### Personal Computer Security Checklist

This is a basic overview of personal computer security practices as would be relevant to the majority of users.

* Basic PC and Device security
  + Always keep your OS updated
  + Stay with currently supported OSs where possible
  + Encrypt the drives of devices that leave the home
    - Look into a drive encryption solution for your OS of choice
    - See “Drive Encryption Tools and Resources” below for more information
  + Do NOT plug in USB devices you do not own
    - Likewise do not give random people USB devices if alternatives are available
    - USB devices can pretend be anything they want
      * This is by design, USB was intended for convenient use of devices you own
    - USB Drive alternatives for transferring data to other people:
      * Somewhat ironically, file upload service is usually safer
        + "Cloud" Services such as Dropbox or Google Drive
        + Self-Hosted Services like OwnCloud, SeaFile, or Pydio
      * If you need physical transfer, other mediums that are storage-only are safer
        + SD Cards
        + Optical Disks (DVD, CD, Blu-ray)
  + Always keep backups of important data
    - If practical, keep at least two different forms of backup:
      * On-site (at home)
      * Off-site (somewhere else or on a "cloud" service)
    - At least one backup should be completely detached from the active system when not being updated
  + Different users need different accounts, avoid sharing logins where practical
    - Sharing accounts often accidentally teaches bad habits
    - Account sharing also happens to sometimes cause personal conflicts between users
* General Software/Application Concerns
  + Always research a piece of software before buying or installing
    - See if the software is reputable
  + Installing Software:
    - If practical, prefer to use your OS's app store or repository instead of installing the software manually
    - I you have to buy a physical copy of the software, try to buy it from a reputable source
    - If downloading the software using a browser is needed:
      * Prefer the software’s official website over mirrors
      * Prefer HTTPS over HTTP for downloads
      * Verify the URL before downloading
* Authentication and Authorization
  + Passwords
    - You should only memorize the password to your machine and password manager (if applicable), all other passwords should be stored somewhere.
    - Password Storage Options:
      * Password Manager
        + Not perfect, but better for most scenarios than memory
        + A password manager should be your preferred method of handling everyday passwords
        + Makes it easy to have a different password for each service/application, minimizing the impact of data breach
      * Physical Storage
        + Also not perfect, but still better for most scenarios than memory
        + Is a good backup for device and password manager passwords
        + Treat the same as you would jewelry or social security cards
    - For the passwords you must memorize, "passphrases" consisting of multiple random words are recommended
* Your vocabulary is one of the largest pools of things you have memorized, and most people have already trained themselves to memorize and type words
* Use 4 or more randomly selected words (6 is recommended)
* Look into the “diceware” method of picking random words
  + - See “Password Management Tools and Resources” below for word lists, password managers, and 2FA tools
  + Two-Factor Authentication (2FA)
    - Use two-factor or two-step authentication where practical
    - Order of preference (best to worst):
      * FIDO Universal 2nd Factor (U2F)
      * Time-based One-time Password (TOTP)
      * Email Codes
      * SMS Codes
    - Keep a copy of your 2FA backup codes in a safe place if applicable, particularly when using U2F or TOTP
    - TOTP may be used alongside U2F, which is helpful if you have devices that do not support U2F such as smartphones
    - See “Two-Factor Authentication Tools and Resources” below for 2FA tools and applications
* Web Browsing
  + Browser preferences
    - Chrome is preferable for most use cases
    - Edge is a big improvement over IE and should be your second choice
    - Firefox is behind but has been improving considerably as of late 2017
  + Browsing Habits:
    - Prefer HTTPS over HTTP, especially for logins and other sensitive info
    - Always check the URL before typing in passwords and other sensitive information
    - Bookmark commonly used important sites and prefer those bookmarks over links
* Email
  + Your email account is one of your most important
    - Your email is used as your “identity” for creating other accounts
    - This should be your most protected online account
    - Your email account is one where you’ll really want to use a long passphrase and/or 2-Factor Authentication
  + Be wary of attachments
    - Contact with the sender via other means to verify they sent the attachment if practical to do so
    - If suspicious, preview using a web client such as Gmail or Outlook Web
      * This allows you to preview an attachment while making it harder for it to do anything malicious

**Password Management Tools and Resources:**

* EFF Wordlists for Random Passphrases: <https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases>
* Password Managers:
  + 1Password: <https://1password.com/>
    - Windows, Linux, Mac, Android, and iOS
    - Online storage
  + LastPass: <https://lastpass.com/>
    - Windows, Linux, Mac, Android, and iOS
    - Online storage
  + DashLane: <https://www.dashlane.com/>
    - Windows, Linux, Mac, Android, and iOS
    - Local file storage with optional online storage
  + KeePass 2 and compatible ports/variations:
    - All KeePass 2 applications use local file storage unless otherwise noted.
      * An online storage service like Dropbox or Google Drive can be used with KeePass 2 files if needed.
    - KeePass 2: <http://keepass.info/>
      * Windows, Linux, and Mac
    - KeePassX: <https://www.keepassx.org/>
      * Windows, Linux, and Mac
    - KeePassXC: <https://keepassxc.org>/
      * Windows, Linux, and Mac
    - KeePass2Android: <https://github.com/PhilippC/keepass2android/>
      * Android
    - MiniKeePass: <https://minikeepass.github.io/>
      * iOS
    - KeeWeb: <https://keeweb.info/>
      * Desktop (Electron) and Web App
  + BitWarden: <https://bitwarden.com/>
    - Windows, Mac, Linux, Android, and iOS
    - Online storage
  + RoboForm: <http://www.roboform.com/>
    - Windows, Mac, Android, and iOS
    - Local file storage with optional online storage
  + Enpass: <https://www.enpass.io/>
    - Windows, Mac, Android, and iOS
    - Local file storage with optional online storage
  + Padlock: <https://padlock.io/>
    - Windows, Mac, Android, and iOS
    - Local file storage with optional online storage
  + Pass: <https://www.passwordstore.org/>
    - This is mainly a Linux and BSD command-line password manager for more technical users, but it has GUIs and cross-platform ports available.
    - Local file storage with the option of using a Git repository
      * An online storage service like Dropbox or Google Drive can also be used with Pass files if needed.

**Two-Factor Authentication Tools and Resources:**

* Two-Factor Authentication Sites/Services List: <https://twofactorauth.org>
* Email Providers that support U2F or TOTP Two-Factor Authentication:
  + Gmail: <https://www.google.com/>
    - TOTP and U2F
  + Outlook.com: <https://outlook.live.com/>
    - TOTP
  + FastMail: <https://www.fastmail.com/>
    - TOTP and U2F
  + Zoho Mail: <https://www.zoho.com/mail/>
    - TOTP
  + Tutanota: <https://tutanota.com/>
    - TOTP and U2F
  + ProtonMail: <https://protonmail.com/>
    - TOTP
  + mailbox.org: [https://mailbox.org/](https://mailbox.org/en/)
    - TOTP and U2F
* TOTP Apps:
  + Authy: <https://authy.com/>
    - Android and iOS
    - Online backup available
  + Last Pass Authenticator: <https://lastpass.com/auth/>
    - Android and iOS
    - Online backup available (needs LastPass)
  + Duo Mobile: <https://duo.com/product/trusted-users/two-factor-authentication/duo-mobile>
    - Android and iOS
    - Online backup available
  + Authenticator Plus: <https://www.authenticatorplus.com/>
    - Android and iOS
    - Online backup available
  + Authenticator: <https://mattrubin.me/authenticator/>
    - iOS only
    - Open Source
  + FreeOTP: <https://freeotp.github.io/>
    - Android only (iOS version not well maintained)
    - Open Source
  + Google Authenticator: <https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>
    - Android only (iOS version not well maintained)
* FIDO U2F Security Keys:
  + Yubikey (Yubico): <https://www.yubico.com/>
    - FIDO U2F Security Key on Yubico store ($18): <https://www.yubico.com/product/fido-u2f-security-key/>
    - FIDO U2F Security Key on Amazon ($18): <https://www.amazon.com/dp/B00NLKA0D8/>
  + Thetis: <https://thetis.io/>
    - Thetis store ($20): <https://thetis.io/products/thetis-fido-u2f-security-key>
    - Amazon: <https://www.amazon.com/dp/B06XHTKFH3/>
  + U2F Zero: <https://u2fzero.com/>
    - Purchase pre-built on Amazon ($9): <https://www.amazon.com/U2F-Zero/dp/B01L9DUPK6>
    - Do it yourself instructions: <https://github.com/conorpp/u2f-zero/wiki>
  + HyperFIDO (HyperSecu): <https://www.hypersecu.com/products/hyperfido>
    - Amazon ($10): <https://www.amazon.com/dp/B00WIX4JMC/>
  + NitroKey: <https://www.nitrokey.com/>
    - FIDO U2F on NitroKey Store (15.00 €): <https://shop.nitrokey.com/shop/product/nitrokey-fido-u2f-20>

**Drive Encryption Tools and Resources:**

* + Windows:
    - Guide for BitLocker: <https://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/>
    - VeraCrypt: <https://www.veracrypt.fr/>
  + OS X:
    - Guide for FileVault: <https://support.apple.com/en-us/HT204837>
  + Linux:
    - See your distro’s documentation for details on full disk encryption
      * Most popular distributions have full disk encryption as an option during installation, which handles the setup for you
  + Android
    - Android should have encryption by default on newer devices as long as you have a pin or password
    - Guide to enabling drive encryption on Android: <https://www.androidauthority.com/how-to-encrypt-android-device-326700/>
  + iOS
    - iOS has encryption enabled by default as long as you have a passcode

**Other Useful Sites and References:**

* Have I Been Pwned: <https://haveibeenpwned.com/>
  + This site collects publicly available data breach information and adds them to a searchable database that can help you find out whether you have an account that may have been compromised.
  + Also offers email notifications if your email address shows up in a data breach
* Electronic Frontier Foundation’s Surveillance Self-Defense Guide: <https://ssd.eff.org/>
  + A guide to security and privacy by the Electronic Frontier Foundation
  + More focused on privacy than this checklist
* The Motherboard Guide to Not Getting Hacked: <https://motherboard.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide>

**Relevant Articles:**

* Troy Hunt - Password managers don't have to be perfect, they just have to be better than not having one
  + <https://www.troyhunt.com/password-managers-dont-have-to-be-perfect-they-just-have-to-be-better-than-not-having-one/>
* Martin Shelton - Shields Up: Developing Security Skepticism
  + <https://source.opennews.org/articles/shields-developing-security-skepticism/>