Pretty Good Security Tips

Jonah Aragon – www.jonaharagon.com – jonah@aragon.ventures

Password and Account Security

- ❑ **Get a password manager!**

  1Password (my personal recommendation, https://1password.com/) starts at $3/month.

  LastPass (https://lastpass.com/) has a free plan, with $3/month premium functionality.

  Can I just write them down on paper? Writing down your passwords is better than using the same one for each service, but using a password manager gives you a built-in password generator when you sign up for a new account, and it makes signing in more convenient, which means you're more likely to use longer passwords...

- ❑ **Use long passwords.**

  Length matters more than complexity, for instance "surprise-cell-often-seem" will be more secure than "$3rdC7!".

- ❑ **Don't trust your browser.**

  Only store passwords in your password manager, don't save them in your browser. Disable auto-saving passwords in your browser now.

- ❑ **Reset all your passwords now.**

  If you've just been hacked you'll need to reset the passwords of **all** your accounts, especially if you reused passwords in the past. Login everywhere and create new passwords with your password manager.

- ❑ **Enable Two-Factor Authentication (2FA**)

  Strong passwords alone can't always protect your accounts: Enable 2FA whenever possible. Most accounts will support some or all of these options (from least to most secure): SMS, a "TOTP" app like Google Authenticator or Authy, or a hardware security key.

  Do not use SMS 2FA unless it is your only option, it's better than nothing but still insecure.

  You can find out who supports 2FA at https://twofactorauth.org/

Email Security

- ❑ **Use Gmail**

  Unless you're hosting your own email, Google is the most secure public email provider. Because all your accounts will be tied to your email address, this is incredibly important.

  iCloud is a good second choice if you don't want a Google account and will only use Apple devices to access your email.

- ❑ **Follow the Password Security tips**

  Even if you don't secure anything else, make sure you secure your email. Use a long password you've never used before, enable 2FA, and everything else mentioned above.

- ❑ **Gmail: Advanced Protection Program**: https://landing.google.com/advancedprotection/

  If you require the most secure setup possible, enable Google's Advanced Protection. This setup restricts your Google/Gmail account heavily and requires you to login with special hardware security keys (a ~$50 purchase), but it is very secure: Google employees use this protection themselves, and no Google employee account has been hacked since it was introduced.

- ❑ **Disable remote image loading**

  If your email client automatically loads images, you can be tracked by any number of malicious actors. Disable loading images by default in your email client and only load images from senders you trust.

Phone Security

- ❑ **Use a strong lock screen PIN**

  Make sure you have a 6-digit PIN (at an *absolute minimum*) set on your phone's lock screen. Make sure this PIN is secure (i.e. not your birthday or 111111, 123456, etc.). You can use a fingerprint scanner or Face ID (on iOS, do not use Face Unlock on Android) so you don't have to enter it too often.
  Android users: use a PIN or password instead of a pattern lock.

- ❑ **Android: Avoid third-party app stores**

  Only use the Google Play Store on Android phones. iOS users don't have to worry about this, because the only app store that can run is the Apple App Store.

- ❑ **Stay up to date**

  Make sure you're on the latest version of iOS or Android your phone can get, this will make sure any security bugs that are known are patched up and secured.

- ❑ **Use an iPhone or Google Pixel**

  If you're able to get a new phone, the two most secure consumer products on the market are the Apple iPhone and the Google Pixel. This is because they receive security/software updates for many years, and they have special security hardware (the Secure Enclave on iPhone and the Titan M on Pixel devices) to keep the phone secure. Other manufacturers like Samsung, LG, etc. commonly don't support their phone's software for long, if at all, leading to many Android devices on the market having significant security bugs.

- ❑ **Watch your permissions**

  On iOS and Android, apps need to ask before accessing things like your files, camera, microphone, location, etc. Make sure you're only granting permissions the app actually needs, and deny anything it doesn't or you're unsure about. On iOS you can check your permissions in the Settings app within the Privacy menu. On Android you can go to the "Apps" menu in the Settings app and click on an app to see its permissions.

- ❑ **Don't root your phone**

  Rooting or jailbreaking your Android phone or iPhone respectively is a massive security risk. If you don't know what this means you most likely don't need to worry about it.

Computer Security

- ❑ **Enable full disk encryption**

  This will protect your data in the event your computer is stolen, especially if you use a laptop!
  On macOS this is called FileVault and can be enabled in System Preferences > Security & Privacy > FileVault. On Windows 10 Pro/Enterprise this is called BitLocker and can be enabled by typing "Manage BitLocker" in the start menu search and opening it, then selecting Turn on Bitlocker. On Windows 10 Home this is called Device Encryption and can be found at Start > Settings > Update & Security > Device Encryption.

- ❑ **Back up your data**

  Protect your data from being lost via theft or ransomware by making frequent backups. On macOS you can use Time Machine, on Windows you can use File History. Either option can be used with an external drive or a network drive.

- ❑ **Stay up to date**

  Make sure you are using the latest version of your operating system at all times. Windows 10 now updates automatically, but you can manually check for updates at Start > Settings > Updates & Security. You can enable automatic macOS updates in System Preferences > Software Update > "Automatically keep my Mac up to date". Do not use Windows 7 or XP, or any macOS version prior to the latest release (Mojave as of July 2019, Catalina is upcoming Fall 2019).

- ❑ **Install Antivirus**

  Windows or Mac, they both get viruses. Windows comes with Defender already, but you should enable "MAPS" for additional protection: Search for "Windows Defender" in Start, click "Settings", and switch Cloud-based Protection to On. For macOS, Avast is a good free choice (download:

https://jda.mn/macavast), but uncheck the SecureLine VPN and Password Manager during the install. For Windows and Mac, MalwareBytes (https://www.malwarebytes.com/) is an exceptional antimalware and antivirus that replaces Defender or Avast, but costs $40+/year.

- ❑ **Adobe and Java Software**

  Java is not needed for any modern application and should be uninstalled. Flash is only necessary if you insist on using Firefox *and* still go to websites that require Flash, otherwise it should be uninstalled. Chrome, macOS Preview.app, and Microsoft Edge all read PDF files, so unless you need to edit PDF files often, there's no reason to install a dedicated PDF reader. If you do, install Adobe Reader DC, because it updates automatically and is an official Adobe app.

- ❑ **Windows: Set UAC to full**

  User Account Control is an important security feature in Windows, and setting it to anything less than "Always Notify Me" (including the default setting) allows malware to gain admin rights instantly. Follow the instructions at https://jda.mn/uac to change your UAC settings.

- ❑ **Enable your firewall**

  Making sure your computer's firewall is active will help prevent many network based attacks like ransomware, or your data being stolen from someone on your network. On macOS this can be enabled in System Preferences > Security & Privacy > Firewall. On Windows this should be enabled by default but you can check in Settings > Update & Security > Windows Security > Firewall & network protection.

- ❑ **Uninstall any applications you don't recognize**

  Regularly remove anything you don't recognize or no longer use. On macOS you can view your applications in the Applications folder in Finder (Go > Applications) and drag anything you don't need to the trash. On Windows you can go to Start > Settings > System > Apps & Features to uninstall apps.

Browser Security

- ❑ **Install uBlock Origin**

  The greatest malware threat for Windows and Mac users come from malicious advertisements on mainstream websites either leading to malware downloads or pop-ups with fake "tech support" numbers. uBlock Origin (https://github.com/gorhill/uBlock) is the fastest and most reputable adblocking software available.

- ❑ **Use Chrome or Firefox**

  As of 2019 Firefox has finally caught up to Chrome in terms of security. Use whichever you wish,

although stick with Chrome if you've joined Google Advanced Protection. Microsoft Edge is too new to recommend at this time. Safari is acceptable if you only use macOS.

- ❑ **Uninstall any unknown or unrecognized extensions**

  Always remove any extensions you don't need or recognize. You need nearly no extensions for a normal browsing experience, so when in doubt delete everything besides uBlock Origin. In Chrome you can view and remove extensions in the Menu > More Tools > Extensions. In Safari you can go to Preferences > Extensions. In Firefox you can click the Menu icon > Add-ons > Extensions or Themes.

Network Security

Home users should read this guide entirely to secure their router: https://decentsecurity.com/#/routerwifi-configuration/

Physical Security

- ❑ **Cover your webcam**

  It's unlikely your webcam will be hacked, but it's very cheap to take this step. Better to be safe than sorry! Cover your webcam with painters/electric tape whenever you don't use it.

- ❑ **Use a privacy shield**

  Cover your screen with a privacy shield to prevent people from snooping on what you're doing, especially if you often work in a public place.

- ❑ **Use a hardware security key**

  Using a physical key – like one made by Yubico or Feitian – to login to your accounts will keep your accounts incredibly secure. Google supports them (via the Google Advanced Protection program mentioned above), as well as Facebook, Twitter, GitHub, AWS, and many more providers. You can check compatibility at https://www.dongleauth.info/

Miscellaneous

- ❑ **Do *not* use a VPN**

  Commercial VPN providers offer very little – if any – protection, and can actually harm your security. Only use a VPN if a) you run the servers yourself, b) your employer provides their own VPN.