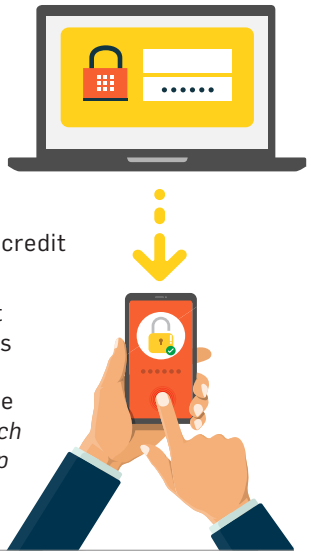
MILTON'S BEST PRACTICES FOR YOUR PERSONAL CYBERSECURITY

I hope you find these tips useful. As new information becomes available, I will keep this document updated and share it via our website and our blog.

Best of luck,

Milton Bartley
Co-founder,
President & CEO
ImageQuest

These are my simple and (mostly) free recommendations to ensure you keep your personal data and that of your family safe against today's most prolific cyber threats.



1 The first and most important thing you should do is activate ***2 Factor Authentication (2FA)*** on every account that offers it. Some services also refer to this as ***Multi-Factor Authentication***, or ***Two Step Verification***. At a minimum that should be your personal email account(s), social media account(s), bank account(s), retirement/brokerage account(s), and credit card account(s).

Setting up 2 Factor Authentication is relatively straight forward for most services and accounts. This site offers a comprehensive list of available 2FA sites. ***https://twofactorauth.org***. If you can't find your specific service there, you can also search for it. *(Example: in your search box type Xfinity 2FA and you will find the Xfinity two step enrollment page).*

2 The second thing you should ensure is that your home network is secure. There are some simple things for you to check.

1. FIREWALL

Unless you are running a business through your home network or are doing something ultra-secure (that others would also know you are doing) on your home network, the out-of-the-box settings on your Internet Service Provider's modem or the wireless router you installed provide adequate protection.

If you need a more advanced firewall on your home network, you likely already know that – as well as how to set it up properly.

2. ANTIVIRUS SOFTWARE

Every computer you own (Mac or PC) should have a good Antivirus solution on it. Typically, a good AV solution is one you paid for, but there is always an exception.

Every computer you own (Mac or PC) should have a good Antivirus solution on it.

- On Windows computers, I recommend ***Webroot SecureAnywhere*** which you can find here: ***https://www.webroot.com/us/en/home***

- They offer three versions. The basic version for $29.99 is excellent for almost every user following our other security best practices. If you have more than one computer to protect, they offer volume discounts when you get to the checkout cart.

- On Mac computers, I recommend the ***Sophos Home Free*** program which you can find here: ***https://home.sophos.com/download-mac-anti-virus***. They offer a Premium version for $50, but the free version is excellent for almost every user following our other security best practices.

3. PATCHING/UPDATING

Every computer and mobile device (iPhone, iPad, Android) should be updated regularly. We call that patching. The simplest way to accomplish that is to turn on automatic updates.

- On Windows computers, make sure ***Windows Update*** is set to automatically download and install updates. You can find your Windows Update settings by clicking the Start button and then typing ***Windows Update***. The settings are self-explanatory. (Tip: If you have a Windows 10 device, Windows Update is set to automatic unless you turned it off.)

- On Mac computers with the latest Mac OS operating system, you can also turn on automatic updates. To do so, go to ***System Preferences*** -> ***App Store*** and check all the boxes, including the ones to "***Automatically check for updates***," "***Download newly available updates in the background***," and "***Install OS X updates***."

- On your iPhones or iPads, Apple does a good job of notifying you when there is a new version of the operating system to install. When those update messages appear, simply follow the prompts to install the latest software. If you want to manually check for updates at any time on an iOS device, go to ***Settings*** -> ***General*** -> ***Software Update*** and it will tell you if there is an update to install.

- On your Android devices, the process can be a little more manual – depending on your operating system version. See chart below:

ANDROID UPDATES

1 Connect your device to WiFi

2 Open your device's settings

3 Scroll down and tap *About Device*

4 Tap *Update*

5 Tap *Check for Updates*

6 Tap *Update*

7 Tap *Install*

- Lastly, are your Internet of Things (IoT) devices. These include, but are not limited to items like Apple TV, Roku, Xbox One, Nest thermostats or cameras, SimpliSafe home security systems, and the list goes on and on. Simply put, if you have these devices on your home network, you need to ensure they have the latest security updates. Many of these devices are automatically updated by the manufacturer. Some, however, require you to manually initiate the process. You will need to check with your individual device manual(s) for complete information. Regardless, make sure you keep them on the most current software.

4. WEB CONTENT FILTERING

- Web content filtering is exactly what it sounds like. Filtering web content on your home network. This is particularly important if you have children in the house and you want to control or limit their access to certain websites or types of content.

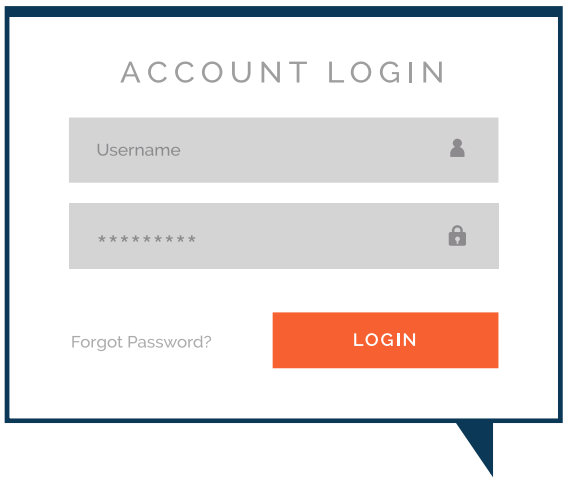
- I recommend Cisco's OpenDNS product – free for home use. I use this at my home and it just works. There are two options available. The first – called OpenDNS Family Shield – simply blocks adult content and requires no sign-up to use. The second – OpenDNS Home – is more customizable, but requires you to register a free account to fully utilize the solution. You can read about both and take your pick. The first option is probably adequate for most home users. Here's the link to the product page. ***https://www.opendns.com/home-internet-security/***

NOTE: You will need to be able to log into your modem or router at your house to deploy either solution. It is very simple to make the changes, and they provide step-by-step instructions.

---

3 The third thing you need to do is find and utilize a secure password tool. Keeping up with passwords is almost an impossible task today. We all know not to write them down, share them, put them in Excel documents, etc., but without alternatives, many still do.

My recommendation is a ***password manager***. There are dozens out there, but these three stand out above the rest. They are safe, simple, and relatively inexpensive. A few even offer a free tier.



Preferred Password Managers

1PASSWORD | ***https://1password.com/***

I have used this for over five years. I started with an individual account and later added a Families account that I share with my wife. It costs $60 per year, but well worth it in my opinion. Simple to set up – and mobile support for iPhone and Android.

DASHLANE | ***https://www.dashlane.com/***

Dashlane is another solid choice that several of my clients use. There is a free version that limits you to a single device (computer or phone). If you want the full features, it is $40 per year.

Keeping up with passwords is almost an impossible task today. We all know not to write them down, share them, put them in Excel documents, etc., but without alternatives, many still do.

The only way to truly protect yourself is to freeze your credit with all three reporting agencies: Equifax, Experian, and TransUnion.

---

4 In the wake of the Equifax breach – and given the current threat landscape – you really should freeze your credit with the three credit reporting agencies. The only way to truly protect yourself is to freeze your credit with all three reporting agencies: Equifax, Experian, and TransUnion. This is not something to be undertaken lightly, however, given the severe and very real threat of identity compromise, I strongly feel this is the best course of action.

More on credit freeze from the FTC: ***https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs***

Credit freezes are not [currently] federally regulated. This link will take you to a site that explains the laws and potential fees by state. ***http://www.elitepersonalfinance.com/credit-freeze-laws***

Here's where you can go to sign up for a freeze at each of the three major credit bureaus:

- Equifax - ***https://www.freeze.equifax.com/Freeze***. Or call 1-800-349-9960.
- Experian - ***https://www.experian.com/freeze***. Or call 1-888-397-3742.
- TransUnion - ***https://www.transunion.com/credit-freeze/place-credit-freeze***. Or call 1-888-909-8872.

You will need to be patient. All three companies' systems and switchboards are overloaded. It may take you several attempts.

Lastly, if you have minor children, I highly recommend you freeze their credit as well. Adolescent Identity Theft is on the rise. All three reporting agencies and most states allow a parent or guardian to place a freeze on a minor child's credit. Here's where you can go to find out more and to enable a credit freeze for your minor children.

- Equifax - *https://www.equifax.com/personal/education/identity-theft/freezing-your-childs-credit-report-faq/*
- Experian - ***https://www.experian.com/blogs/ask-experian/requesting-a-security-freeze-for-a-minor-childs-credit-report/***
- TransUnion - ***https://www.transunion.com/fraud-victim-resource/protected-consumer***