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, PC, or Chromebook, and enabled automatic updates where possible		
I have applied all application updates to my Mac or PC, and enabled automatic updates where possible		
I have encrypted my laptop drive (Macs, PCs)		
The passphrase on my Mac, PC, or Chromebook is at least 12 characters long		
I have installed the HTTPS Everywhere browser (Chrome/Firefox) extension, and enabled "Encrypt All Sites Eligible" - If a site doesn't work, you can manually disable E.A.S.E.		

Created by: Daniel Bardenstein
Updated: 5/4/2021

I have installed the uBlock origin browser (Chrome/Firefox) 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 or to my Android phone, and enabled automatic updates where possible		
I have updated all application updates (iPhone, Android), 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 ○ T-Mobile ○ Verizon		

Download Phone Apps

& begin integrating these apps in to your routine

App	Purpose	Apple	Android	Completed?
Gmail	Secure Gmail access	Link	N/A	
Google Drive	Secure File share	Link	N/A	
Google Calendar	Secure calendar	Link	N/A	
Google Docs	Secure GDocs access	Link	N/A	
Google Sheets	Secure GSheets access	Link	N/A	

Created by: Daniel Bardenstein
Updated: 5/4/2021

Google Meet	Secure audio/video conferencing	Link	Link	
Signal - **NOTE**: there is no need to let Signal be your default SMS app!	Secure messaging	Link	Link	
Authy	Two-factor authentication	Link	Link	

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.	
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 for instructions for the most common sites. ● Gmail (work & personal) ● Apple ID ● Twitter (work & personal) ● Facebook (work & personal) ● LinkedIn ● [Add more as desired]	

Created by: Daniel Bardenstein
Updated: 5/4/2021

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 - 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	

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.

Here is a video to provide more information.

Created by: Daniel Bardenstein
Updated: 5/4/2021