CHECKLIST – PROTECTING YOUR DEVICES, ACCOUNTS AND DATA

This is a Checklist of basic device, account and data security measures that you and your organization's staff can take to prevent or mitigate many common security and privacy vulnerabilities. There are many more things you can do to safeguard your digital life, but these steps really are the essential ones to protect you from the most common threats to your personal data and privacy. This is important stuff.

Who is this Checklist for? This Checklist is intended for individual users of technology devices (laptops, phones, tablets), online accounts (email, social media, cell phone, bank accounts) and online data (personal or business confidential information), and for small- to mid-size businesses for their individual users.

How to Use this Checklist? (or … Feeling Overwhelmed? Not to Worry!) This Checklist is organized into 3 parts:

(1) Securing your Devices (protect your laptops, desktops, tablets and phones from the most common security problems).
(2) Securing Your Accounts (protect against account access problems for email, social media, cell phone, bank accounts).
(3) Securing Your Data (protect against unwanted people seeing, using, stealing / misusing and corrupting your data).

This Checklist contains a lot of steps and can seem daunting. Still, most of these steps will take just a few minutes to complete. While all these steps are recommended, incremental implementation will simplify your life. Prioritize by starting with Part 1 (Devices), before proceeding with Parts 2 (Accounts) and 3 (Data). It's ok if you don't get this done today – you already waited this long!

This Checklist is provided by Mirsky & Company, PLLC (mstreetlegal.com), a law firm in Washington, DC.

This checklist is not legal advice and not a substitute for legal advice, and is provided for information only. This Checklist is written broadly and is not necessarily comprehensive for you or your business. Please be sure to consult with appropriate technology and legal professionals with knowledge of your organization in order to implement these measures.

For an interactive "Quiz" version of this Checklist, please go to:

https://forms.gle/ScxZ8NZv25UAK8nt8

	Action Item	How to Do This?		Why Do This? (more info than you may want, but if you're curious ...)
Part 1:	**Securing Your Devices** (things you can do - easily and quickly - to protect your laptops, desktops, tablets and phones from the most common security problems).			
□	**1. Update your computer's operating system** (and enable auto-updates if available).	How to set up auto-updates for your Mac.	How to set up auto-updates for your PC	Keeping your computer's operating system updated is one of the most important ways to keep it (and your data) secure. Operating system updates regularly contain numerous security updates. Bad guys seeking to exploit vulnerabilities frequently take advantage of devices that have not been updated recently.
□	**2. Update your computer's software apps** (such as anti-virus software, Zoom, VPN, Adobe or Microsoft products, etc.)			Same rationale as with keeping your operating system updated, see above.
□	**3. Install anti-virus and malware protection on your computer and other devices** (where available).			Install and regularly update the anti-virus and malware protection on your computer to provide additional level of protection while browsing on the internet and potential threats from ransomware attacks.
□	**4. Set up an unlock code or passphrase on your computer and other devices** (at least 6 characters long).			
□	**5. Update your phone/tablet's operating system** (and enable auto-updates if available).	How to update iPhone or iPad O/S	How to update Android O/S.	Same rationale as with keeping your laptop or desktop computer updated, see above.

	Action Item	How to Do This?			Why Do This? (more info than you may want, but if you're curious ...)
□	**6. Update your phone/tablet's software apps** (and enable auto-updates if available).	How to update iPhone / iPad apps	How to update Android apps		Same rationale as with keeping your operating system updated, see above.
□	**7. Enable automatic session timeout on your computer and other devices.**	How to set up automatic session timeout for your Mac.	How to set up automatic session timeout for your PC.		Setup your device to log out or lock after a period of inactivity such as 5-10 minutes. This covers the situation where you walk away from your computer without logging out or shutting down, and prevents bad actors from accessing your important stuff.
	Securing Your Accounts (easy and quick things you can do today to protect against unwanted people causing you account management and account access problems for your email, social media, cell phone, bank accounts, etc.)				
□	**1. Use a password manager to store all your passwords** (such as 1Password, LastPass, Keeper, etc.).	A decent "how-to" article (with video) on how to implement using a Password Manager.	LastPass	1Password	You may have dozens of online accounts, making effective management of all of the various passwords impossible. Using the same password for all of your accounts is definitely not a good solution! Instead, a password manager can generate a unique, complex password for each account and password management. Password managers such as LastPass and 1Password help you create, store and enter login credentials. They will create passwords that are long, random and unique and store them (encrypted) on your device.

	Action Item	How to Do This?			Why Do This? (more info than you may want, but if you're curious ...)
□	**2. Make the "master password" (for your password manager) at least 16 characters and unique.**	Passphrase generator: https://www.useapassphrase.com/	Passphrase generator: https://www.worksighted.com/random-passphrase-generator/		The "master password" for your Password Manager is the single password that you have to remember in order to access your Password Manager account. (And by remembering that one master password, you don't have to remember any other passwords.) The password manager will use that master password to encrypt/decrypt your individual website passwords. But be careful!! If someone obtains or guesses your master password, they may be able to decrypt all your individual passwords. So, the master password must be long and unique, but also memorable. You will use it every day. To create a strong master password, use a passphrase generator (a few are listed in the resources section here).
□	**3. Enable 2-factor authentication (2FA) for your password manager.**				The simplest way for you to secure your Password Manager account is to add a single extra level of access protection via requiring a second confirmation of your identity. That's what 2FA does.
□	**4. Enable 2-factor authentication (2FA) for your various important accounts** (email, cloud storage, social media, banking etc.).	Example: Instagram	Example: Gmail	Example: Microsoft Outlook/Hotmail	2-factor authentication (sometimes called 2FA, “two step”, “multi-factor authentication” or MFA) adds an additional and critical step to a website’s login process. 2-factor systems use your smartphone or a hardware device to identify you to the website.

	Action Item	How to Do This?	Why Do This? (more info than you may want, but if you're curious ...)
□	**5. When you use 2FA, set it up to avoid text-based (SMS) authentication.** (Instead, use an app-based authenticator (like Google Authenticator), or 1-time passcodes displayed on trusted devices, or security keys.)	Google Authenticator 2FA for Apple Devices	Be careful with SMS-based 2FA!! Many websites offer SMS-based (text message) 2-factor access. Unfortunately, it is possible to steal someone's phone number (called "SIM-swap attacks"), and then to intercept 2-factor codes sent via SMS. You can decrease your chances of someone gaining access to and taking over your phone number by adding a PIN code or password to your wireless account. T-Mobile, Verizon and AT&T all offer the ability to add a PIN code. An even better approach – if practical for you and your organization to do – is to avoid SMS-based 2-factor authentication altogether and instead use app-based authenticators (like Google Authenticator), one-time passcodes displayed on trusted devices (like for Apple devices) and security keys.
□	**6. Enable a PIN on your mobile carrier account** (not same as your phone's password).	How to enable my PIN on my AT&T Mobile account. How to enable my PIN on my T-Mobile account. How to enable my PIN on my Verizon account.	PINs for your mobile account are not the same as passwords for your phone or tablet because passwords are generally tied to the devices you use. If your phone carrier allows you to set a login PIN, you should enable the feature because having a PIN makes it harder for attackers to take over your account. For example, an attacker with your social security number could use this information to contact your carrier and transfer your account information to a new device (by changing your SIM card). And that in turn will allow the attacker to access login codes that are sent to your phone when you use 2-factor authentication to access your various online accounts. Having a PIN enabled on your account will prevent attackers from accessing your mobile provider account and transferring your account credentials to a new device.
	Securing Your Data (easy and quick things you can do today (or start doing today) to protect against unwanted people seeing, using, stealing / misusing and corrupting your data).		

	Action Item	How to Do This?		Why Do This? (more info than you may want, but if you're curious ...)
□	**1. Set up and enable a local (on-site) automatic backup of files, passwords and configurations on your laptop or desktop computer, phone and tablet devices** (using either Time Machine (for Macs) or File History (for PCs)).	(For Macs) How to set up and use Time Machine	(For Windows) How to set up and use Window's File History	External drive backup (i.e. on-site) avoids the problem of dependency on a cloud provider's security and/or your loss of passwords or passwords being compromised. But since a hard drive is in the same physical location as your computer and may actually be physically networked to your machine, it therefore has the same security vulnerabilities as your computer and same risk of damage (from water or fire or other corruption) or physical loss (from theft, misplacement etc.). Therefore, at a minimum, good idea to encrypt that external device. For Apple users, Time Machine creates (and updates) a backup of your computer's entire hard drive. For Windows users, Windows 10's File History creates backup versions of your files. Both Time Machine and File History store backups of your files on an external hard drive.
□	**2. Set up and enable a remote (off-site) automatic backup of files, passwords and configurations on your laptop or desktop computer, phone and tablet devices, using a cloud backup service** (such as Backblaze, IDrive and Carbonite).	How to set up and use a remote (offsite) automatic backup service		Having a remote (i.e. off-site) backup avoids the problem of physical theft of your backup device or water or fire damage if you keep the backup device in the same location as your computer, and achieves the separate backup goal of redundancy. Redundancy is important (i.e. implementing both offset and onsite backup options), in light of the impossibility of guaranteed backup protection and better to assure availability. Note also that Dropbox, Box, Google Drive and Microsoft OneDrive are not technically backup services, but rather file syncing services allowing file sharing across multiple devices, plus they don't offer private-key encryption protection.

	Action Item	How to Do This?	Why Do This? (more info than you may want, but if you're curious ...)
□	**3. Encrypt your computer’s hard drive** (Macs (using FileVault) and PCs (using Bitlocker)).	How to encrypt your Mac hard drive using FileVault How to encrypt your PC hard drive in Windows 10	Encrypting your hard drive itself (as opposed to its contents) means that users need an encryption key in order to access the hard drive or anything on the hard drive. This is great, because it means that if someone steals your computer, they can’t really do much with the contents of the hard drive without also having the encryption key (password). The only serious flaw with this is that once you’ve de-encrypted the hard drive using the encryption key, anyone who has access to the computer at that point would also have unprotected access to the hard drive and its contents. So, for example, if you access the internet via an unsecure network, your (now) de-encrypted hard drive may be accessible to any snooper. That’s why you should also separately encrypt any sensitive files prior to storing them, to secure any individual files that could be improperly accessed by anyone getting around FileVault and any other hard drive encryption.
□	**4. Encrypt all external storage devices that you use for backups or for any other uses** (such as USBs and External Hard Drives).	How to encrypt an External Drive How to encrypt a USB flash drive	Secure these external devices with encryption especially if used to store personal or sensitive information. You can either purchase encrypted USBs or encrypt them yourself by following the instructions under "How to Do This?"

	Action Item	How to Do This?	Why Do This? (more info than you may want, but if you're curious ...)
□	**5. Encrypt all files containing sensitive or other confidential data before storing or sharing them** (and avoid sending passwords together in the same emails with the sensitive files or use a different method entirely such as SMS or telephoning recipients).	How to password-protect Microsoft Office documents How to password-protect PDF documents	File password-enabling protects the actual files containing sensitive information on your device and helps comply with regulations such as HIPAA, PCI-DSS and GDPR. File encryption can be done by password-protecting Microsoft Office documents and PDFs. Note also that encrypting sensitive files prior to storage also protects those same files from improper access during transit, for example when sent as email attachments. Of course, take care when sharing passwords with recipients of sensitive files, by avoiding sending passwords together in the same emails with the sensitive files or using a different method entirely such as SMS or telephoning the recipient.
□	**6. Use email services only from providers that offer at least Transport Layer Security (TLS) encryption.**		Most major email service providers currently offer TLS encryption, including Google (Gmail/G Suite), Yahoo! and Microsoft (Outlook/Outlook 365). While TLS encryption provides significant protection against uninvited access to messages, TLS is not the same as end-to-end encryption, because (for example with Gmail) Google still retains the ability to scan (and does scan) emails to filter out spam and phishing attacks.
□	**7. Install the "HTTPS Everywhere" Extension in web browsers you use.**	How to get and install the "HTTPS Everywhere" Extension	As an additional layer of protection when accessing websites that don't use SSL encryption, "HTTPS Everywhere" is a Firefox, Chrome, Microsoft Edge and Opera extension that strengthens the encryption between your device and websites. (Not - yet - available for Safari.)