Knock, Knock, Knock!

Identity Thieves are at Your Virtual Doorstep Waiting To Get In

The Ultimate Guide to Securing Your Home Network

TECHHELP BOSTON

Table of Contents

The Ultimate Guide to Securing Your Home Network

1. Securing Your Wireless Internet Connection

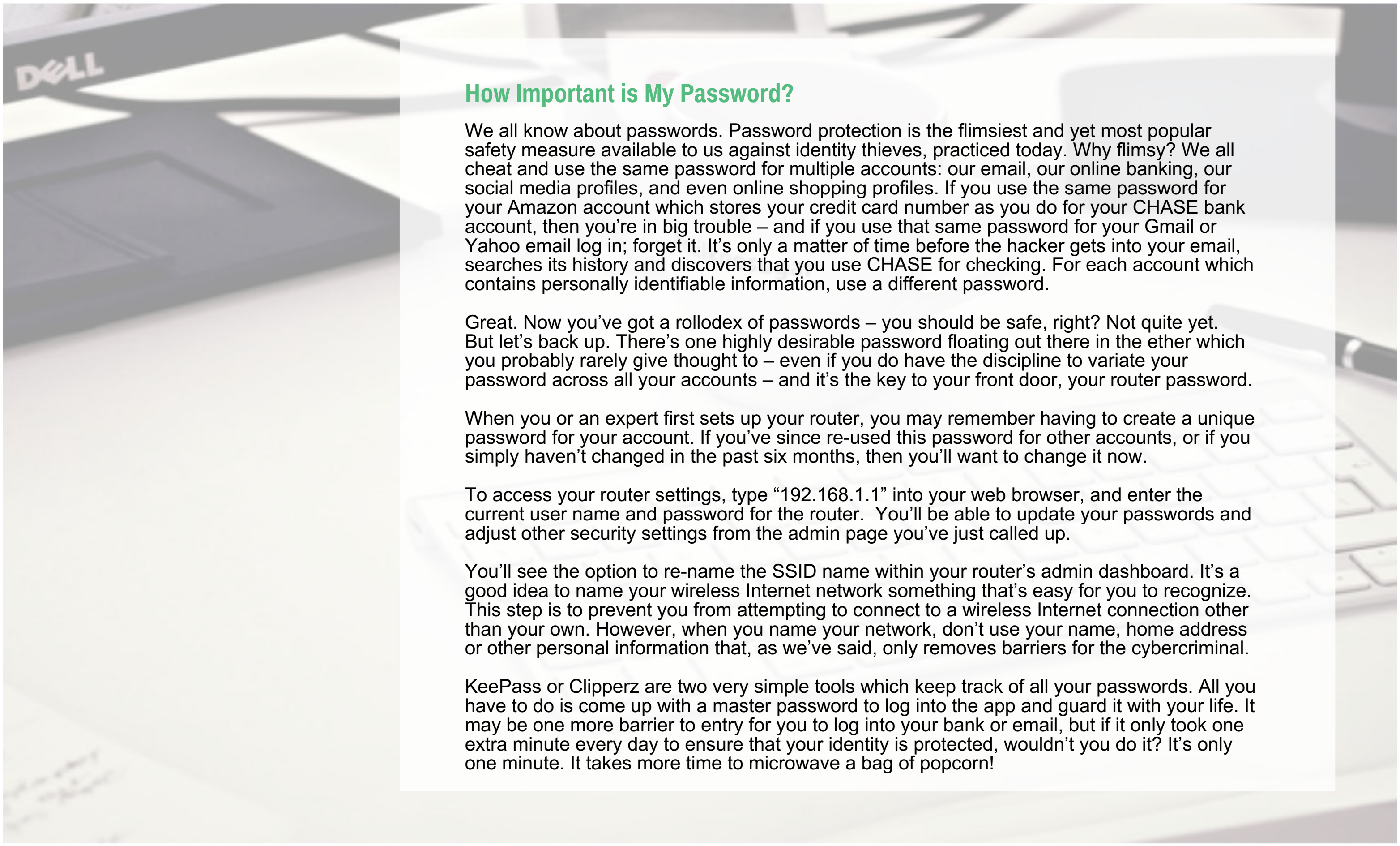
2. Protecting Your Home Computer

3. Browsing Online Safely

4. Apple, and Android, & Windows, Oh My!

Part One: Securing Your Wireless Internet Connection

What if there was a key to your front door that you weren't aware of -- would you feel safe? Whether you like it or not, wireless network security is the key to your front door, or more accurately, your wireless Internet connection with its multiple entry points is a set of keys which are all too easy to misplace. Unfortunately, there are cybercriminals out there with metal detectors hoping to scoop your keys up before you do.The best way to prevent the hackers from stealing your identity is to develop an awareness of your wireless Internet connection inherent vulnerabilities and how to patch them up.



How Important is My Password?

We all know about passwords. Password protection is the flimsiest and yet most popular safety measure available to us against identity thieves, practiced today. Why flimsy? We all cheat and use the same password for multiple accounts: our email, our online banking, our social media profiles, and even online shopping profiles. If you use the same password for your Amazon account which stores your credit card number as you do for your CHASE bank account, then you're in big trouble – and if you use that same password for your Gmail or Yahoo email log in; forget it. It's only a matter of time before the hacker gets into your email, searches its history and discovers that you use CHASE for checking. For each account which contains personally identifiable information, use a different password.

Great. Now you've got a rollodex of passwords – you should be safe, right? Not quite yet. But let's back up. There's one highly desirable password floating out there in the ether which you probably rarely give thought to – even if you do have the discipline to variate your password across all your accounts – and it's the key to your front door, your router password.

When you or an expert first sets up your router, you may remember having to create a unique password for your account. If you've since re-used this password for other accounts, or if you simply haven't changed in the past six months, then you'll want to change it now.

To access your router settings, type "192.168.1.1" into your web browser, and enter the current user name and password for the router. You'll be able to update your passwords and adjust other security settings from the admin page you've just called up.

You'll see the option to re-name the SSID name within your router's admin dashboard. It's a good idea to name your wireless Internet network something that's easy for you to recognize. This step is to prevent you from attempting to connect to a wireless Internet connection other than your own. However, when you name your network, don't use your name, home address or other personal information that, as we've said, only removes barriers for the cybercriminal.

KeePass or Clipperz are two very simple tools which keep track of all your passwords. All you have to do is come up with a master password to log into the app and guard it with your life. It may be one more barrier to entry for you to log into your bank or email, but if it only took one extra minute every day to ensure that your identity is protected, wouldn't you do it? It's only one minute. It takes more time to microwave a bag of popcorn!

A Great, Little Trick : Reduce Your Wireless Signal Range

Ten out of ten people who deploy Wi-Fi throughout their home think the bigger the range, the better. Yes. All the common wisdom concerning Wi-Fi suggests placing your router centrally within your home and away from signal barriers to improve its strength and reach. However, what if you live in a tiny little apartment or you have a personal policy against working in bed. You don't need a high signal range. Set the mode of your router to 802.11g rather than 802.11n or 802.11b or use a different wireless channel.

Here's another crazy idea. Turn off your router occasionally. If you know you're going out of town or won't be using the computer for a long stretch of time, don't leave it vulnerable to attack or piggybacking! Turn it off for peace of mind and lower electricity bills

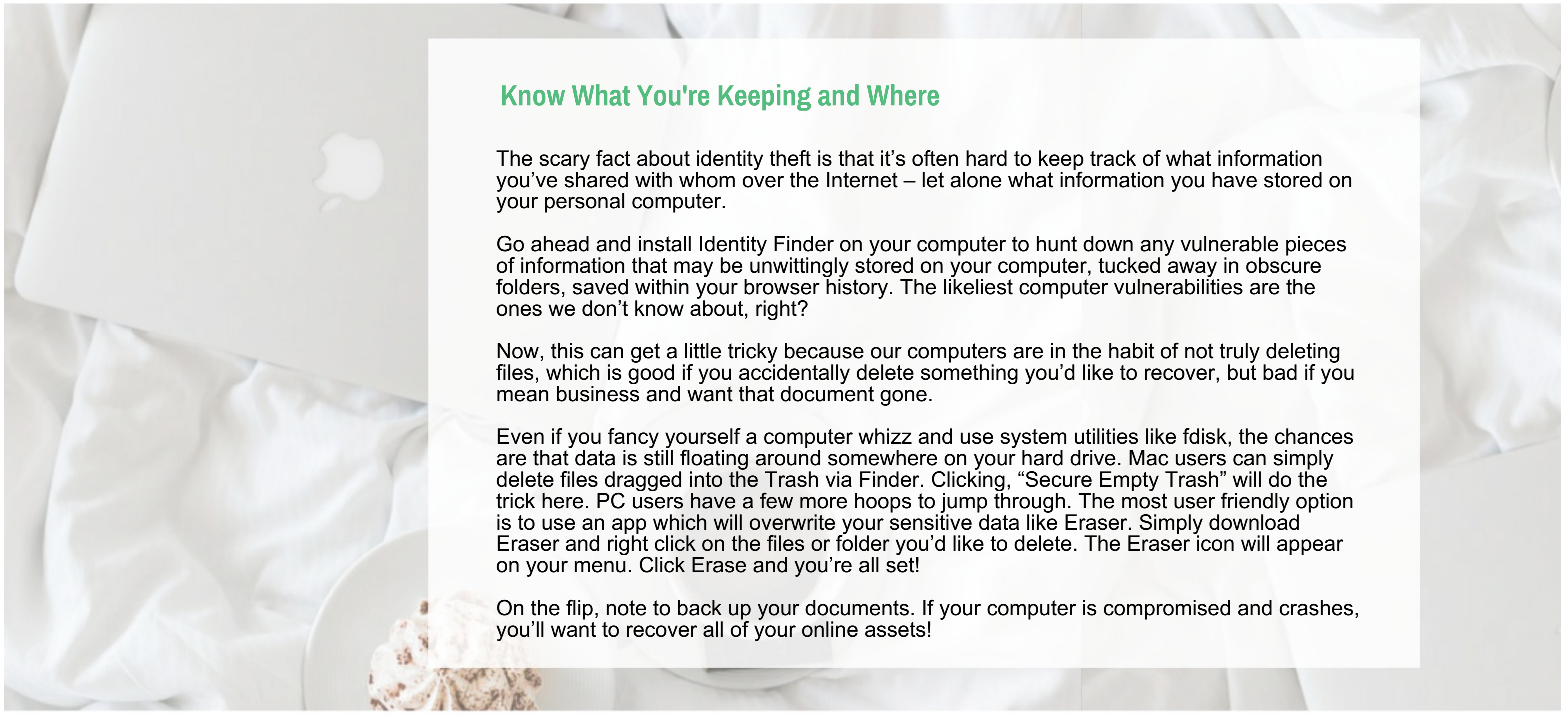
You'd Be Surprised: It's Very Easy to Enable Network Encryption

In order to prevent other computers in the area from using your internet connection, you need to encrypt your wireless signals. Don't let the word encrypt throw you off. It's very simple. When you took a look at your wireless network configuration page – you should have noticed the option to adjust the security method of your network, in order of security strength: WEP or WPA or WPA 2.

Why does your computer give you the option, if the two former methods are less secure? WPA 2 is the latest version and only compatible with devices manufactured after 2006. Ideally, you'd have a newer computer which is inherently more secure. Otherwise, you've got to deal with the equipment you have on hand.

Part Two: Protecting Your Home Computer

You've done all that you can to protect your wireless Internet network, but despite your best efforts, you're still not out of the clear. The most common issues homeowners run into when protecting their devices is user error.



Know What You're Keeping and Where

The scary fact about identity theft is that it's often hard to keep track of what information you've shared with whom over the Internet – let alone what information you have stored on your personal computer.

Go ahead and install Identity Finder on your computer to hunt down any vulnerable pieces of information that may be unwittingly stored on your computer, tucked away in obscure folders, saved within your browser history. The likeliest computer vulnerabilities are the ones we don't know about, right?

Now, this can get a little tricky because our computers are in the habit of not truly deleting files, which is good if you accidentally delete something you'd like to recover, but bad if you mean business and want that document gone.

Even if you fancy yourself a computer whizz and use system utilities like fdisk, the chances are that data is still floating around somewhere on your hard drive. Mac users can simply delete files dragged into the Trash via Finder. Clicking, "Secure Empty Trash" will do the trick here. PC users have a few more hoops to jump through. The most user friendly option is to use an app which will overwrite your sensitive data like Eraser. Simply download Eraser and right click on the files or folder you'd like to delete. The Eraser icon will appear on your menu. Click Erase and you're all set!

On the flip, note to back up your documents. If your computer is compromised and crashes, you'll want to recover all of your online assets!

Be Humble

There's a phrase in the computer world, 'path of least privilege,' which refers to how much access, you the user have to the backend of your device. Whether you're exercising the privilege or not, if you're an administrator then you have more access to the meat of your computer, the kind of data that cybercriminals salivate over.

Chances, are you don't really use your administrative privileges, so, why not log on as a simple user? If you're logged on as an administrator when a hacker attacks and gets through – you've just given him the keys to your front door, basement, garage, windows, and car.

At the very worst, a hacker will use their newly stolen admin access to create a new user account which also has admin access privileges. You're handing the keys to your front door to a stranger! Keep it simple. Only log onto your computer if you must, must, must perform a specific task and log out as soon as you're through. Otherwise, don't risk it.

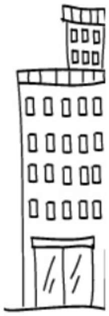
Never Forget: Your Computer is a Physical Thing

Why did you create a log in password for your laptop? To keep out anyone who might steal your physical computer and gain access to all of your personal information. You might want to consider installing a lock on the door to your office. It's just a thought. You can never be too careful.

Update Early and Often

It's tough to keep track of software updates. These days, the majority of updates are automated. You'll receive a little pop-up reminder on your computer as the clock ticks down to zero.

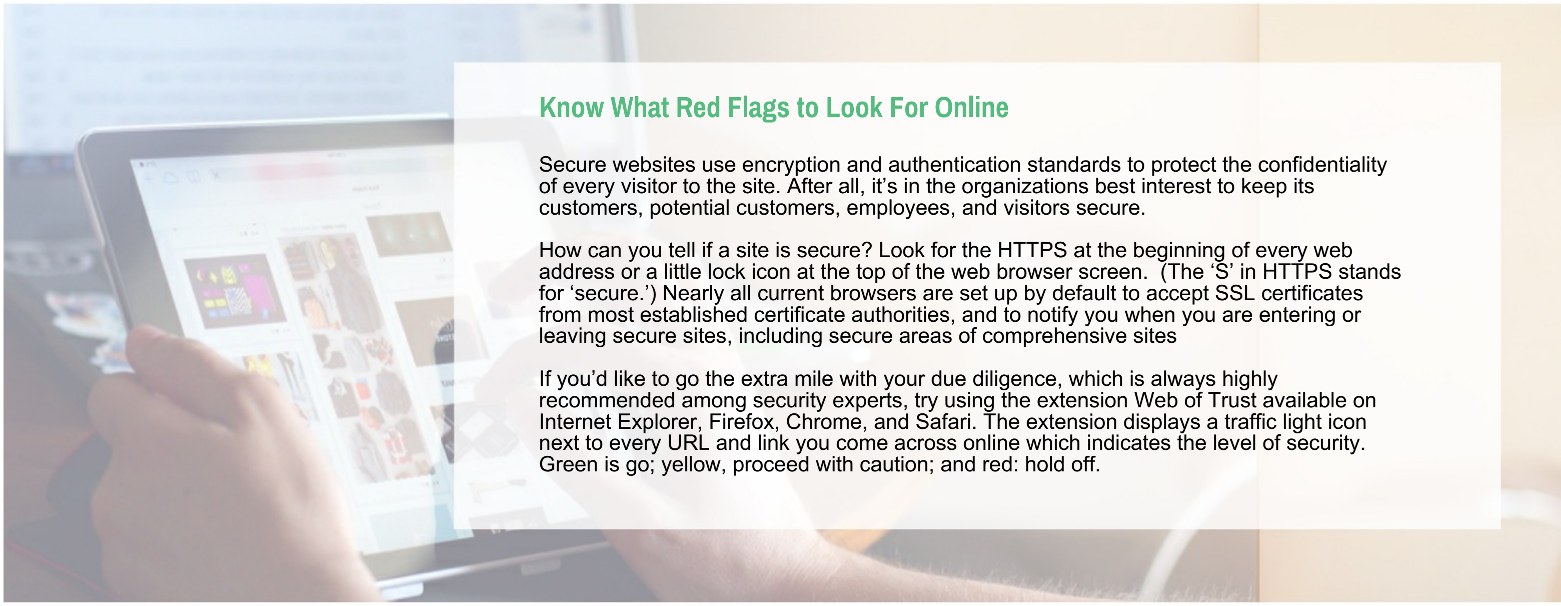
Your best course of action is to install an app that alerts you to nearing expiration dates. And, more importantly, to update when the time comes! Don't make it a habit of ignoring these alerts. Act on them.



Part Three: Browsing Online Safely

You've protected your router and consequentially the Internet connection it provides to your computer. You've protected your computer, both physically and upon logging on, its contents. There's one last step glaring weakness standing in between you and improved security: your browsing behavior.

We can arm ourselves with every defense against the wild, wild West that is the Internet, but without the proper strategies our tactics are easily rendered useless.



Know What Red Flags to Look For Online

Secure websites use encryption and authentication standards to protect the confidentiality of every visitor to the site. After all, it's in the organizations best interest to keep its customers, potential customers, employees, and visitors secure.

How can you tell if a site is secure? Look for the HTTPS at the beginning of every web address or a little lock icon at the top of the web browser screen. (The 'S' in HTTPS stands for 'secure.') Nearly all current browsers are set up by default to accept SSL certificates from most established certificate authorities, and to notify you when you are entering or leaving secure sites, including secure areas of comprehensive sites

If you'd like to go the extra mile with your due diligence, which is always highly recommended among security experts, try using the extension Web of Trust available on Internet Explorer, Firefox, Chrome, and Safari. The extension displays a traffic light icon next to every URL and link you come across online which indicates the level of security. Green is go; yellow, proceed with caution; and red: hold off.

Anti-Virus is Great, But Have You Heard of Anti-Exploit?

Anti-exploit programs harden your web browser against some of the most common types of attacks, based on behavior of potentially harmful programs and software.

The two most popular and free options for home users are Microsoft's EMET and Malwarebytes Anti-Exploit.

Be Wary of What You Share – Especially on Social Media

Remember that the Internet is a public resource and anyone can see what you post and you don't control what is archived and what is deleted.

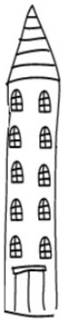
That means that you should never share any of the following information on social profiles: your Social Security number, your birthdate, your full address, your phone number, or your mother's maiden name.

The Single, Safest Browser is an Updated Browser

There really is no single, safest browser by design. However, there are several steps you can take to ensure that your browser of choice is as safe as possible. For one, if you use a PC, make sure that you're using a 64-bit version of your browser, rather than the less secure, 32-bit version.

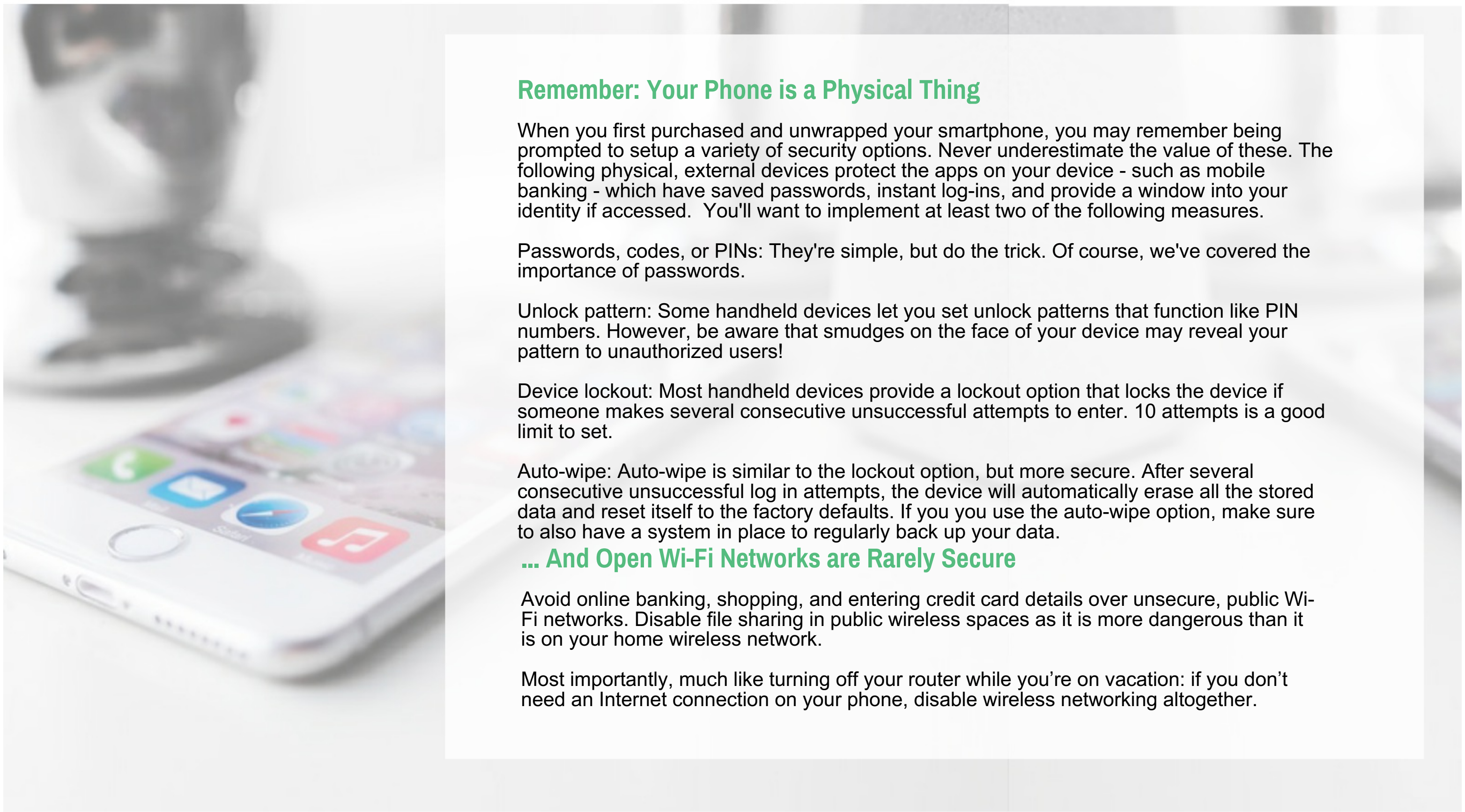
Google Chrome is available in both 32-bit and 64-bit versions, but there's a good chance you still have the 32-bit version installed. On Firefox, you'll have to use a developer build. Go into your browser settings to About or Properties. You'll see immediately which version you're running, with the option to download the latest update, if yours happens to be outdated. All web browsers available through Mac and Linux are 64-bit.

To save yourself future stress and chores, keep automatic updates enabled. In fact, you might even consider setting up Google alerts for your browser to stay apprised of any security issues or updates.



Part Four: Apple, and Android, and Windows, Oh My!

Remember that there is no single, safest browser? The same rule applies to your mobile device. There is no single, safest smartphone. Rest assured, you won't have to switch providers or transition to a new carrier to protect your identity against mobile identity thieves. Let’s start on the outside and work our way in.



Remember: Your Phone is a Physical Thing

When you first purchased and unwrapped your smartphone, you may remember being prompted to setup a variety of security options. Never underestimate the value of these. The following physical, external devices protect the apps on your device - such as mobile banking - which have saved passwords, instant log-ins, and provide a window into your identity if accessed. You'll want to implement at least two of the following measures.

Passwords, codes, or PINs: They're simple, but do the trick. Of course, we've covered the importance of passwords.

Unlock pattern: Some handheld devices let you set unlock patterns that function like PIN numbers. However, be aware that smudges on the face of your device may reveal your pattern to unauthorized users!

Device lockout: Most handheld devices provide a lockout option that locks the device if someone makes several consecutive unsuccessful attempts to enter. 10 attempts is a good limit to set.

Auto-wipe: Auto-wipe is similar to the lockout option, but more secure. After several consecutive unsuccessful log in attempts, the device will automatically erase all the stored data and reset itself to the factory defaults. If you you use the auto-wipe option, make sure to also have a system in place to regularly back up your data.

... And Open Wi-Fi Networks are Rarely Secure

Avoid online banking, shopping, and entering credit card details over unsecure, public Wi-Fi networks. Disable file sharing in public wireless spaces as it is more dangerous than it is on your home wireless network.

Most importantly, much like turning off your router while you’re on vacation: if you don’t need an Internet connection on your phone, disable wireless networking altogether.

✓ Advice You've Probably Never Heard

Whether you have a laptop or a Wi-Fi enabled phone, all your wireless devices have a unique MAC address (which has nothing to do with an Apple Mac) much like your computer has a unique IP address that allows it to connect to the Internet.

For an added layer of protection to your home network, add the MAC addresses of all your devices to your wireless router’s settings so that only specified devices can connect to your Wi-Fi network.

To enable MAC address filtering, first make a list of all your hardware devices that you want to connect to your wireless network. You can find the MAC addresses of your mobile devices under the network settings of each device.

Within your router’s admin dashboard simply add each MAC address and save the information! This will prevent any random and potentially harmful devices from connecting to the same network that your computer relies on for its Internet connection.

✓ Conclusion

What’s the secret to staying safe online? Staying informed. Know where your data is and how it’s being protected.We simply can't afford the alternative! Not with our identities at stake.

For more information about our team, free home technology resources, or to schedule a house call visit our FAQ page at TechHelpBoston.com

TECHHELP BOSTON