Blueprints for Change

HOW-TO DRAFT:

DIGITAL SECURITY BASICS FOR CAMPAIGNERS

This doc was designed to travel. Please feel free to share this around with other progressive campaigners. You can download this (look under File menu top left) in several formats or link to it / embed it on a web page.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

For commenting permissions and other feedback, contact us at: **blueprintsfc@gmail.com**

Full library of how-to's and more info at: **www.blueprintsfc.org**

Disclaimer / request for your help

This is a work in progress that is meant to evolve over time with input from campaigners. At the moment, the tips and ideas here reflect the voices of the contributors/reviewers listed below. We are always looking to add more voices of campaigners that have knowledge and experience on this topic. If this is you, please contact us here: blueprintsfc@gmail.com.

Summary

Digital security practices help protect campaigners from malicious online attacks and intrusive surveillance efforts led either by groups that are hostile to your agenda or by repressive government agencies.

Who needs this?

Groups working on social/racial justice, environmental, immigration and refugee issues, as well as gender and reproductive rights are being targeted by hackers/trolls that are intent on subverting their work for political reasons. These groups often learn the price of unsecured digital tools the hard way when their accounts are accessed and corrupted by malicious actors. Campaigners working in environments under repressive regimes must also adapt their digital security practices to prevent surveillance and attempts to neutralize their groups through hacking and information leaks.

Impact/ Why do this?

Groups that put in place some basic digital security practices and tools are saving themselves from some potentially damaging attacks with a little effort and attention.

Take your internal digital security seriously! Make it as high a priority as data analysis, matching voter files to internal records, etc. Recent reports suggest that the Clinton campaign actively rejected advice to turn on two-factor authentication on its Google

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.
For commenting permissions and other feedback, contact us at: **blueprintsfc@gmail.com**
Full library of how-to's and more info at: **www.blueprintsfc.org**

accounts. The result was Clinton's campaign manager getting hacked -- in a way that couldn't have happened had he turned on two-factor authentication. This in turn enabled the release of thousands of damaging emails. The rest is history. Without security it's potentially game over.

Important first step: Threat/risk level assessment

Dia Kayyali, writing for the Center for Media Justice, explains that a threat modeling or risk assessment requires asking yourself the following five questions and recommends taking out pen and paper, brainstorming and consider discussing these questions along with the people you work closely with, since security is a collective effort:

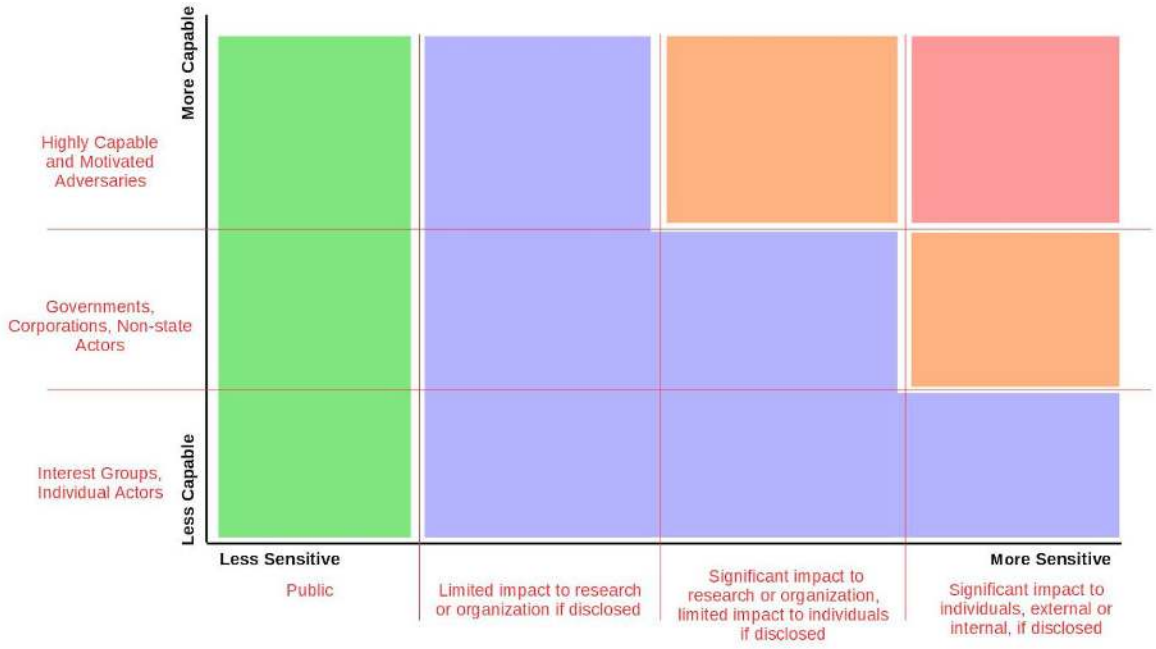
- What do I need to protect?
- Who do I need to protect it from?
- How much do they want that information, and how easy is it for them to get it?
- What happens if they do get it?
- What am I willing to do to stop that from happening?

A useful tool for conducting a risk level assessment is the Secure Communications Framework (SCF), developed by Tim Sammut. This tool uses a simple chart on which you can plot the different kinds of information, materials and data that your organisation works with, according to:

- The **capability** of external actors (adversaries, be they individuals or organizations) that would like to acquire this information, for undesirable purposes
- The **impact** of having this particular type of information compromised or exposed.

If your organisation manages data or information that falls in the blue quadrants (in the illustration below) then following basic best practices for digital security, as outlined in this guide, is sufficient. If you manage information in the orange quadrants then more stringent measures are required and it may be desirable to seek support from trusted security experts, such as the groups listed below. If your organisation manages information that falls into the red quadrant then working with trusted security experts is a must.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.
For commenting permissions and other feedback, contact us at: **blueprintsfc@gmail.com**
Full library of how-to's and more info at: **www.blueprintsfc.org**



Secure Communications Framework (Tim Sammut)

Setup steps/ stages

***If your threat level assessment reveals a very high risk of attacks, it is best that your organizations seek direct support from one of the groups listed below.

Groups facing a low to moderate threat can start with this list of 'must-do' practices that will close some of the basic vulnerabilities that are most often exploited by hackers.

Check if you have updated your OS, browser, and apps on all org computers and devices

More than 90% of software and operating system (OS) updates are to patch security vulnerabilities in programs!

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.
For commenting permissions and other feedback, contact us at: **blueprintsfc@gmail.com**
Full library of how-to's and more info at: **www.blueprintsfc.org**

Safety and privacy whilst browsing

If you are using public / untrusted wifi, using a Virtual Private Network (VPN) is recommended. A good open source option is Psiphon. If you are concerned about particular websites tracking your internet browsing then you can install an extension like Privacy Badger.

When you are browsing, a useful extension you can install is HTTPS Everywhere, which ensures you always use encrypted communication with a website, where possible.

Turn on two-factor authentication for every cloud service you use, work and personal.

"Two-factor authentication" adds an extra step when logging into an account. It requires you to enter a code (generated by an app or by a text message) in addition to a password. It's an important protection against "phishing" attacks, which can trick you into providing your login credentials to someone else. Services that provide two-factor authentication include Google accounts (covering Gmail, Calendar, and Drive), iCloud, Twitter, Facebook, Dropbox, Box, Microsoft accounts, and more (a more comprehensive list can be found here). For more protection, consider Google's Advanced Protection Program, which provides hardware "keys" that are necessary to log in to your accounts. (The Digital Security Exchange can provide these kits for free.). As a rule of thumb, if a service provider does not offer two-factor authentication then do not use it to store sensitive information.

Download and use Signal and Jitsi and get your colleagues to do it too.

Signal is a popular and secure messaging app that encrypts all of your conversations with other Signal users. It's important because regular SMS text messages are easy to intercept by law enforcement and other third parties. Signal makes it impossible for anyone but you to read the messages of those your communicating with. Plus, it has a great desktop app and it's easy to set up groups.

For secure online conferencing, campaigners who face security concerns recommend Jit.si - https://jitsi.org/

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.
For commenting permissions and other feedback, contact us at: **blueprintsfc@gmail.com**
Full library of how-to's and more info at: **www.blueprintsfc.org**

Blueprints for Change

Use a password manager to create and store strong passwords.

Weak passwords are an invitation to be hacked. A password manager like LastPass, 1Password or KeePass makes it easy to create unique, strong passwords for every account you have. Install one of those apps and start replacing and saving your passwords for all of your accounts. In addition, make sure the login passwords for your personal devices and for your password managers are strong.

Pro tip: It's a myth that strong passwords must contain every character under the sun. In fact, length is what matters. So when possible, use passphrases, not passwords. For example, a passphrase like "the russians probably interfered in our election" is a very strong passphrase!

Sarah Lange and Holly Davis from Blue Pine Strategies recommend the following wrt passwords:

- At least 13 characters in length
- Add numbers and special characters
- Use both uppercase and lowercase letters

Easy to remember, hard to crack:

- Line from a favorite book, movie, or song
- Address (not linked to you!)
- Mantra or intention
- Passphrase

Do not use information publicly available about you:

- Name of your partner, child, or pet
- Favorite sports team
- Favorite food

Change passwords frequently:

- Ideally every 3-6 months

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.
For commenting permissions and other feedback, contact us at: **blueprintsfc@gmail.com**
Full library of how-to's and more info at: **www.blueprintsfc.org**

Prioritize accounts for complex passwords

- Use one password per account

Make sure all of your devices are encrypted.

This makes it much harder for law enforcement or hackers to access the data on your devices. iPhones are already encrypted. Android phones are not (unless you have a Google Pixel), so you should go into the the Security settings and enable encryption. On Mac computers, go into System Preferences, then Security & Privacy, and turn on FileVault. On Windows, you should use the BitLocker application (preinstalled) to encrypt your drive.

If you want to encrypt specific information / files on your device then you can use an open source program like VeraCrypt.

Pay special attention to external hard drives and USB keys

Often forgotten in these measures are the external devices that we store our data on. Consider though that some of the most serious data leaks cames as a result of people leaving these devices around unprotected!

- First step is keeping a close eye on these devices and not leaving them around
- It is recommended that you encrypt your flash/hard drives and set password protection to access them

Mobile device security

- Make sure your mobile PIN is at least 6 digits, it is much easier to crack a phone with only 4.
- Make sure you keep auto-update of your applications switched on and ensure they are kept up to date. For Android, only download applications from the Google Play Store. If this is not possible, you can first upload APK files to www.virustotal.com.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.
For commenting permissions and other feedback, contact us at: **blueprintsfc@gmail.com**
Full library of how-to's and more info at: **www.blueprintsfc.org**

- Take extra care when accessing organisational information over public wifi - if you need to do this regularly then invest in a VPN.
- For groups that have more acute security concerns, a factory reset of mobile devices is recommended every few months to make sure any malicious tracking is wiped out (but this presents the inconvenience of re-configuring devices)

Tricky parts/ fixes

Most digital security measures take some time to implement and get used to. In the busy and resource-strapped world of advocacy campaigning, this can be a drag. However, if your security risks are low to moderate, then the measures outlined above may take some adjustment to implement but generally do not add a lot of extra time to day to day operations once they have been put in place.

Support groups

For groups around the world

If you represent a progressive group that needs immediate help, reach out to Access Now's Digital Security Helpline, which is available 24/7: https://www.accessnow.org/help/

For U.S. civil society groups

The **Digital Security Exchange** is here to help grassroots organizations build up their digital security. Contact us at info@digitalsecurityexchange.org for a free risk assessment.

The folks at **Ragtag.org** run a 'help desk' to support progressive campaigners. You can submit digital security questions to them here: https://www.campaignhelpdesk.org/

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.
For commenting permissions and other feedback, contact us at: **blueprintsfc@gmail.com**
Full library of how-to's and more info at: **www.blueprintsfc.org**

Blue Pine Strategies

Holly and Sarah, who helped with this guide, are available to discuss your group's situation and can help build a digital security approach for orgs large and small.

Get in touch for more information and services:
holly@bluepinestrategies.com
sarah@bluepinestrategies.com

Further resources

- Center for Media Justice - Getting Started with Digital Security: Tips and Resources for Activists

- Electronic Frontier Foundation's guide to Security Self-Defense: https://ssd.eff.org/ and guide to Surveillance Self-Defense: https://ssd.eff.org/

- Access Now's "A First Look at Digital Security," which features a number of risk profiles (and is great for leading trainings): https://www.accessnow.org/first-look-at-digital-security/

- Martin Shelton's "Securing Your Digital Life Like a Normal Person": https://medium.com/@mshelton/securing-your-digital-life-like-a-normal-person-a-hasty-and-incomplete-guide-56437f127425

- How to Lead a Digital Security Workshop https://motherboard.vice.com/en_us/article/4xby8g/how-to-give-a-digital-security-training

- "A DIY Guide to Feminist Cybersecurity": https://hackblossom.org/cybersecurity/

- APC's Digital Security First Aid Kit for Human Rights Defenders: https://www.apc.org/en/irhr/digital-security-first-aid-kit

- Tactical Technology Collective's Security in a Box: https://securityinabox.org/en/tools/

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.
For commenting permissions and other feedback, contact us at: **blueprintsfc@gmail.com**
Full library of how-to's and more info at: **www.blueprintsfc.org**

Attribution

Input and resources for this guide were provided by:

Josh Levy from Digital Security Exchange, Sarah Lange and Holly Davis from Blue Pine Strategies, Dia Kayyali from Witness, Martin Shelton, Steve Anderson, Chris Alford from Amnesty International

This guide was prepared and reviewed by:

Tania Mejia, Tom Liacas, Josh Levy, Chris Alford, Sarah Aoun, Steve Anderson

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.
For commenting permissions and other feedback, contact us at: **blueprintsfc@gmail.com**
Full library of how-to's and more info at: **www.blueprintsfc.org**