Security Recommendations

The security of a research group depends on the entire team implementing and maintaining a strong security policy with the intent to keep themselves and each other safe. We can never be 100% secure but we can implement a number of measures that will make it much harder for those with malicious intentions. This guide tries to find a balance between recommending software and tools that are secure, while still remaining relatively easy to use. You may refer to the end of the guide for more references and further reading.

Security measures need to be reviewed regularly to make sure that the team is up-to-date on recent attacks and methods that may be used, as well as to make sure that the entire team is on the same page. Security measures should be reviewed once a year, at the very least.

Contents:

Basic Security Measures

1) **Use strong passwords and do not re-use them.** A password should not be a word in any language, personal information, name of someone you know or a predictable string of words (such as "letmeinnow"). As well, a password should be longer than 10 characters and a mix of uppercase and lowercase characters, symbols and numbers. **Towards these ends, all members of the research team should use a password manager**, which stores all of your passwords in a single encrypted file so that you don't have to remember them. A password manager also allows you to easily create strong and unique passwords for accounts and services. KeePassXC (keepassxc.org) is recommended for a number of reasons. Firstly, the password database is not stored on cloud servers unless you put it there, which means there are fewer security vulnerabilities. Secondly, it is currently being worked on and updated. You can install and set-up KeePassXC using the instructions here: ssd.eff.org/en/module/how-use-keepassxc.

- Note that if you are using a password manager, the guidelines for creating a secure password to the rest of your passwords is more stringent. You should use a Diceware passphrase, not a password, even a strong one. You can create a Diceware passphrase using the instructions in the video posted here: ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice or the instructions written here: theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/ If you are worried about forgetting your master passphrase, you can write down your passphrase on a piece of paper and carry it with you for reference until you memorize it. Diceware passphrases do not need to be created whenever a password is required for an online service as it takes some time and may not fulfill the password requirements for the service (for example, some sites restrict the length of your password, which is a problem when using Diceware passphrases).
- If you do not wish to use a password manager, another relatively a secure method of remembering many unique passwords is to write them down on a physical piece of paper. Assuming you keep this paper secure, (and not stored on or near your computer) this is safer than reusing passwords or using insecure ones. Tips on quickly creating strong passwords can be found here: securityinabox.org/en/guide/passwords
- There are similar suggestions for security questions: do not reuse them and do not use an answer that can be easily guessed or obtained. For better security create an answer that is a non-sequitur, a code or an answer to a similar sounding but unrelated question. You can also create a password to use as an answer to a security question.
- For all of your accounts, turn on two-factor authentication, if the service provides it. A list of services that allow for two-factor authentication can be found here: twofactorauth.org. The most secure option for receiving codes is through a code generator rather than receiving codes via e-mail or text. A how-to for implementing two-factor authentication for a number of services is here: eff.org/deeplinks/2016/12/12-days-2fa-how-enable-two-factor-authentication-your-online-accounts
- Do not use application specific passwords. An explanation of why they are risky to use is here: howtogeek.com/199804/warning-your-"application-specific-passwords"-aren't-application-specific

2) Back up important files, like a copy of your password manager file, to an external hard drive or flash drive. Store the backup somewhere secure and in a different location from the original set of files, in case of a fire or theft. The external storage device should only be connected to a computer when the backing up of files is in progress to avert the corruption of the backup in case your computer gets infected. You can read more about creating a backup strategy for yourself here: securityinabox.org/en/guide/backup

3) Keep all of your software up-to-date and make sure your firewall is enabled. While your firewall should be on by default, instructions for how to check the status of your firewall are here: lifehacker.com/5805326/how-to-turn-your-computers-firewall-on-and-off
4) Try to keep informed of recent security breaches that may affect services that you use and change your passwords accordingly. You should check regularly if any services that you use have been breached by using haveibeenpwned.com By entering an e-mail address that you have used to sign up for other services, this website checks if that e-mail appears in any data leaks and informs you of what was included in the leak. Alternately, you can check the list of services which have been breached here: haveibeenpwned.com/PwnedWebsites
5) 3rd-party applications often request access to your personal information, without having strong security measures for storing it. Revoke 3rd-party app permissions as described here: yoursosteam.wordpress.com/2015/09/04/tip-8-review-third-party-permissions-on-twitter-and-facebook/ As well, don't log into 3rd-party sites using your Gmail, Facebook or Twitter account. This is insecure as the 3rd-party site may be malicious or simply have poor security measures. Either way, it is then easier for others to learn your password.
6) Regularly review the privacy and security settings of the online services and social media sites that you use as they often change.
7) Delete old accounts that you don't use anymore. Instructions on how to do this for many sites can be found here: accountkiller.com and direct links to deletion pages for each site can be found here: backgroundchecks.org/justdeleteme/
8) When travelling across borders, you are advised to carry the minimum amount of data necessary, due to the broad legal authority that is afforded to border agents, particularly in the United States of America. A summary of what aspects you should consider when travelling is here: ssd.eff.org/en/module/things-consider-when-crossing-us-border A very in-depth examination of things you should consider can be found here: eff.org/wp/digital-privacy-us-border-2017

Use End-to-End Encryption for Communications

Try to avoid transmitting sensitive information online or on a cell phone as these can be insecure. Most e-mail, chat, text messaging, file sharing, phone and video conferencing services are never truly "off-the-record" without extra steps taken. Also be aware that you are trusting whoever you are giving this sensitive information to and their security measures (or lack thereof).

As such, communications between members of the research group should be encrypted in order to prevent eavesdropping. However, end-to-end encryption usually requires more work to implement than a few simple steps. Each communication method that the team uses should be encrypted, and there are a large number of services providing some level of encryption for online communication. As

such, there are a number of options to examine, depending on the needs of the group and the ease of use desired by the group. Secure recommendations for e-mail, chat, file sharing and video conferencing software can be found at privacytools.io under the respective headings.

Encrypt Your Computer

Encrypting your computer is necessary to prevent an unauthorized person who may have physical access to your computer from accessing your files. Putting a password on your computer is NOT encryption, nor is it a particularly strong security measure. If someone has physical access to your device, there are several ways that they can get around a password. **Thus, it is recommended that the research team encrypts the hard drives that sensitive information is stored on.** Why encryption is important, what it does and its weaknesses are explained here: theintercept.com/2015/04/27/encrypting-laptop-like-mean/ This article recommends and provides tutorials for using the built-in encryption software on various platforms, however VeraCrypt is the recommended software in this document for a variety of reasons. Since VeraCrypt is cross-platform (which means that you can transfer VeraCrypt encrypted files between Windows and Macintosh computers) and independently verified to be secure (unlike proprietary software) it is ideal.

Try to keep your laptop physically secure, even when using encryption. There are several methods to circumvent encryption, but most of them require you to type in your password after your computer has been tampered with. As well, make sure your laptop is shut off completely if you intend to leave it somewhere. When your device is powered on, it is vulnerable. Another option is to not store any data locally on the device.

If you are using Windows you can follow the instructions to encrypt it here: securityinabox.org/en/guide/veracrypt/windows **OR here:** howtogeek.com/howto/6169/use-truecrypt-to-secure-your-data

If you are using a Mac, follow the instructions to encrypt it here: securityinabox.org/en/guide/veracrypt/mac

If you want to hide the fact that you are using encryption software, you can create a portable version of VeraCypt instead of installing it, as described here: securityinabox.org/en/guide/veracrypt/windows/#portable-veracrypt

In order to encrypt a flash drive or other external drive, you can follow the instructions given here: esecurityplanet.com/open-source-security/how-to-encrypt-flash-drive-using-veracrypt.html

All of these tutorials link to an older version of the VeraCrypt site. The project has migrated from their old site to: veracrypt.fr/en/Home.html

Destroy all Information

Destroy all information before disposing of or selling something. Shred any papers that has your name or other personal information on it. Wipe all data from your devices before disposing, selling or donating them. (Note that there is no way to securely wipe flash devices. However, if you have completely encrypted the flash drive, any information that remains will be unable to be read, which is the closest you can get to wiping them.)

If you are using a Windows machine, instructions for how to delete your data can be found here: ssd.eff.org/en/module/how-delete-your-data-securely-windows

If you are using a Macintosh machine, instructions for how to delete your data can be found here: ssd.eff.org/en/module/how-delete-your-data-securely-mac-os-x

In order to securely wipe your phone before disposing of it, you can follow the instructions here: lifehacker.com/5808280/what-should-i-do-with-my-phone-before-i-sell-it

As well, it is advised to install and be familiar with remote wipe services for your mobile device, in case it is stolen or lost. It is relatively easy to retrieve personal data from a phone, including a home address. A how-to guide to set up remote wiping of your phone is here: pcmag.com/article2/0,2817,2352755,00.asp

Secure Browsing

There are a number of ways that simply browsing the internet can expose you to malware and eavesdropping. For browsers, Firefox is recommended due to its ease of use and respect for privacy, as well as its available security settings and extensions. There are a number of extensions that have been created to help maintain your privacy, some of which work with other browsers. The majority of these extensions will run silently in the background, while others require you to approve sites you trust. Choose which extensions you want to install, but know that each will protect your privacy in slightly different ways.

For safer browsing it is best to avoid auto run features, such as Flash (which has a history of exploits). To avoid malicious code **don't run Flash automatically**: yoursosteam.wordpress.com/2015/09/04/tip-15-start-using-click-to-play/

You can **adjust the privacy settings in Firefox** by following the instructions here: myshadow.org/how-to-increase-your-privacy-on-firefox

A list of extensions that protect your privacy are here: privacytools.io/#addons and here for Windows machines: securityinabox.org/en/guide/firefox/windows and here for Macintosh machines: securityinabox.org/en/guide/firefox/mac

Encrypt all Web Traffic

When browsing the internet on a public computer or your phone be particularly careful, as many protections that can be put in place on personal computers are not available. **Use a virtual private network (VPN) when not on a trusted network** (UWS is trusted. An airport or coffee shop Wi-Fi is not. It is relatively easy to eavesdrop on public Wi-Fi, even if it requires a password). Using a VPN will prevent someone connected to the same network as you from reading the information that you send over the internet. This can include passwords and other personal information. A VPN encrypts this information, so it is unreadable. As well, a VPN masks your IP address, preventing others online from knowing where you are. You do, however, need to be able to trust the provider of the VPN, as they can snoop on all the data you send. The University of Alberta provides VPN services that allows users to route their traffic through UWS. Using this will also allow you to easily access University services, such as library databases. IST recommends the Cisco AnyConnect client, but any VPN client can be used.

The how-to install guide and download links for the University of Alberta VPN can be found here:
uofaprod.service-now.com/kb_view_customer.do?sysparm_article=KB0012158

As well, the team should install *HTTPS Everywhere* for use in their browser. The extension re-directs all website requests you make through HTTPS, so that any data being sent is encrypted. However, websites that do not support HTTPS will not become encrypted, which exposes your to data eavesdropping. Most major e-mail providers support HTTPS browsing. As well, keep in mind that *HTTPS Everywhere* does not mask the metadata of your browsing, so others can still see things such as the domain name of the websites you are browsing and your IP address. It provides extra protection on top of using a VPN, but is not a substitute.

Get HTTPS Everywhere here: eff.org/https-everywhere A visual representation of what *HTTPS Everywhere* does is here: eff.org/pages/tor-and-https

Avoiding Attacks

Those employing phishing attacks can make their e-mails and the enclosed links look like they come from a trusted source. They can masquerade as others in the research group sharing a link to a inconspicuous file or they can look like Google is informing you that someone has logged into your account from a new computer. Links in these e-mails can then install spyware once they are opened or they can direct to a site that looks like a legitimate log-in screen. Therefore, never log into an account using a direct link from an e-mail. Navigate to the site manually, then log in and then complete any required tasks. In some cases your browser will give you a warning when you are linked

to a distrustful site, but as always, do not depend entirely on technology to protect you. Always be suspicious of anyone requesting any information. If you are unsure, use a different communication method to verify the validity of the request. Also be cautious of e-mail attachments, USB devices and files downloaded from the internet as these can all infect your computer with malware, which can record your keystrokes and steal your passwords.

An overview of malware attacks is here: ssd.eff.org/en/module/animated-overview-protecting-your-device-hackers
Information on phishing attacks, what they do and what they look like is here: ssd.eff.org/en/module/how-avoid-phishing-attacks

Posing as a "friend" is a common way to get access to your personal information, since sites like Facebook generally allow your "friends" to access all of it. Check with friends through a different communication channel if they own the account that is requesting friend status. If you do not know the person, do not accept the friend request. Information that may seem innocuous can be potentially harmful in the wrong hands, particularly when you take into account the metadata that may be packaged with it.

On Preventing Doxing

Doxing, the act of making personal information accessible with an intent to harm, can include information that may be embarrassing, taken out of context or may be a threat to your personal safety. This can include home and work addresses and personal habits, such as where your favourite place to eat lunch is. There are a number of ways that doxers can acquire this information.

1) **The best way to find out what information is available for doxers is to go looking for it yourself.** This is called self-doxing and a longer explanation of it is here: gendersec.tacticaltech.org/wiki/index.php/Complete_manual#Self-doxing This can be as simple as searching for your full name on Google. Depending on how common your name is and if you search for your name in quotes, the search results may be about you or unrelated to you. It is important to know what information about you is publicly available for a variety of reasons. You will have to decide for yourself if you are comfortable with the information that is obtainable. As well, it can be less intimidating if you know where someone found their information.
2) One of the easiest ways doxers obtain information is from what you have publicly provided through Facebook or other social media sites. **Make sure that your security settings for social media sites are as strong as they can be.** As well, be cautious of linking your accounts, as each account has different security settings and thus may inadvertently reveal some private data. **Always be aware of what you have posted about yourself, but also what you have posted about**

others, who may want their information kept more private. It is important to encourage a culture of asking for permission before posting, both within the research group and in your social networks. Also be aware that information that you share can be re-shared by your friends and used in unexpected ways.

- Instead of posting identifying information on public accounts, you can write "Info by e-mail request", which allows you to control the flow of your information.
- Use unique usernames for accounts you are trying to keep separate. As well, do not re-use pictures of yourself between accounts as a simple reverse image search can lead a doxer to other accounts. A more in-depth explanation of keeping accounts separate can be found here: blog.totallynotmalware.net/?p=15
- With this in mind, do not give out any personal information unless it is absolutely necessary and it is being given to a trusted party. If you want to sign up for an online service, but are unsure if you should give them your information, create fake information and use a disposable e-mail address. fakena.me generates fake "identities," complete with a temporary e-mail address that you can use for these purposes. Other disposable e-mail address services can be found here: gendersec.tacticaltech.org/wiki/index.php/Complete_manual#Disposable_email_addresses

3) A way to mitigate damage done by such attacks is to avoid having a single point of failure, for example, one e-mail that you use for everything. A good choice is to **have several e-mail addresses that are used for different online accounts or purposes**, such as a private e-mail address solely for online banking.
4) Know which services can leak your location. Both the content and metadata of photos and status updates can reveal yours and others' location. **Turn off geolocation services for your applications, cameras and online services and avoid posting information that may allow others to determine your location.** An outline of different types of location tracking can be found here: myshadow.org/location-tracking
   - Trollbusters outlines how different services, such as opening an e-mail, can be used to learn your location and how to prevent it: yoursosteam.wordpress.com/2015/09/04/tip-9-dont-leak-your-location/
   - You can see what metadata a file contains using a tool like Jeffrey's Exif Viewer, here: exif.regex.info/exif.cgi
   - You can remove or edit the metadata contained in a file using a program like ExifTool, which can be found here: owl.phy.queensu.ca/~phil/exiftool/
   - As well, turn off Wi-Fi on your phone when you are not using it. Allowing your phone to search for available networks can accidentally leak information, as described here: myshadow.org/location-tracking/#wifi-history
5) If you own a domain, the information that you used to sign up for the domain name may be publicly available through the domain registrar and WhoIs. A factor to consider when choosing a

domain provider is that some domain providers sell WhoIs privacy while others provide it for free. **Check if your domain provider offers WhoIs privacy and know what information is publicly available.** You can check what information is available by using the tool here: whois.net

6) There are also 3rd-party sites which collect and host data on people so that it can be easily found. A list of data broker sites can be found here: yoursosteam.wordpress.com/2015/08/30/remove-your-mailing-address-from-data-broker-sites and an article on these 3rd-party sites can be found here: computerworld.com/article/2849263/doxxing-defense-remove-your-personal-info-from-data-brokers

   Many of the sites regularly used in doxing are for U.S. residents only, however, you can still search by Facebook profile or e-mail. PeekYou and Pipl are two that allow you to search for Canadian residents, and several of these sites are looking to expand to Canada. These sites also regularly update with new information, which will then have to be removed again.

Dealing with Harassment

The research team needs a plan in place in the case that all or one of the members becomes a target of harassment. In the event that this occurs:

1) The team should keep records of everything: all threats and harassment should be documented. In order to do this, links and text should be copied-and-pasted into a shared file and screenshots should be taken of everything. IP addresses, screen names and e-mails of harassers should also be collected and stored on a shared file, along with the previous files. An offline backup of all of these files should be made.
2) A third party (someone who is not currently being harassed) should be available to screen messages in particularly bad situations.
3) Self-care should be of utmost priority. Those being harassed should remember to eat, sleep, consume media, socialize and get away from the online world as one usually would. In addition, those who are screening the harassment should be aware of their own needs and limitations. As well, the team as a whole should be available for discussion and support.

A quick outline of steps you can take to help mitigate harassment can be found here: geekfeminism.wikia.com/wiki/Mitigating_internet_trollstorms A longer article discussing a course of action after being doxed, which also applies to general harassment, is here: crashoverridenetwork.tumblr.com/post/114270394687/so-youve-been-doxed-a-guide-to-best-practices

This section of "Speak Up & Stay Safe(r)": onlinesafety.feministfrequency.com/en/#people-focused-strategies and this article: ashedryden.com/blog/you-asked-how-do-i-deal-with-online-harassment-

how-do-i-help-the-targets-of-online-harassment provides information on how to approach your social network and how to practice self-care. This article: iheartmob.org/resources/bystander_self_care outlines self care for bystanders and those in supporting roles.

Resources and References

Useful Guides to Online Safety

- ssd.eff.org
- onlinesafety.feministfrequency.com
- gendersec.tacticaltech.org/wiki/index.php/Complete_manual
- hackblossom.org/cybersecurity

Further Reading and Explanatory Links

Thoroughly research the online services and tools that you are going to use. Me and My Shadow has a good set of considerations to make when choosing new tools: myshadow.org/frameworks As well, privacytools.io is a site that recommends security focused software for a variety of functions.

Me and My Shadow project explains digital traces and provides information on how to control your data: myshadow.org

Explanation of the metadata of browsing and what is visible to others: ssd.eff.org/en/module/why-metadata-matters

Explanation of the security weaknesses of mobile phones: ssd.eff.org/en/module/problem-mobile-phones and here: securityinabox.org/en/guide/mobile-phones

Security suggestions for Windows 10: securityinabox.org/en/guide/basic-security/windows