Device and Account Security Checklist

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 are released.

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.

Laptop 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 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
- Randomly generated. Technology has reached the point where if you can remember your password is it not effective.
- Unique: never used twice. Attackers take advantage of password reuse, so do not reuse them.

Most people have dozens of online accounts. Without a photographic memory, organizing passwords with the above requirements is difficult at best. The solution is to use a password manager.

Password Managers

Password managers such as Bitwarden and KeePassXC help you to 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. We do not recommend using one password manager account to manage both your personal and work accounts. You should have one for personal and one for work accounts. 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 "main password". The password manager will use that 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.

Mulit-factor Authentication (MFA)

Mulit-factor Authentication adds a critical step to a website's login process. MFA systems use your smartphone or a hardware device to identify you to the website. Visit https://authy.com/ 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-swapping"), and then to intercept two-factor codes sent via SMS. Avoid multi-factor authentication based on SMS.

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

Beyond the Checklist

Secure Messaging

While text messages are very convenient and work on any phone, they are not secure. We recommend you standardize on either Signal or Wire 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?" This may seem like a innocent question, in a world of social media, many of these answers can be found on the internet or the dark web.

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 "unwed sublease underfoot tractor."