Electronic device security best practices

Public Lab privacy and security guidelines, https://publiclab.org/security - v1.0 Jan 8 2019

What's at risk?

Security and privacy is a broad topic, and the best way to begin is to identify what you're trying to protect. Consider:

- **What are you protecting?** Names and addresses? Photos, health data, passwords, or secrets?
- **Whose information is it?** Yours? Community members? International activists? Customers?
- **Who should it be kept from?** "Hackers"? Governments? What resources do they have to find it out?
- **Where do you store or transmit information?** Using your phone or laptop? By email, text message, or phone call? On Dropbox or Slack?
- **Who are you trusting when you store or transmit information?** Your colleagues? An online service? Your office neighbors? People who share your printer?

Basics

There are a few simple things you can do to dramatically increase your security and prevent breaches:

Build habits gradually

Don't change everything at once! You'll disrupt your work and get frustrated. Instead, change your habits gradually, building on good practices without upsetting your workflow. Try keeping a checklist of what you aspire to change, and track your progress over time.

Running updates

Most security issues aren't up to you, they're the responsibility of the companies who make and maintain your computer and phone operating systems. **The most important thing you can do to remain secure is to keep your computer, phone, web browser, and other apps up to date.**

Sometimes you may be running out of space, or have no time, and are reluctant to upgrade. Schedule time — regularly if need be — to offload files and make sure to install any new updates as soon as they're available.

Lock your screens

If your accounts or devices are compromised, it can have a ripple effect: once someone gets into your Gmail account, they can often reset passwords for other accounts, sowing chaos throughout your digital life.

This often happens when you lose a device, and the most important thing you can do to protect yourself is to **set a lock screen on your phone and computer**. This way, if you lose your computer or phone, all your accounts are relatively safe and there is no 'ripple effect.'

Two factor authentication

Many services (Gmail, Slack, Dropbox) now offer this service (also known as 2-factor verification), which sends a verification code to your phone when you log in, to ensure that both your phone and your password are needed to get into your account. This vastly reduces the chance of your account being hacked.

Disk encryption

If your computer or phone is lost or stolen, it's not hard to access its contents even without a password, unless you've enabled disk encryption. The following pages cover encryption on various devices, although newer Android and iOS devices are encrypted by default:

- Mac OS X: https://en.wikipedia.org/wiki/FileVault
- Android: http://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/ (slightly different for more recent versions)
- iOS: https://support.apple.com/en-us/HT202064
- Linux (Ubuntu): http://www.howtogeek.com/116032/how-to-encrypt-your-home-folder-after-installing-ubuntu/

Jump drives, flash drives, pin drives, USB drives, SD cards: These are risky to share; they can carry viruses.

Everyday habits

Security is easier when you can build good everyday habits around it, that don't stress you out (so you try not to think about it), and that don't block you from doing your work.

Good passwords

Creating good passwords can be tough -- folks often use easy-to-remember ones which are then easy-to-break, or they use the same ones everywhere. Both of these are best avoided; here are some helpful tips:

Passphrases: A growing practice is to use "passphrases" -- words strung together like this: "**astheappleturnsaround**" which is a nice long password which is an easy phrase to remember and type, and is MUCH more secure. Read about one method for creating passphrases at https://eff.org/dice

Special characters: However, some systems require special characters, so you can **Sw4p ch4racter5!k3 th!s, t00!**

Random passwords: Some programs, like KeyPassX, will generate really random passwords, that look like this: **`c&3j2##rBw`** -- these are OK, but they usually require a password storage solution and cannot be easily memorized. Read on!

Good passwords are unique. It does not matter how strong a password is if it used multiple places, and one of them is compromised. Having multiple passwords may quickly require you to start using a password manager, as detailed below.

Good password storage

If you have lots of passwords, you can store them in a file which is ITSELF encrypted with a very secure password. KeePass/KeePassX are good apps for this (and are EU-FOSSA audited). Also consider LastPass, a commercial solution which offers easier user interface, including a a mobile app.

Storing passwords on paper in a locked drawer is also an option, but if you save in a digital file, you can store that file online, for example in Dropbox, and you don't have to carry paper with you, which would be unsafe.

Secure storage & channels

Email is unencrypted -- it's the digital equivalent of sending private information around in an open envelope, as anyone can read it if they want to. This means: **don't send passwords, or private information like social security or credit card numbers, in emails**. Read on!

So how DO you send private or confidential things digitally? There are a few options.

Signal: This is a well-trusted, open source project with iOS and Android apps, where you can send secure encrypted messages between two people who both have the app. Look for a little "lock" icon when texting someone (send a test message first!), and you should be safe to send passwords over this channel. Be sure to delete messages containing private information from both parties' phones when you're done.

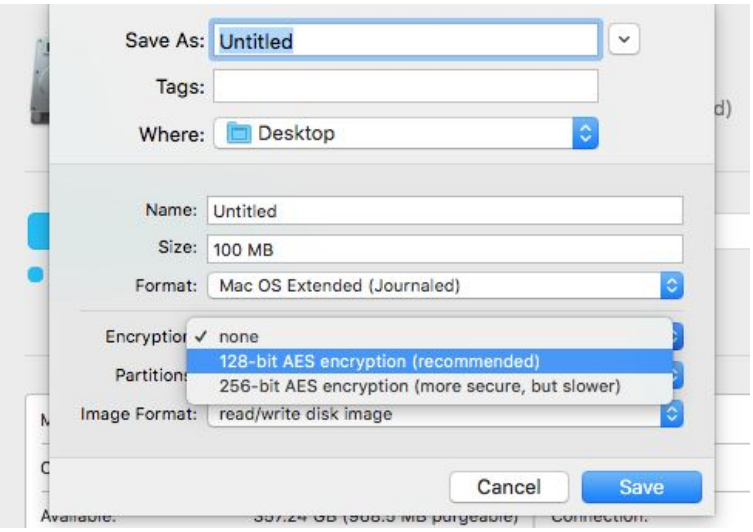
WhatsApp: This app is more popular than Signal but uses the same core technology (actually provided by Signal). It's not quite as secure, but pretty good. (Paul Manafort's private messages were extracted by the FBI when his WhatsApp account was backed up onto Apple iCloud. Whoops!)

Voice calls: Calling someone and reading passwords over the phone is not ideal, because you could be overheard at either end, but are an OK fallback if you have no other options.

Secure Chat, such as https://crypto.cat/ can provide a temporary encrypted channel for communication

Secure file storage/Sending files

You can encrypt a file with a password and send it by email or Dropbox, then send the password to someone through a separate channel, such as phone or SMS text.



Apple's **Disk Utility** can be used to create a password-protected virtual disk to keep sensitive files in; it can be emailed or passed around and only opened when actively using the data inside. To create a new secure file, click **File > New image** and choose an encryption type (see screenshot). **7zip** is a program for Linux and Windows with similar capabilities: http://7-zip.org/

Temporary passwords: One good way to add some security is to send a password in as secure a means as possible, but be sure the end user changes their password immediately upon receiving it. Then, even if it's been intercepted, there's only a small time window for a potential attack.

While traveling

When you're traveling, your devices and information are at greater risk. You might leave them in unexpected places, or need to use unfamiliar WiFi networks, or need to let other people access them, whether voluntarily or not (like at the border).

The best strategy is to 1) travel light; 2) travel with less data; 3) travel encrypted (see above)

Traveling light: Use a second, minimally set-up phone just for travel to places where your device may be subject to search or theft. You can also set up a second user account on Android phones, and have a more innocuous set of apps and data than your main account for when you pass through borders. Set up per-app locking on some apps - such as Signal and Authy - so even if border guards ask for your password, they'll need another one to get into those apps. Consider using an international wifi hotspot instead of a local SIM card; in China, some hotspots can route around the Great Firewall. Avoid public USB charging ports as they may be able to connect to your device without permission; charge a battery on them instead of your phone.

Consider using a second, minimally set-up computer just for travel to places where your device may be subject to search or theft. For instance, a $100 Chromebook that is not synced with cloud-based storage. Upon return, factory reset these devices.

Traveling with less data: Strongly consider un-syncing to cloud storage like Dropbox or Google Drive Offline before you cross borders.

Reducing exposure

Changing our habits can reduce the amount of data that we leak and that can be harvested as we move around the internet.

Review browser extensions/plugins: Browser extensions have access to your online activity, and can perform activities on your computer. Since they update automatically, extensions can be made malicious long after you originally authorized their access. Review and remove frequently.

Use a VPN: VPNs hide your browsing activity from your local network and Internet Service Provider (ISP). A VPN is useful for protecting your privacy on a public wifi network such as a coffee shop, or to disguise your location so that you can access content and parts of the internet that are not available in your current geographic region due to country-level censorship or copyright issues. A VPN relays your internet connection through one in another place. At time of writing, ExpressVPN is popular; also see Shadowsocks, https://shadowsocks.org/.

Use the Tor Browser: Tor relays your internet traffic through a series of other computers, obscuring your activity on the internet: https://torproject.org/. Orbot is the official version of Tor for Android phones: https://guardianproject.info/apps/orbot/. Onion Browser is the equivalent for iOS: https://onionbrowser.com/. Tor can replace VPNs and provide even more privacy. In some cases, Tor may allow you access outside the Great Firewall. Use the Tor browser instead of a normal browser, especially on cheap phones that can be loaded with spyware and malware.

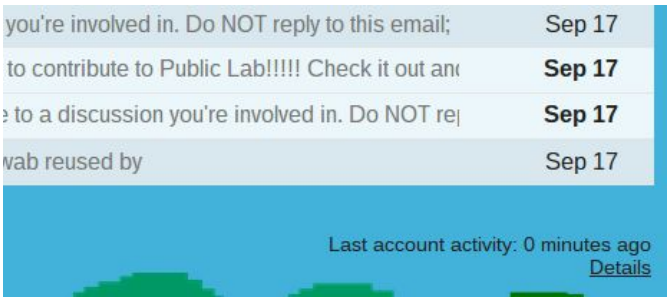
What to do when things go wrong

Losing your device

There are various ways to remotely lock some devices. Please try to do this, and email web@publiclab.org and alert fellow staff as quickly as possible, borrowing a phone if necessary. If we lock/disable devices and accounts as soon as possible, we may be able to prevent a broader privacy/security breach.

Remote log-out

Gmail and other services allow remote log-out, and let you see who's currently logged in. You can check for it to the lower right corner of your inbox, as shown here:



Change passwords

If you're worried someone may have gotten access to your Gmail account or another account, change your password(s) for these accounts, and for any accounts where you've used the same password.

Resources

http://www.teenvogue.com/story/how-to-keep-messages-secure (practical)
https://thenextweb.com/apps/2013/10/06/10-of-the-best-multi-platform-password-managers-for-ios-android-and-the-desktop/
https://1password.com/

https://securityinabox.org/en/ (thorough and clearly organized, via Tactical Tech Collective)

https://www.cryptoparty.in/learn/how-tos
https://www.cryptoparty.in/learn/handbook
https://www.cryptoparty.in/learn/tools
https://uit.stanford.edu/security/travel/high-risk-countries-recommendations