Prismstop.com LLC

11 STEPS YOU CAN TAKE TODAY TO PROTECT YOUR PRIVACY.

www.prismstop.com

Overview

Maintaining your privacy online has been always been a challenge, and with each passing day it seems to become more difficult. Companies are spending millions in identifying who you are, what you like and where you go through pervasive and subversive means, Internet Service Providers are seeing their client base as a potential goldmine of detailed data and the US government has a long and storied history of gathering all sorts of information on all of us.

To take on any one of these challenges to your natural right of privacy can seem daunting. As more of our lives move online many become jaded at the thought of having to perform basic security and privacy protection for every web site we visit. For example, a 2013 study by instantcheckmate.com showed that 73% of people use the same password for more than one web site, and 33% of people use the same password for EVERY web site.[1] Needless to say, this makes people's personal data less secure, their accounts easier to hack and the likelihood of their private information being made public increases.

Most Internet users are casual about their Internet usage. More of our time is spent online from our mobile devices – smart phones, tablets, ultrabooks and laptops. But are we good about protecting those devices? In a 2011 study by Lookout.com – a maker of smartphone security apps include provide lost phone services – an estimated $30 billion dollars' worth of smart phones are lost each year. [2]They based this on real usage of their services.

Do most users protect their devices in case they are lost or stolen? According to a McAfee/One Poll study 36% of users do not password protect their phone. From McAfee's blog, "for example, only one in five respondents have backed up the data on their smartphone and tablet, and more than one in ten (15%) save password information on their phone. This means that if their phone falls into the wrong hands, they risk opening up all sorts of personal information such as bank details and online logins to whoever finds the device." [3]– sobering thoughts.

In our homes we frequently feel "safe" on the Internet – we feel that we are in control. But are we? Your Wi-Fi router typically sits behind your cable modem, and does a number of jobs that make using the Internet easy for us. It is your gateway to the Internet - allowing us to roam around our homes using Wi-Fi anywhere, it provides a basic level of protection against hackers and might have some features that balance or prioritize certain types of traffic to ensure a good Internet experience. Is your router adequately protected? Have you disabled remote administrative access, have you changed the admin or root password to something highly complex? Is your home's Wi-Fi running the highest standard of encryption with a highly complex password? Have you ever updated the firmware on your router? Without these basic steps your home Internet connection is subject to hacks via Wi-Fi or over the Internet. And when your router is compromised, everything in your home is compromised – your laptops, smartphones, PCs, iPods, tablets and so on. In a 2013 article CNET reported findings from Independent Security Evaluators entitled "Top Wi-Fi routers easy to hack, says study" detailing how 13

[1] http://blog.instantcheckmate.com/is-your-password-really-protecting-you/
[2] http://usatoday30.usatoday.com/tech/news/story/2012-03-22/lost-phones/53707448/1
[3] http://blogs.mcafee.com/consumer/unprotected-mobile-devices

of the most popular off-the-shelf wireless routers could be exploited by a "moderately skilled adversary with LAN or WLAN access". [4]

Who are our adversaries in our effort to protect our privacy and our personal data? They are hackers, identity thieves, government officials and sometimes just people with too much time on their hands. With all that we do online – shopping, banking, social networking, paying bills and so on every Internet user represents an attractive and potentially lucrative target.

With the revelations about the US government's intrusive NSA programs – PRISM (designed to gather data from social networking sites, telephone companies, mobile phone companies and so on), XKeyscore (an easy to use front end application allowing NSA analysts to find all data gathered by PRISM with a phone number, email address, credit card number, etc.), and the latest batch of programs titled Blarney, Fairview, Oakstar, Lithium and Stormbrew as reported by the Wall Street Journal[5]. These programs together are capable of intercepting and analyzing approximately 75% of all Internet usage in the US.

With basic threat analysis one would have to conclude that the most likely threat to our privacy comes from our own government. While their intentions may be pure (to protect us from further terrorist attack, etc.) it also exposes information that you may wish to be kept private. There have been numerous stories in the media over the last several years including the Washington Post report of August 15, 2013 detailing how an internal NSA audit revealed that the agency violated their own rules for privacy thousands of times per year.[6]

Can we do anything about this? The answer is yes. Part of it means adopting new habits, and part of it means adopting new technologies. While there is no such thing as completely safe Internet usage (no more than you can be assured that you'll never have an accident at work) we can take some simple steps to dramatically improve our privacy and make it much more difficult to have our privacy compromised.

[4] http://news.cnet.com/8301-1009_3-57579981-83/top-wi-fi-routers-easy-to-hack-says-study/
[5] http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html
[6] http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html?hpid=z1

11 STEPS YOU CAN TAKE TODAY TO PROTECT YOUR PRIVACY.

#1. Realize that protecting your personal information is up to you, and that no one else can do it for you.

I know that sounds like the beginning of a 12-step program, but it is the most important step you can take. It takes time, effort and diligence but you have a right to your privacy, and a responsibility to protect it.

#2. Secure your browser.

The most popular web browsers in use today are Internet Explorer (by Microsoft), Safari (by Apple), Chrome (by Google) and Firefox (by Mozilla). All can be made more secure by following a number of FAQs available online, but if you're not using Firefox you might consider switching to it. It supports a number of privacy plugins including Adblock Plus and Electronic Frontier Foundation's HTTPSEverywhere and was not developed by companies that are actively working with the NSA (Microsoft, Google, Apple, etc.).

#3. Review your social networking permissions and sharing.

Most Americans use some form of social networking such as Facebook, Twitter, Pinterest, Google+ and so on. It is up to you to decide what information you want to share with family, friends and the public at large. Every social networking site is different and has various methods to secure your data – go through all that you use and see what information others can see about you. Is your phone number or address available to the public, have you posted pictures that you'd prefer remain viewed only by family or do you play games online that have access data you'd prefer they didn't? It takes some time and effort but if you are concerned about your privacy it is a necessary step to take.

#4. Begin changing your habits.

If you frequently post online, share pictures, use instant messaging and so on, take a moment to ask yourself if you're sharing more than you should, or if you are sharing anything you would not want your government to see. If you're conducting financially related activities, such as paying bills, banking or shopping is the web site trusted and do they support HTTPS (a protocol supported by web browsers and most internet applications to ensure security during transmission)? If you're being asked to provide personal information to open an account with a company or web site online, are they asking for more than you are willing to provide? The vastness of the Internet allows us as consumers the ability to find what we need and to be picky about who we do business with – make sure those you trust with your personal information are requiring the minimum data to conduct transmissions and that they have a trustworthy privacy policy in place.

#5 Use various e-mail addresses.

Most people have an email address that they received from their Internet Service Provider when they established service and use it for the majority of their email. This can quickly lead to increases is spam received, and email borne attacks by virus, malware, phishing and so on. If you're logging into or posting on sites you don't frequent or know a lot about consider using free email accounts such as

Hotmail, Yahoo or Gmail. While none of these can be trusted with your personal information (due to the NSA's monitoring within their data centers) they can be useful as "disposable" email addresses or even used a single time.

#6 Review your company or school's Internet Usage Policy.

Many large companies (and many small ones) use programs like Websense to log and track what their employees, students and faculty are doing on their networks. This type of privacy intrusion is usually tied to the Internet Usage Policy or terms of service. It is safe to assume that your usage is being logged and possibly monitored.

#7 Adapt good security practices on all your Internet connected devices, particularly mobile devices.

This means using a good security and privacy software suite like Symantec, McAfee or others, using complex passwords (a mixture of UPPER CASE, lower case, numbers and symbols no shorter than 8 characters in length) and your home network is highly protected. This protection begins at your Wi-Fi router and extends to every device you use. Ensure that your mobile devices are encrypted (see your user's manual or research online how to do this) and that they are protected by passcode, password, gestures, facial recognition, fingerprints (some smartphones support this) or other method. It is likely that logins and passwords are stored on your mobile devices and could compromise your privacy (and cause you to incur financial loss) if they fall into the wrong hands.

#8 Consider using a password management system.

A few companies have sprung up to handle the issue of managing all of our login IDs and passwords. This is an area definitely worth investigating and does not have to be expensive. For example Lastpass.com can create a complex password as you're setting up an account, store your login information, allow you to "audit" all of your passwords and works on virtually all web browsers, operating systems and mobile devices for $1 per month. Other password management companies provide similar services.

#9 Never reply to spam messages, never click on pop-up ads and be skeptical of every offer.

These are common sense measures that too many people forget about, or out of temptation disregard. You put yourself at great risk – so don't.

#10 Never use publically available Wi-Fi networks without strong encryption.

"Open" Wi-Fi networks are conveniences but represent a high degree of danger to your security and privacy. Simply put anyone on their network who is using some very basic hacking tools can log every keystroke you make, steal your passwords and potentially connect to your device and steal your information. Publically available hacker applications can do all of this and much more. If you must use their network use a Virtual Private Network service like those provided by Prismstop to ensure that your data is completely encrypted and unreadable by anyone on their network.

#11 Secure all of your home Internet traffic and the traffic on all of your mobile devices with Prismstop.

Prismstop provides a complete encryption, cloaking of your Internet address, firewall, identity theft protection and uncensored Internet access for every device in your home with our Secure Privacy Routers and Recommended Virtual Private Network Services. Prismstop Protection does not stop at your front door, but provides the same levels of protection on all of your mobile devices – smart phones, tablets, laptops and more – for the same price. You can use public Wi-Fi hotspots with confidence that your personal data is encrypted and secure.

Prismstop Secure Privacy Routers remove the inherent insecurity of off-the-shelf routers, are individually configured to our best practices standards and tailored to your particular requirements. We believe that you have a natural right to your privacy, and we want to help you protect it by providing a highly affordable and effective solution.

For more information visit Prismstop on the web at www.prismstop.com, our Facebook Page at www.facebook.com/Prismstop or follow us on Twitter @Prismstop.

prismSTOP

950 Walnut Bottom Road
Suite 15-169
Carlisle, Pennsylvania 17015

info@prismstop.com
855-PRISMSTOP