BEALL
FINANCIAL PLANNING

Digital Safety Checklist

BASIC STEPS TO BEGIN TO LIMIT YOUR RISK OF HAVING YOUR IDENTITY, PRIVACY AND CREDIT COMPROMISED.

BEALL
FINANCIAL PLANNING

"When we do not know our true identity as powerful creators, we are susceptible to being used and manipulated."
Bryant McGill Voice of Reason

This document is meant to be a guide to some of the most basic things you can do to protect your Identity, your Credit, and your Privacy. It is not a comprehensive document for we are not aware of every threat you face nor can we prevent every threat. It is meant to reduce your risk. We are not experts on the subjects we cover. We are all amateurs in this digital age. I've grown up with computers since I was in 8th grade. My children have grown up surrounded by them all their lives. My youngest started using the iPad the day they arrived. He was 2 ½ years old. He's almost 8 and has had his own computing device for years. We all have different levels of comfort and experience with computers, programs, and other digital devices. I don't expect you to do everything in this guide but to use it as a reference and take the steps you are most comfortable with doing. I've also put the least fun but often most important one last in the document. Passwords are both a necessity and a nuisance and are necessary. This checklist covers the physical world, the internet, and the hardest part - our mindset.

Feel free to read it, share it, discuss it, and provide us some feedback on it so we can continue to improve it.

BEALL FINANCIAL PLANNING

Contents

1/ The Physical World

The things you can touch, your mail, phones, computers, and digital devices are ways that a corporation or a criminal can gather information about you. In many ways the first two items on the checklist; The Mail and The Phone are some of the easiest to implement and have the potential for a dramatic improvement on the quality of your life.

The Mail – Opt Out

Taking this step not only reduces the risks to your Identity but your wallet as well. The mail that is delivered to your mailbox by the United States Postal Service is one of the many resources of the Identity Thief. They can get the pre-approved credit card offers right from your mailbox when you are not at home and you never know that it happens. You can eliminate this risk by opting out of the offers. You will not only reduce your risk of identity theft but you will also save a few trees as well. This step will also limit insurance solicitations you receive in the mail.

Mail Resources:

Option 1/ the 5 year Opt Out: Call 888-5-OPT-OUT (888-567-8688) or visit www.optoutprescreen.com these are run by the four major credit reporting bureaus. The four bureaus are Equifax, Experian, Innovis, and TransUnion.
Option 2/ the permanent Opt Out: visit www.optoutprescreen.com and make sure you sign and return the Permanent Opt-Out Election Form that should be provided after you start this request.

The Phone - Do Not Call Registry

Tired of unwanted phone calls interrupting your life? Register your home phone and mobile for free at the National Do Not Call Registry

Phone Resources:

https://www.donotcall.gov/
You can also submit a complaint as well as verify your registration. The website is run by the Federal Trade Commission.

Your Computer and its accessories

Considering the number and variety of devices that have been available for purchase over the years this part can only be generalizations. There are a few specific steps you can take but the ultimate outcome will be determined by the devices you own. I've narrowed down the type of computers to two Windows (a PC) and Apple. We will review Windows first then Apple.

Windows based Computers

1. Make sure that you have installed all of the latest updates and security patches for your version of Windows. If you are still using Windows XP it is time to upgrade your computer. Adjust the computer settings to automatically install updates.
2. You will want an antivirus program installed; set it to automatically update.
3. Make sure any other programs you use are fully up to date as well.

Apple based Computers

1. Make sure that you have all the updates installed.
2. While you may have not felt the need for an antivirus program in the past, there are some security vulnerabilities in the Operating System that hackers have been trying to exploit. You will want to get an antivirus program installed and the settings configured to automatically update.
3. You will also want to make sure any other programs you use are fully up to date.

I found a couple of articles regarding anti-virus programs for both Windows and Apple computers. They will soon be out of date. They are a good starting point for determining which program is right for you.

Windows Antivirus Review:
http://www.pcmag.com/article2/0,2817,2372364,00.asp

Apple Antivirus Review:
http://www.tomsguide.com/us/best-antivirus,review-2588-6.html

Your Modem /Router /Wi-Fi Device

It's that electrical box with lights that your internet connection comes through. You may have a separate device for each or it may be combined into one device. You want to keep the software that comes preinstalled on the device up to date. This software is referred to as Firmware.

[Firmware = permanent software programmed into a device]

Never buy one of these devices that isn't new. For a real world example, a Thief bought a bunch of new routers, installed his malicious software along with the manufacturer's software onto the device. The Thief then sold them cheaply on the internet at an auction resell site. Presto! The thief had access to everything that the new owner did on the internet including usernames, passwords, date of birth, and any other information that was sent over the internet connection of the unsuspecting victims.

If you use a cable modem to receive your internet you may not be able to update the devices firmware as updates would be handled by the cable company. This is because the internet service provider wants to control the connection between your computer and theirs for security purposes.

One thing I have found useful is to take a picture of your device where it tells you the model number and serial number. I use my phone for this. It is a lot easier to look at your phone screen or a downloaded picture from your digital camera than it is to crawl under your desk or flip a device over to get to the little sticker that has the information. Then when I am at the computer I pull up the picture and can zoom in on the numbers to better be able to read them. You can then do an internet search for your device's manual. It will contain the instructions on how to log into your device and change the settings. It will also tell you how to reset the device if necessary.

Quick summary:

1. Encrypt your Wi-Fi Network. WPA2 is the strongest WEP is the weakest and shouldn't be used.
2. Give your Wi-Fi Network a strong password. See Section 5 of this document for more information on setting strong passwords.
3. Change the default settings
4. Turn off Remote Access related features
5. Update the device's firmware. The latest firmware should only be downloaded from the manufacturer of your device.
6. Log out properly.

Some of you are scratching your head and wondering what I am talking about. That is OK, we all have are different levels of technical skill. Fortunately, the trend is towards easier to use and implement fixes which will benefit all of us. Read the resource article linked to below for the full details. It even includes a note on how the Apple Airport is different from most other devices.

Device Update Resource Article

http://www.cnet.com/how-to/home-networking-explained-part-6-keep-your-network-secure/

Printers and other desktop devices:

If it connects to the internet it is vulnerable to hackers. Nothing is secure forever. Similar to the Router, Modem, Wi-Fi device you will want to read the manual that came with your printer or other device for how to update the device if necessary. More modern devices come with a little program that will automatically check for an update to your device every month or week depending upon the setting. Not all devices do this however so we have to do a little bit of work to find out.

1. Determine your devices current settings by referring to the manual. You can also do a search online for the manual by typing into your browser's search box the name and model of your device and the words "User Manual".
2. Compare that to what the manufacturer says is the latest firmware. Note: Some printers and devices come with programs that allow you to check for updates. This is the quick and easy way to upgrade the software.
3. If you need to install a firmware update follow the steps provided by the manufacturer.
4. Turn on any encryption
5. Use a complex password to secure access to the device
6. If it uses a profile/user name like Administrator or Admin and it lets you change the name consider doing so. This makes it harder for someone to hack your system since most people don't change the name.

USB thumb drives

Do not insert one into a computer that you use that is vital to you. This is especially important regarding the ones you are given at trade shows, find in the parking lot, or that has been out of your hands and sight. If you must use one that is given to you consider the following steps.

1. Plug it into a computer that isn't connected to the internet and that isn't vital and have an antivirus program and malware program scan it.
2. Copy the file you need after the scan onto a USB device you trust is clean and transfer the data to your computer.

If you think this bit sounds a bit crazy or too extreme and you can't be bothered that is understandable. It is time consuming and more difficult to do it this way. I would recommend that you read these two articles from 2014 before you make a final decision:

This Thumbdrive hacks computers. "BadUSB" exploit makes devices turn "evil".
http://arstechnica.com/security/2014/07/this-thumbdrive-hacks-computers-badusb-exploit-makes-devices-turn-evil/

This is a bit more technical but it might be fun for you to do in your spare time. It's a step by step method of creating your own Thumbdrive to steal passwords.
http://lifehacker.com/create-a-usb-password-stealer-to-see-how-secure-your-i-1650354166

Mobile Devices

I've focused on the two most common mobile devices. Basic Security is simple on these devices. You just have to be willing to do it. Things have gotten a bit easier with Apple's Touch ID which allows you to use your fingerprint to use the device instead of typing in a passcode. Android has more options than just a passcode so it comes down to personal preference.

Apple:

Step 1. Install and turn on the Find my iPhone app using your Apple ID
Step 2. Turn on Passcode Lock with an automatic logout time.
Step 3. Use Apple Keychain.
Step 4. Encrypt your backups with a different password. You are backing up your devices right? You've only been told for a couple of decades now. It should be a habit.
Step 5. Turn on Two factor authentications for everything you can.

For more on security for Apple devices go to their website: https://support.apple.com/en-us/HT201303

Android:

A bit more here:
Step 1. Do not save all your passwords to the device particularly your banking passwords.
Step 2. Use the built in security including screen locks and encryption
Step 3. Lock your apps using a free app like App Lock
Step 4. Be aware of your app features and permissions. Not all apps in the Play Store are safe.
Step 5. Use a mobile security App. Only download from a reputable source.
Step 6. If you share a device use multiple user accounts.
Step 7. Make your device trackable. Some apps even allow you to remote wipe the phone if it gets stolen.
Step 8. Enable Remote Wipe. If your phone is stolen don't let them get your information.
Step 9. Use complex passwords.
Step 10. Turn on Two factor authentications for everything you can.

For more on Android Security you can go here: https://source.android.com/devices/tech/security/

Remove unwanted Computer Programs

If you have had your computer for a number of years there may be old programs that are out of date and you no longer use. They might be for an old printer or the 2008 Tax filing program you used. Use your computer's uninstall program to remove these from your computer. It will free up space and removes vulnerabilities from your computer. One program you might consider removing that is almost always in need of a patch or update is Adobe Flash Player. My personal amateur recommendation is that you uninstall it and see if it affects your web browsing. If it does then you can download and install the latest version and TURN ON AUTOMATIC UPDATES. Sorry didn't mean to shout but it is not the most secure program in the world and exploits often happen before you can patch it. Now if you just have to have it go to your Chrome browser settings and select the "let me choose when to run plugin content" for Firefox: the extension Flashblock will help, in Internet Explorer go to settings>safety> and make sure there is a check next to ActiveX filtering.

2/ Cyber Security

Social Media

Today, one of our most valuable possessions is our identity. Corporations spend billions of dollars to collect, research, and trade minute details about our individual lives in the desire to be more profitable. The most innovative way this is being done is through Social Media where we trade our privacy and details of our lives so that we can remain connected to our friends.

Your identity has value not just to you but to criminals as well. Information about you can be used to manipulate you, steal from you, and blackmail you. It is a big business to provide services that will allow you to protect your identity. Often these services are provided by the very companies that collect and collate data about you.

The fourth amendment to the Bill of Rights states:

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

It is supposed to protect us from the government but it does not provide the same protection from corporations or criminals.

FaceBook

They have gotten better at letting you choose what is seen by others but they still collect a ton of information about you.

1. Click on the icon that looks like a padlock and go through the privacy checkup, who can see my stuff, and who can contact me options to select what works best for you.

Google

Google has a new privacy shield that lets you go through your options for protecting your information much like FaceBook. I highly recommend your turn on two factor authentication. The rest is based on personal preferences.

[Two Factor Authentication is an extra layer of security that requires at least one more bit of information beyond just a username and password. It is often a code that can be delivered by text to your phone.]

Other Social Media

This is where security and privacy is a mindset. Be aware of what information you are telling the world. When you are on vacation, how often you travel for business or pleasure, and whether you work from home or at an office. It is all valuable information and affects your security profile.

Email Tracking

The current threat level for compromising your security is low but it does have an effect on your privacy.

Currently, companies who do not value your privacy can put a picture in an email they send you that is the size of 1 pixel. A pixel is smaller in size than the period at the end of this sentence. You will not see it. You will not know it is there. Yet it will tell them a host of information about you from the time you open the email, to the program used to open the email, the device you used, and other data. It's a neat bit of work.

If you check your email using Chrome

1. install a tracker blocking extension like Pixelblock and Ugly Mail
2. adjust your settings in Chrome Settings>General>Images *adjust the setting to ask before displaying images*

If you check your email using Outlook

1. Go to Tools > Options > Preferences tab > E-mail Options and then choose "Read all standard mail in plain text". You can also include messages signed with a digital signature, choose "Read all digitally signed mail in plain text"
2. Then go to Tools > Options > Preferences tab > E-mail Options > Tracking Options and choose the "Never send a response" radio box.

If you check your email using another program:

1. Check your setting they should be similar to Outlook's procedure.

If you check your email using another browser:

1. The two extensions might also be available for the browser or search for tracker blocker and review the options.
2. You can adjust the settings in your browser to ask before displaying images.

Browsers

This is a personal preference. I currently use Chrome as my main web browser. I run Facebook on Opera (a chrome like browser). Internet Explorer is used for limited items usually business related. I use a version of Chrome called Epic Privacy Browser for sensitive searches and client related activities. I used to use and recommend Firefox but I do not personally use it anymore. At home I set my kids up with their own personal browser. (IE, Firefox, Opera) that way it is personalized to each and we can adjust settings based upon their age. They do grow up quick with varying levels of technical ability. I used to use safari on the PC for Facebook but I kept having serious stability issues with my operating system so I stopped. Your experience will be different.

Find a browser or browsers you like and make sure they are the latest version. Chrome is automatically updated and the others are moving in that direction. This allows the corporations to rapidly patch security vulnerabilities when they arise along with other improvements.

You can also apply add-ins or extensions to your browser. These are little programs that integrate into your browser that can be used to improve your experience. One of the most well-known is Ad Blocker which does what it says; it block ads when you are surfing the web. Some extensions will slow down your browsing experience but usually not a noticeable amount.

The number one extension for Chrome I recommend is HTTPS Everywhere extension. It was created by the Electronic Freedom Foundation. This turns on the default for your browsing to the more secure HTTPS protocol instead of the less secure HTTP protocol. They are found here https://www.eff.org/

> *In your browser address bar look at the website part of the address before www it will usually say either HTTP or HTTPS. HyperText Transport Protocol Secure*

Digital Tool Resources

These two websites have a host of links and resources that you can use to better protect yourself. Security-in-a-box is a guide to digital security created for activists and human rights defenders throughout the world. You can find information here: https://securityinabox.org/en
Journalists often travel to unsafe parts of the world or need to protect their sources. Here's a good place to start to find out the tools they use: http://ijnet.org/en/blog/8-tools-greater-digital-security-2015

3/ Identity

Your Credit

The first thing we need to secure is your Credit Identity. This is a prime target for identity thieves. They want your info so they can open up credit in your good name and spend it on themselves. The first thing you need to do is get the free copy of your credit report you are entitled to receive annually from the credit bureaus. The three major credit bureaus are Equifax, Experian, and TransUnion with Innovis being the fourth credit bureau.

Step 1. Get a copy of your credit report from the three major bureaus by going to www.annualcreditreport.com or by calling 877-322-8228. Every other "free" report offer website is trying to sell you something usually a credit monitoring service.

Step 2. If you are not going to need credit in the next year to get a loan then you will want to enact a credit security freeze. This step involves a little bit more work and a small fee but it will stop creditors from being able to view your credit files. Few corporations will make a loan to ID thieves if they can't pull your credit file. Since each pull of your credit file lowers your credit score a freeze will keep your score higher. You will want to place the freeze at all four credit bureaus. Once you have completed the procedure at each bureau you will receive a PIN number from them that you can use to thaw your credit file in the event you need to access your credit file in the future. Store your four PINS in a safe place that you have access to and will remember the location where they are stored.

Limitations: If you thaw your credit file to get a loan you will have to pay to refreeze it. This will still be cheaper than a years' worth of credit monitoring. For More Information on fees which vary by state go to: https://help.equifax.com/app/answers/detail/a_id/75/~/security-freeze-fees-and-requirements

Step 3. If you are unable to do Step 2 then you might consider putting a fraud alert, extended fraud alert or if you are in the military an active duty alert on your file. A fraud alert tells the credit lenders or service providers to contact you by the method you chose when setting up the fraud alert (usually by phone or mail) before granting credit. The extended fraud alert is available to those who have an official record or police report showing that you've been the victim of identity theft. The active duty alert is available for 12 months if you are on active duty in the military and you also removed from the pre-approved credit offers for 24 months.
Limitations a fraud alert lasts only 90 days but can be renewed indefinitely. While the alert is active it tells the creditors and service providers to notify you they are not legally obligated to do so.

Resources:
Equifax Online Dispute: https://www.ai.equifax.com/CreditInvestigation/home.action
Experian Fraud Center: https://www.experian.com/fraud/center.html
TransUnion Fraud Alerts: http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page
Innovis Fraud & Active Duty Alerts: https://www.innovis.com/personal/fraudActiveDutyAlerts

Digital ID

Eventually we will have a Digital ID. The country of Estonia has already had one for 15 years! They vote and pay their taxes online. The conduct transactions and a host of other activities with a secure digital ID. They also have the lowest rate of credit card fraud in the Eurozone.

By giving each of us a simple individual identification number known as a social security number the government is one of the key entities in making us less secure. How many times at doctor's offices have you been asked for your social security number? Yes, your doctors are targets for hackers as they have a wealth of information available to be stolen. They have your full name, address, medical history and payment details. They also have your Social Security number if you gave it to your doctor. All it would take would be a mischievous patient left alone with a computer. They could insert a thumbdrive and have access to the computers until it was discovered and removed. It sounds implausible but you and I tend not to think in terms of security risks.

The leading solution to fix this problem and the one used by Estonia is known as a blockchain. You can better understand what blockchain is by reading this:
http://recode.net/2015/07/05/forget-bitcoin-what-is-the-blockchain-and-why-should-you-care/

I confess that I find the blockchain to be complex and hard to wrap my mind around. The more I study it and read about it the more intrigued I become. It has the potential to eliminate some of the digital identity problems we are currently facing.

Stolen Identity

If you are currently dealing with a stolen ID then go to
https://www.identitytheft.gov
It is run by the Federal Trade Commission. It has more detailed information than I could provide on how to handle a stolen identity.

4/ Mindset

Habits

Security and Privacy are about good habits. Once you learn and establish good habits then it only takes a few minutes a month to keep yourself more secure than the average consumer.

1. Automatic installs of patches and updates. Once you have these settings set you should only check for optional updates about once a month for your Windows program. If you hear about a major threat then review it and see if you need to do anything.
2. Turn on Two Factor Authentication whenever possible. This makes it much harder for someone to steal your identity or compromise your accounts than just a password.
3. Be suspicious of USB thumbdrives you didn't buy new personally.
4. Be suspicious if your computer or browser acts different. Run a deep thorough scan with your antivirus, malware, & spyware software. It may take an hour or more. Losing your identity takes days and weeks to fix. It is also a lot more stressful.

Be Informed

I am an amateur at digital security. I make no guarantees that this will keep you safe online or anywhere else. I can't guarantee that it will protect your identity, privacy, your possessions, or anything else. I rely on others who have put much more time and effort into researching these issues than me. I have a whole section devoted to them and I encourage you to read them.

There are a couple of great individuals who write about security and in no small part are inspirations for this document.

The first is Brian Krebs. His writings can be found at http://krebsonsecurity.com/
The second is Bruce Schneier. His writings can be found at https://www.schneier.com/

The great thing about them is that you can take what is useful and applicable to your life and probably ignore the rest.

Automatic Pay

Automate your bills, where you can, so you have less information that can be intercepted in the mail.

Step 1. Have a credit card that gives you points, miles, cash back or another reward for using it.
Step 2. For every recurring bill set it up so that the above credit card which will be paid off every month is the one billed. DO NOT use your checking account and DO NOT use your debit card. If they don't have access to your checking account they cannot drain the account of funds.

Electronic Statements

Your brokerage accounts and retirement accounts should have the option for you to receive a notification that your statements are ready by email. You will want to select this option now. It will once again reduce the chance an ID thief will get your vital information.

5/ Passwords

There is lots of advice out there. Some of it is out of date. The worst part is that you feel you have to write it down somewhere in order to remember it which defeats the purpose. You can develop your own system for passwords just make sure it complex and the longer the better.

Complex=Upper & Lower Case letters + Numbers + Symbols at least 12 digits long.

Just be aware some websites don't allow you to use symbols or have other requirements. It makes remembering everything a pain in the arse.
If you want to check how secure your password is go here:
https://howsecureismypassword.net

Password Managers

You could leave a majority of this hassle behind by considering a password manager. A password manager takes the hassle out of remembering dozens or hundreds of passwords. Some of the top rated ones are

LastPass https://lastpass.com
DashLane https://www.dashlane.com
KeePass www.keepass.info
RoboForm www.roboform.com/everywhere

One small note of caution. These sites are prime targets for hackers as they obviously hold the key to your identity. That being said the corporations also put every bit of effort into protecting the information because otherwise they are out of business.

For Further Reading:

US-CERT – United States Computer Emergency Readiness Team
https://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf
Here's Google's Advice
http://www.google.com/goodtoknow/online-safety/passwords/
Here is the Advice from the UK
https://www.cyberstreetwise.com/passwords

6/ References

When researching this I came across a number of great websites you can check out that cover most of these issues and more in greater detail. There is a lot of information out there on videos and websites. Always try to find a trusted resource.

Her Majesty's Government in the UK has a great one:
https://www.cyberstreetwise.com
The United States government has a growing set up sites and services:
https://www.identitytheft.gov/ Identity Theft
https://www.us-cert.gov/ United States Computer Emergency Readiness
http://www.dhs.gov/topic/cybersecurity Department of Homeland Security
Other Organizations
https://www.staysafeonline.org/ Stay Safe Online
http://www.idtheftcenter.org/itrcbod.html ID theft center

In closing, I would like to thank Bob Veres (@BobVeres) who was the original inspiration for this document. Originally, it was supposed to be an article in our newsletter. It quickly became too large to fit. A quick thanks to Joel Bruckenstein (@fintechie) and Bill Winterberg (@BillWinterberg) as well who do a lot of tech writing for advisors. As I finished writing this I realized that as much as I put in; I also left a good bit out. (Encryption, VPNs, etc.)

Stay Safe out there.

Jim Beall (@jameslgb)
President
Beall Financial Planning, Inc.