# Instructions

This guide aggregates suggestions across several organizations and best practice security measures in an easy-to-consume way.

The person in charge of security (IT/security person, campaign manager, etc.) should create a copy of this guide, customize it with the appropriate apps for their organization, and share it with the team. Each team member should make their own and fill out the checklist, and send back to the person in charge for verification.

-------------------------

# Security Checklist

Welcome to the team! We take security **very** seriously, as data privacy and security are a core part of our operations & mission.

Please complete the below checklist to make sure your devices & accounts are secure. To complete this form, copy this page, and write **“Yes”** in each box as you complete them. Then return them to your [IT department | campaign manager] when complete.

## Securing Your Devices

| **Laptop Instructions** | **Work Comp** | **Personal Comp** |
| --- | --- | --- |
| I have applied all ​operating system​ update(s) to my [Mac​](https://support.apple.com/en-us/HT201541), [​PC​](https://support.microsoft.com/en-us/help/311047/how-to-keep-your-windows-computer-up-to-date), or [​Chromebook​](https://support.google.com/chromebook/answer/177889?hl=en), and enabled automatic updates where possible |  |  |
| I have applied all ​application​ updates to my [​Mac​](https://support.apple.com/en-us/HT201541) or [​PC](https://support.microsoft.com/en-us/help/311047/how-to-keep-your-windows-computer-up-to-date), and enabled automatic updates where possible |  |  |
| I have encrypted my laptop drive ([​Macs​](https://support.apple.com/en-us/HT204837), [​PCs​](https://www.windowscentral.com/how-use-bitlocker-encryption-windows-10)) |  |  |
| The passphrase on my [Mac](https://support.apple.com/en-us/HT202860), [PC](https://support.microsoft.com/en-us/help/4490115/windows-change-or-reset-your-password), or [Chromebook](https://www.howtogeek.com/396611/how-to-change-your-password-on-a-chromebook/)  is at least 12 characters long |  |  |
| I have installed the ​HTTPS Everywhere​ browser ([Chrome](https://chrome.google.com/webstore/detail/gcbommkclmclpchllfjekcdonpmejbdp)/[Firefox](https://www.eff.org/files/https-everywhere-latest.xpi)) extension, and enabled **“**Encrypt All Sites Eligible**”**   * If a site doesn’t work, you can manually disable E.A.S.E. |  |  |
| I have installed the uBlock origin browser ([Chrome](https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=en-GB)/[Firefox](https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/)) extension |  |  |
| I have installed [ name of Password Manager ]   * This is often a multistep process, ie: making an online account with the password manager, downloading the password manager, and adding it as an extension to your web browser. |  |  |
| [ Add additional to-do items as desired ] |  |  |

| **Phone / Tablet Instructions** | **Work Phone (if applicable)** | **Personal Phone** |
| --- | --- | --- |
| I have applied all ​operating system​ update(s) to my [​iPhone/iPad](https://support.apple.com/en-us/ht204204)​ or to my ​[Android phone](https://www.wikihow.tech/Check-for-Updates-on-Your-Android-Phone), and enabled automatic updates where possible |  |  |
| I have updated all ​application​ updates ([​iPhone​](http://osxdaily.com/2018/05/22/how-update-all-apps-iphone-ipad/), [Android​](https://support.google.com/googleplay/answer/113412?hl=en)), and enabled automatic updates where possible |  |  |
| I have downloaded all the relevant apps (see below) |  |  |
| I have set a passcode for my mobile provider   * + [AT&T](https://www.att.com/olam/passthroughAction.myworld?actionType=ViewProfile)   + [T-Mobile](https://www.t-mobile.com/customers/secure)   + [Verizon](https://www.verizonwireless.com/support/account-pin-faqs/) |  |  |

### Download Phone Apps

& begin integrating these apps in to your routine

| **App** | **Purpose** | **Apple** | **Android** | **Completed?** |
| --- | --- | --- | --- | --- |
| Gmail | Secure Gmail access | [Link](https://apps.apple.com/us/app/gmail-email-by-google/id422689480) | N/A |  |
| Google Drive | Secure File share | [Link](https://apps.apple.com/us/app/google-drive/id507874739) | N/A |  |
| Google Calendar | Secure calendar | [Link](https://itunes.apple.com/us/app/google-calendar-time-planner/id909319292?mt=8) | N/A |  |
| Google Docs | Secure GDocs access | [Link](https://apps.apple.com/us/app/google-docs-sync-edit-share/id842842640) | N/A |  |
| Google Sheets | Secure GSheets access | [Link](https://apps.apple.com/us/app/google-sheets/id842849113) | N/A |  |
| Google Meet | Secure audio/video conferencing | [Link](https://itunes.apple.com/us/app/hangouts-meet/id1013231476?mt=8) | [Link](https://play.google.com/store/apps/details?id=com.google.android.apps.meetings) |  |
| Signal   * **NOTE**: there is no need to let Signal be your default SMS app! | Secure messaging | [Link](https://itunes.apple.com/us/app/signal-private-messenger/id874139669?mt=8) | [Link](https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms) |  |
| Authy | Two-factor authentication | [Link](https://itunes.apple.com/us/app/authy/id494168017?mt=8) | [Link](https://itunes.apple.com/us/app/authy/id494168017?mt=8) |  |

The most secure applications for email, calendar, and web browsing are made by Google – they provide the best security features, and offer more timely security fixes, than native Apple apps (e.g. Apple Mail, Calendar, Safari, etc.). You should use these apps to securely work with G Suite.

## Secure Your Accounts

| **Task** | **Completed?** |
| --- | --- |
| Take the Google phishing quiz to learn more about phishing emails [here](https://phishingquiz.withgoogle.com/). |  |
| The master password for [preferred password manager] is longer than 16 characters and is unique. |  |
| I have enabled two-factor authentication (2FA) for my password manager |  |
| I have enabled 2FA on the following sites and on any other websites or apps that I use regularly. Look [here](https://2fa.directory) for instructions for the most common sites.   * Gmail (work & personal) * Apple ID * Twitter (work & personal) * Facebook (work & personal) * LinkedIn * [Add more as desired] |  |

## Google Accounts

| **Task** | **Completed?** |
| --- | --- |
| Run a Security Checkup |  |
| * Under “Your Devices”, make sure only devices you use on a regular basis are present. Remove any others. |  |
| * Under “Recent Security Events”, make sure it says “No events in 28 days” (or that you recognize all the events that are there). If it does not, please report that fact to your IT team |  |
| * Under “2-Step Verification” remove any devices you do not use anymore |  |
| * Under “Third-party apps with account access” (if present) remove access from any apps you do not use anymore or do not recognize * (May also be under “Signing in with Google” or “Linked Accounts”) |  |
| Enroll in Google’s Enhanced Security [here](http://goo.gle/enhanced-security)  * This program, exclusive for U.S. campaigns, provides extra monitoring of large attachments and geographically diverse log-ins of accounts. Your administrator may set this up for you - if not, you can submit yourself. |  |
| Enroll in Google’s Advanced Protection Program [here](https://landing.google.com/advancedprotection/) |  |

**Note for Google’s Advanced Protection Program: This step requires additional setup and may require technical assistance, but is important for high-security environments like high-stakes campaigns.**

If you have a personal Gmail account, please enroll in Google’s ​Advanced Protection program​. It uses a physical key to log you into your Gmail account, and dramatically reduces the risk of getting phished.

The risk of phishing is high. Enroll yourself, key staff, and your family members in the [Advanced Protection Program](https://landing.google.com/advancedprotection/).

Here is ​[a video to provide more information](https://youtu.be/pONS04Rjydg)​.