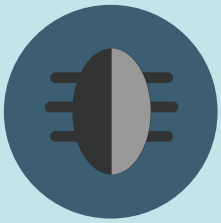
2. Assume You've Been Compromised

With so many breaches and personally identifiable information (PII) records being lost or stolen in the millions each month – like the 80,000,000 records Anthem breach or the 110,000,000 in the Target breach or the 22,000,000 in the Office of Personnel Management (OPM.gov) breach, or this month's Comcast breach, you really need to assume you've already been compromised – your identity has probably been stolen and is being sold on the black market. But those are just the tip of the iceberg. When it comes to your personal privacy, have you read the Privacy policy on your new SmartTV or any of the apps you've installed on your computer, tablet or smartphone? Right now just about everyone who has access to your webcam, microphone, contacts list, internet browsing habits, search engine keywords or even Microsoft Windows 10 are all collecting information on you. It's up to you to turn off everyone's access to your privacy wherever you can do so without breaking things.

3. Change Your Passwords – All of Them

Change your passwords - all of them. Now. And do it as frequently as you can tolerate. Also, if you don't want to change it often, then use any unique characters you can think of like a dollar sign $ or an exclamation mark ! or replace an "O" with a "zero" 0. This goes a long way in preventing brute force attacks against your password. One of the top methods of stealing from consumers is called 'social engineering'. What this means is you'll get a phone call from someone asking you for your password and pretending to be someone important, such as an employee at the IRS or your bank.

Never trust anyone on the phone who is asking you for your password, especially if they called you. The same holds true with emails. The #1 attack method is called a phishing attack or a spear phishing attack. What happens is you'll receive an email asking you to reset your password at your bank or some other account you might have (a retailer, the IRS, the US Social Security Administration, etc.) and the link takes you to a page that looks real but the web address (URL) is slightly off, for example it might say Amaz0n.com instead of Amazon.com – all it takes is a subtle change in the web address and you may be typing in your real password to help them 'reset' it for you. They end up stealing your real password, logging into your account and stealing your money. Don't trust any inbound emails that request you click a link to reset your password and asking you to type in your current, real password. Call the merchant or your bank and ask them about the email or visit their real website and look to see if they have any news about a breach. By the way, when you buy a new wireless router, or anything that connects to the internet, such as a baby monitor or wireless webcam, it will probably come with a default password. Login and change it immediately so this device never gets breached by a simple attack against the default password.



4. Turnoff wireless protocols and geolocation services

Make it harder to wirelessly pickpocket or hack you by turning off all these services that you don't need or use. Protect your smartphones and tablets by turning off WiFi, Bluetooth, NFC and GPS, except when you need them. That way, if you are at a local coffee shop or in a shopping mall, no one can spy on you using nearby (proximity) hacking attacks and they can't track where you were and where you are going on your GPS. If you installed a mobile wallet, it might want to use NFC when you are at the merchant doing the transaction, so turn on NFC just during the transaction and make sure no one is really close to you with a smartphone or laptop bag where they might be eavesdropping on your transaction. Then, turn off NFC right away and you'll have secured your mobile wallet from wireless pickpockets.

5. Cleanup Your Apps

Assume most of your smartphone or tablet apps are creepware – malware that spies on you and your online behavior. Do you really need them? Delete all of the apps you aren't using that often. Replace those apps that take advantage of too many of your privacy settings like GPS, phone & sms logs, personal identity information, with similar apps that don't. On an iPhone, you're not being eavesdropped on until you run the app.

Let's take the most popular apps – Flashlight Apps. We've investigated them and found that some of the most popular are actually malicious and creepy (see: http://www.snoopwall.com/flashlight-apps/). On an Android, if you download the second-most popular flashlight app, Brightest Flashlight from Golden-Shores Technologies, it turns your light on without your permission, loads their privacy policy over the Internet — which means it's taking an Internet connection without your permission — and it brings up 25 pages saying, "I'm eavesdropping on you, I'm geolocating you, I'm spying on you," so that they've complied with a ruling by the FTC against them – which was a 2013 settlement over privacy violations. This is only the beginning – we've found similar problems with Bible Apps, QR Readers and even popular games. You can read more about those that steal your privacy at http://www.privacygrade.org where they give many free apps grades on how much information they access. Here's their review of one of the many free flashlight apps, for example: http://www.privacygrade.org/apps/com.rvappstudios.flashlight.html.

When it comes to free Apps – ask yourself, why are they free? Have they made any money from you clicking on in-App advertisements? Most people will say they never click these ads, so how do they monetize their free apps?. The industry's dirty little secret is that with Google Android, Apple iPads and iPho-

-nes, the Microsoft smartphones, and even Blackberry devices — all of them have tool kits for developers to make apps that make money. The tool kits include the ability to turn on all the ports — hardware input/output ports, GPS, Wi-Fi, Bluetooth, NFC, microphone — they have literally created a spyware developer's kit to monetize advertising networks. That's the dirty little secret. So even if you think an app is trustworthy, like Angry Birds, if they integrated with one of these advertising networks, their free game becomes a piece of spyware for malware advertisers (known as 'malvertisers'). Paying for an app that has no need for internet access is the best thing you can do to protect yourself, your children and your family from eavesdropping creepware apps.

6. Opt-out of Information Sharing

It's really important, if you want to protect your privacy, you should opt-out of every advertising network that you can. Visit the National Do Not Call Registry and register your smartphone and home phone numbers at https://www.donotcall.gov/. If you use a google email account and have an Android phone, you'd be surprised that even with your GPS off, it's tracking your every move. You can login to https://-maps.google.com/locationhistory/b/0 and see for yourself.

You have to go into your smartphone or tablet settings and turn this feature off. It is possible to turn this off. In your Android phone, go to Settings, then Location, select Google Location Reporting and set Location History to off. The same holds true for the Apple iPhone, iPad and iTunes. You need to find the location and privacy settings and turn off access under Settings, then Privacy then Location.

Many companies you do business with are required to give you privacy notices that explain their information-sharing practices. In turn, you have the right to limit some — but not all — sharing of your information. The law balances your right to privacy with a company's need to provide information for normal business purposes. Credit reporting companies also may sell information about you to lenders and insurers who use the information to decide whether to send you unsolicited offers of credit or insurance. This is known as prescreening.

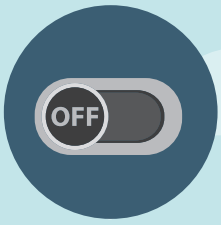
You can opt out of receiving prescreened offers by calling 1-888-567-8688. There are two federal laws which cover different aspects of how companies can share your financial information: the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA). Learn more about your financial and credit information privacy rights at http://www.consumer.ftc.gov.

When it comes to your medical or health care records, the law that is designed to protect your information is called the Health Insurance Portability Accountability Act (HIPAA). Learn more about your privacy rights on HIPAA at http://www.hhs.gov/ocr/privacy/.

7. Cleanup and Protect Your Web Browsing Experience

Your browser is a 'double-agent' spying on you for advertisers, unless you block and remove cookies and delete the cache frequently. Go into your web browser settings and delete your history, all cookies and passwords and the cache. You should do this frequently so you don't leave personal information sitting around on your computer, smartphone or tablet. There are some free and paid web browser privacy tools out there that you should checkout and consider installing into your favorite web browser. Some of these best tools include AdBlock, Adblock Plus, Disconnect, DoNotTrackMe, Ghostery and Privacy Badger, which is a promising privacy tool because it comes from the Electronic Frontier Foundation (EFF) who is on a non-profit mission to defend civil liberties in a digital world. To see for yourself, visit them here: https://www.eff.org/privacybadger.

If you want to try something new and innovative, scrap your Internet Explorer, Firefox, Opera or Chrome for a privacy web browser such as the Epic Browser located at https://www.epicbrowser.com or Comodo's Dragon web browser located at https://www.comodo.com/home/browsers-toolbars/browser.php or the most famous, the Tor browser, which has become the watchword for the anti-surveillance because it is built on an entire infrastructure of 'hidden' relay servers. Tor is built on top of a modified Firefox and it can be installed on a Windows, Mac or Linux PC as well as on a USB stick. Learn more about Tor at https://www.torproject.org/index.html.en.



8. Remove Third-party Social Media Plugins

Don't allow third party plugins to be installed in Facebook, Twitter or any other social media platform. Also, think about what you like in Facebook – all of those likes are cookie crumbs for others to learn a lot about you. Third party plugins are mini applications designed to eavesdrop on your behavior and in social media platforms like Facebook, to grab information about your habits inside the platform, your friends, messages, etc. Some websites you visit will require you to login using Facebook and then you have to trust them to connect to your Facebook account, this is very risky. Read their privacy policy and make sure they are a legitimate business before you risk doing this.

To disable third-party plugins, when you're logged into Facebook: Click on "Account" at the top-right of the screen and click "Application Settings. "Change the "Show" drop-down box to "Authorized" to list the applications you've ever given permission to access your Facebook information. Click the "X" button on the far right next to each app you want to remove to uninstall it. In the dialog box, click "Remove" then click "Okay" to confirm app deletion.

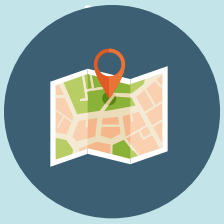
In Twitter, to revoke access or remove an application: Review the applications you've connected in the Apps tab of your account settings. Simply click the Revoke Access button next to the application. For other social media services like LinkedIn or others, simply do an online search for "remove third party apps from [LinkedIn]" and you'll find similar instructions.

9. Only Shop Online from Websites You Trust

Only shop on websites you know and trust. If you don't know where the merchant is located, don't shop online there. If they don't have a corporate address or are located in another country, it could be risky for you to ever see the goods you think you purchased. Also, if their shopping cart experience is not an HTTPS browser session, then everything you type in, your name, address and credit card information is going over the internet unencrypted, in plain view.

Never buy anything online using your credit card on a site that doesn't have SSL (secure sockets layer) encryption installed. It's real easy to tell you are in a secure, encrypted session if you see an icon of a locked padlock in your browser and the website URL starts with HTTPS not HTTP. Also, if you receive any emails from the merchant, no matter the reason, don't give them your credit card information over email. In addition, if it looks too good to be true, it probably is. Do additional research on the merchant before buying. Check reviews, their phone number, mailing address and test all of their contact information to make sure they are for real, before buying online.

Most importantly, if you do trust the merchant, make sure you understand their return policy, so there are no surprises if you need to return an item. If you are buying online and they don't have a local retail outlet near you, this could be a headache for you if you can't meet with a customer service representative in person.



10. Turn Off GeoTagging – Your Pictures Say Too Much

Global Positioning System satellite technology, better known as GPS, is embedded into all of our smart-phone devices. While you may enjoy using it to get door to door directions while traveling, most of us take for granted the fact that it is being used for many other purposes, the most popular of which is to tag information into your photos. This is called Geotagging. Even though you don't see the geotag informa-

-tion by looking at your photos, there are free tools which allow anyone to read the embedded geotag. Besides location, geotagging can also include elevation, bearing, distance, and even the name of a place like restaurants and retail outlets.

Twitter and Instagram as well as your Android, iPhone, Blackberry device or Windows Phone will give away your location. Most people don't realize Twitter and Instagram both use geotagging for everything you send out. Geotagging is storing your latitude and longitude of your tweet or image. Pictures you take on an iPhone usually store geotagging information, as well.

The less information you give out about where you are located, the safer you are. Depending upon the operating system of your device, you'll either find GeoTagging in the Location Services area of settings or under the built-in Camera App where you should set "include location (GPS) info in Pictures you take" to "Off".

11. Don't Use Cash or Debit Cards, Use Credit Cards

You have three major choices when shopping - use cash, use a credit card or use a debit card. In rare but growing instances there's even a fourth option called "Bitcoins" which are now accepted at some merchants including Overstock.com. Bitcoins could be considered the equivalent to the cash option, because once used, you can't get them back. So, if you have to choose between these options, believe it or not, the best is the credit card.

Here's why – your cash is precious to you – whether it's in your pocket or your bank account – once it's stolen, it's very difficult to get back. So, you probably travel with less cash and if you are purchasing something online, it's also safer to use your credit card than your debit card. The same holds true when you visit your local shopping mall or retail outlet.

The reason is, if you experience identity theft, the credit card laws allow you to keep all of your credit immediately, with no responsibility during an identity theft or fraud investigation. However, with a debit card, the policy of your local bank can be to tie up your hard earned money in the amount of the fraudulent transactions for up to thirty days and some have been known to take up to 60 days to resolve the issue in your favor and give you your money back into your account.

However, you still should not spend more than you can afford. Just use this security feature of your credit card to protect your hard earned savings. Taking advantage of the shift in risk and responsibility is the key – let the credit card companies worry about the monies lost, not you.

12. If You Think You're A Victim of Cyber Crime, Here's What To Do

If you think your computer or personal information has been compromised, you can place a fraud alert by contacting the three major credit bureaus and place a 90 day "fraud alert." This helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets an "alert" that there may be fraud on the account.

Experian	1-888-397-3742
Equifax	1-800-525-6285
TransUnion	1-800-680-7289

You will reach an automated telephone system. You will also be sent instructions on how to get a free copy of your report from each of the credit bureaus. Order the reports. You can get these for free at least once per year from the free Annual Credit Report website at: https://www.annualcreditreport.com/. Another smart move is to place a security freeze on your credit files as it offers longer term protection. For information on how to do this, see "How to Freeze Your Credit Files" at http://www.oag.ca.gov/privacy/info-sheets. Then, consider filing a complaint about Internet-related frauds, scams, and suspicious activity with the following organizations:

• The Federal Trade Commission - The Federal Trade Commission is the nation's consumer protection agency and collects complaints about fraudulent, deceptive, and unfair business practices. If you think you may be a victim of fraud, file a complaint with the FTC.

• spam@uce.gov - If you receive an email that you think may be a scam, forward it to the FTC and it will be stored in a database that law enforcement agencies use to generate legal cases.

• Your State Attorney General – In addition to the FTC, you can also file a complaint with your state Attorney General's office if you think you may be a victim of fraud. Your state Attorney General's office handles a wide range of complaints related to consumer protection.

• The Internet Crime Complaint Center – The IC3 is a partnership between the FBI, the Nation al White Collar Crime Center, and the Bureau of Justice Assistance, whose mission is to serve as a vehicle to receive, develop, and refer criminal complaints related to cyber-crime.

• reportphishing@antiphishing.org – In addition to forwarding spam to spam@uce.gov, you can also forward spam to reportphishing@antiphishing.org. The Anti-Phishing Working Group is a consortium of ISPs, security vendors, financial institutions and law enforcement agencies that use this email to fight phishing.

• http://www.bbb.org – The Better Business Bureau accepts complaints from consumers against businesses or services, and is dedicated to fostering an ethical business environment.

• National Crime Prevention Council – The mission of the NCPC is to be the nation's leader in helping people keep themselves, their families, and their communities safe from crime. To achieve this, the NCPC produces tools that communities can use to learn crime prevention strategies - including a podcast series for children and adults on the facts of cyber bullying, how to prevent it and manage it.

• National Center for Missing and Exploited Children – This non-profit organization has a Congressionally-mandated CyberTipline as a means for reporting crimes against children. Reports may be made 24-hours a day, 7 days a week online at www.cybertipline.com or by calling 1-800-843-5678.

• Department of Justice – The DOJ's Computer Crime & Intellectual Property Section tells you where to go to report hacking, password trafficking, spam, child exploitation and other Internet harassment.

• USA.gov: Reporting Internet Fraud - A list of official government resources to help you report, prevent, and learn about Internet fraud.

About The Author

Gary recently blew the lid on the how Russian, Chinese and Indian hackers are behind the top 10 flashlight apps specifically designed to collect and expose your personal information to cybercriminals abroad. Fox News Bret Baier's interview with Gary broke records for Fox with over 5m views. Gary is a consumer advocate who has been recently featured on ABC, Good Morning America, World News Tonight, NBC's Today, FOX News, CNBC and elsewhere for his expertise as a cyber security expert. He is Founder of SnoopWall, Inc., a cutting edge counter-intelligence technology company offering free consumer based software to secure personal data on cell-phones and tablets, while generating revenues helping banks and government agencies secure their networks. He has been extremely active in the INFOSEC arena, as the Executive Producer of Cyber Defense Magazine and a regular contributor to Hakin9 Magazine. He has patents and patents pending on his inventions for Computer and Network Security. He is a member of ISC2.org, CISSP® and Advisory Board of the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. He also advised the National Infrastructure Advisory Council (NIAC) which operates within the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace. Miliefsky is a founding member of the US Department of Homeland Security, served on the OVAL advisory board of MITRE and is a founding Board member of the National Information Security Group. Email him at ceo@snoopwall.com.