Device and Account Security Checklist

Checklist Instructions

Use this checklist to make sure you have covered all the device and account security basics. Print out the document and check off the boxes like this: ☑

Secure your devices

Keeping your laptops, phones, and tablets, as well as the applications on them, updated is one of the most important ways to keep them (and your data) secure. For example, most operating system updates contain numerous security updates. Adversaries frequently take advantage of devices that have not been updated recently. Always apply your updates as soon as they come out!

Laptop disk encryption

Encrypting your laptop can keep your data safe even when it is lost or stolen. Disk encryption is easy to enable and does not take much time. Here are the instructions: for Macs and for PCs.

Web encryption

Some websites do not properly enable encryption for all connections. Luckily, there is something you can do to make sure your internet connections are secure. In your web browser, you should install the HTTPS Everywhere extension. HTTPS Everywhere is a Firefox, Chrome, and Opera extension that strengthens the encryption between your device and major websites.

Secure your mobile phones and tablets

Some phone carriers allow you to set a login PIN. If your carrier supports this feature, you should enable the feature because having a pin makes it harder for attackers to take over your account. Even if they guess your name and password, they will still need to obtain the PIN to access your account.

Secure your accounts

Passwords

For every one of your online accounts, you should use a password that is **long**, **random**, and **unique**. Here is our current thinking:

- **Long**: at least 16 characters
- **Random**: generated by a computer, not you. Humans are not wired to generate random numbers or passwords.
- **Unique**: never used twice. Attackers take advantage of password reuse, so don't do it.

Most people have dozens of online accounts. Unless you have a photographic memory, organizing passwords with the above requirements is a tall order. The solution is to use a password manager.

Password managers

Password managers such as LastPass and 1Password help you create, store, and enter login credentials for you. They will create passwords that are long, random, and unique. They will store them, in encrypted form, in a database. When logging in to a website, they can enter your user name and password in the correct field so you don't need to type them.

Although you can use one password manager account to manage both your personal and work accounts, we do not recommend it. We recommend you separate your personal and work accounts and data, and that also includes where you store passwords. Having separate personal and work password managers (with separate master passwords, of course) sounds like a lot of work, but with just a little practice it's almost transparent.

The password manager will store all of your website passwords. To protect all of those individual website passwords, you need to supply a "master password". The password manager will use that master password to encrypt/decrypt all of your individual website passwords.

Caution: 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 type it every day.

To create a strong master password use a password generator such as this passphrase generator. A good passphrase might look something like this: sixth golf glean pact hassock

Two-factor authentication

Two-factor authentication (sometimes called 2FA, "two step", "multi-factor", or MFA) adds an additional and critical step to a website's login process. Two-factor systems use your smartphone or a hardware device to identify you to the website. Visit twofactorauth.org for instructions to popular sites.

Caution: Many websites offer SMS-based (text message) two-factor access. Unfortunately, it is possible to steal someone's phone number (called "SIM-swap attacks"), and then to intercept two-factor codes sent via SMS. *Avoid two-factor authentication based on SMS*.

Confirm that you have 2FA set up for these sites. Note that you may have more than one account on these services. Protect them all.

Gmail users

Enroll in Google's Advanced Protection Program (APP)

If you are working in a political party or on a campaign, and you have a personal or work 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. Consider it **mandatory**.

Here is a video to provide more information.

Google account security

If you use Gmail, you should get a security checkup. Go to https://myaccount.google.com/security-checkup. Click on each of the four rows, starting with "Your Devices." A few points:

1. Under "Your Devices", make sure only devices you use on a regular basis are present. Remove any others.
2. Under "Recent Security Events", make sure it says "No events in 28 days". If it does not, please report that fact to your IT team.
3. Under "2-Step Verification" remove any devices you do not use anymore.
4. Under "Third-party access" (if present) remove access from any apps you do not use anymore or do not recognize.

Beyond the Checklist

Mail servers

For your organization's mail system, only use mail services hosted by Microsoft or Google (Outlook/Outlook 365 or Gmail/G Suite). *Do not use other mail services and do not host your own mail server under any circumstances*. Even an Exchange server hosted by a reputable company will not be sufficient.

While there are other services that might be attractive, none of them match the security programs and teams at Microsoft and Google. Do not take risks with your mail provider.

Facebook privacy

Facebook has a number of privacy settings. You can review them here. Consumer Reports has also produced a guide to help you tune the settings. When using a campaign page, or a public person page, be sure that anyone who has access to edit those pages has completed this checklist.

Use a Chromebook or iPad

A key technique to reducing the risk of a breach is to reduce your attack surface. To that end, consider migrating to a Chromebook or an iPad. Both devices offer a number of key security features, and dramatically limit the options our adversaries have for running malware.

Secure chat

While text messages are very convenient and work on any phone, they are not secure. We recommend you standardize on either Signal or Wickr Pro for your text messaging.

Security questions

A few websites still rely on using account security questions ("ASQ") to help identify you in the event that you forget your password to the site. They often ask for information like "Where did you travel on your honeymoon?" While that might seem like a harmless question, in a world of social media, many of these answers can be found on the internet or the dark web. In 2008, this is how an attacker broke into the mail account of Sarah Palin.

To that end, if you encounter a website that requires account security questions, you should use random words to answer those questions. Then store the random answers in your password manager. Be sure to use a passphrase generator like this one. For example, the answer to "What was the name of your high school?" might be "mystique parterre virelay".

For more information

The information above is general guidance that will dramatically reduce the risk of attackers compromising your devices and accounts. But, given the daily news about security problems, it will come as no surprise that these practices will not be sufficient in all cases.

To that end, please contact the DNC's security team with any questions or suggestions you have. We look forward to helping you stay secure!

The checklist

Securing your devices

Task	Personal Devices	Work Devices
Laptop: I have applied all *operating system* updates to my Mac, PC, or Chromebook**,** or enabled auto-updates where possible	❑	❑
Laptop: I have applied all *application* updates to my Mac or PC	❑	❑
Laptop: My laptop drive is encrypted (Macs, PCs)	❑	❑
Laptop: The passphrase on my laptop is at least 12 characters long	❑	❑
Laptop: I have installed the HTTPS Everywhere extension	❑	❑
Phone/tablet: I have applied all *operating system* updates to my iPhone/iPad or to my Android phone	❑	❑
Phone/tablet: I have updated all *application* updates (iPhone, Android)	❑	❑
Phone: I have set a passcode for my mobile provider (AT&T, T-Mobile, Verizon)	❑	❑
Phone/tablet: I set an unlock code that is at least 6 characters long	❑	❑

Securing your accounts

Task	Personal Accounts	Work Accounts
I use a password manager to store all my passwords	❑	❑
The master password for my password manager is longer than 16 characters, and is unique	❑	❑
I have enabled 2FA (see below) for my password manager	❑	❑

Two-factor authentication (2FA)

I have enabled 2FA on all of the following accounts. Note that you may have more than one account on these services. Protect them all.

Task	Personal Accounts	Work Accounts
Gmail	❑	❑
AppleID	❑	❑
Outlook.com	❑	❑
Yahoo	❑	❑
AOL	❑	❑
Twitter	❑	❑
Facebook	❑	❑
Instagram	❑	❑
LinkedIn	❑	❑
Dropbox	❑	❑
Evernote	❑	❑
Snapchat	❑	❑

Don’t forget to review accounts for gaming services (Nintendo, Twitch, Steam, XBox), online stores (Amazon, Groupon, EBay, Etsy), and financial services (Paypal, bitcoin, Venmo, Square, CashApp, bank accounts, 401k, investments).

For people who use Gmail for personal or work mail:

Task	Personal Accounts
I have enrolled my personal account in the Advanced Protection Program	❑
I have reviewed my account security at https://myaccount.google.com/security-checkup	❑