DIGITAL FIRST AID KIT

BETA VERSION

CREATED BY:

EFF, GLOBAL VOICES, HIVOS & THE DIGITAL DEFENDERS PARTNERSHIP, FRONT LINE DEFENDERS, INTERNEWS, FREEDOM HOUSE, ACCESS, QURIUM, CIRCL, IWPR, OPEN TECHNOLOGY FUND AND INDIVIDUAL SECURITY EXPERTS

TABLE OF CONTENT

The Digital First Aid Kit (Beta version)

Introduction

The Digital First Aid Kit aims to provide preliminary support for people facing the most common types of digital threats. The Kit offers a set of self-diagnostic tools for human rights defenders, bloggers, activists and journalists facing attacks themselves, as well as providing guidelines for digital first responders to assist a person under threat.

The Kit begins with ways to establish **secure communication** when you or a contact are facing a digital threat and want to reach out for support. The Kit then moves on to sections on **account hijacking, seizure of devices, malware infections** and **DDoS attacks**. Each section begins with a series of questions about you, your devices and your situation. These questions will guide you through a self-assessment or help a first responder better understand the challenges you are facing. It then lays out initial steps to understand and potentially fix the problems. The steps should also help you or a first responder to recognize when to request help from a specialist.

The Digital First Aid Kit is not meant to serve as the ultimate solution to all your digital emergencies. It strives to give you tools that can help you make a first assessment of what is happening and determine if you can mitigate the problem on your own. If at any moment you feel uncomfortable or unsure about implementing any of the solutions outlined here, ask for help from trained professionals.

The Digital First Aid Kit came about when a number of organizations working in the digital emergency field observed that once a person is targeted digitally, he or she often does not know what to do or where to turn for assistance. It was inspired by the belief that e*veryone has the ability to take preventative measures* to avoid emergencies and responsive steps when they are in trouble. Further, *everyone has the ability to help* out a colleague facing trouble. The self-diagnostic quality of the Kit should also enable journalists, bloggers, activists and human rights defenders to understand what is happening to their digital assets, to be able to determine more rapidly when they should reach out for help, what kind of help they need, and improve individual digital safety. In addition, the Kit serves as a first responder checklist for individuals who a person under possible digital attack reaches out to first.

The Digital First Aid Kit is a collaborative effort of EFF, Global Voices, Hivos & the Digital Defenders Partnership, Front Line Defenders, Internews, Freedom House, Access, Qurium, CIRCL, IWPR, Open Technology Fund and individual security experts who are working in the field of digital security and rapid response. It is a work in progress and if there are things that need to be added, comments or questions regarding any of the sections please go to Github.

Sections:

Secure Communication

This section will provide you with guidance on ways to **establish secure communication** when reaching out for help when confronted with a potential digital attack. As a general rule, it is important to understand that most 'normal' communications tools are not very secure against eavesdropping. Mobile and landline phone communication is not encrypted and can be listened to by governments, law enforcement agencies, or other parties with the necessary technical equipment. Sending unencrypted communication is like sending a postcard, anyone who has access to the postcard can read the message. Sending encrypted communication is like placing the postcard inside a safe and then sending the safe, which only you and those you trust know the combination to and are able to open and read the message.

Secure communication is always a trade-off between security and convenience. Choosing the most appropriate form of secure communication will depend on your unique situation, your threat model and the activities in which you are involved. The Digital First Aid Kit is specifically meant for those who are under digital attack; therefore, this section on secure communication assumes you are at high risk.

Finally, when communicating there are different levels of security. How and what kind of encryption a tool makes use of will increase or decrease your communication security. A communication tool that provides end-to-end encryption (such a PGP-encrypted email, or chat with OTR or Textsecure on your phone) is better than using a tool with transport-layer encryption (such as Gmail, Facebook, or Twitter). This, in turn, is better than using unencrypted communications (such as a postcard, your phone or text messages). Do the best that you can with the resources and skills available. Start with the most secure form of communication you can manage and the person you reach out to may be able to help you establish a line of communications that is more secure, if necessary. In many cases, it is better to reach out for help insecurely than not to reach out for help at all.

Where to start? If you believe that your computer has been compromised by malware and the device you are using cannot be trusted, please go directly to the **Safer Computing section p.7**. If you think that your communication might be targeted and/or you have just changed to a safer computer, the **Safer Communication section p.8** and **Safer Communication on a Smartphone section p.9** below provides steps to establish secure communications.

Seeking and providing remote help

When you are seeking remote help from a third party please keep the following in mind:

1. If you think there is something wrong with one of your devices or accounts and you are uncomfortable or unsure about what to do next, ask for help from a trained technical professional or **(inter)national organizations** whom you feel you can trust. The guides referenced in the **Resources section p.13** can also help. If possible, do not rely on unknown people you find online. Among the organizations you may reach out to include:

- **EFF**
- URL: https://www.eff.org/
- email: info@eff.org
- **Front Line Defenders**
- URL: http://www.frontlinedefenders.org/
- email: info@frontlinedefenders.org
- **CPJ**
- URL: https://www.cpj.org/
- email: info@cpj.org
- **RSF**
- URL: http://en.rsf.org/
- email: internet@rsf.org
- **Access**
- URL: https://www.accessnow.org/
- email: help@accessnow.org
- PGP key fingerprint: 6CE6 221C 98EC F399 A04C 41B8 C46B ED33 32E8 A2BC
- **Digital Defenders Partnership**
- URL: http://digitaldefenders.org/
- ddp@hivos.org
- **Freedom House**
- URL: http://freedomhouse.org/
- **Internews**
- URL: https://www.internews.org/
- **IWPR**
- URL: https://www.cyber-arabs.com/
- **Open Technology Fund**
- URL: https://www.opentechfund.org
- email: info@opentechfund.org
- PGP key fingerprint: 67AC DDCF B909 4685 36DD BC03 F766 3861 965A 90D2

2. When seeking help, also remember that the device you are using might be the subject of the attack. In order to establish a secure line of communication with a person who can help you, it may be necessary to contact them from an alternate, trustworthy device.

Safer computing: What to do when you can't trust your device?

If at all possible, you should switch to a completely separate device; one that you have no reason to suspect is compromised. Think of a device owned by a friend or family member. Cybercafes may be an option, but in many countries cybercafes are under heavy surveillance by local governments and law enforcement.

If you don't have access to a secure device, you may be able to download and install TAILS. TAILS is a 'live CD' (or USB) that runs a custom operating system that is built to be highly secure, but does not alter the computer you run it on. It has many features to help protect you from a compromised computer and to help you protect your communications.

Download, verify, and install TAILS carefully, following the instructions provided on the site [https://tails.boum.org/getting_started/index.en.html]. You will need a blank DVD, or a USB or SD card that is 2 gigabytes or larger. Some of the steps, particularly verifying the download, can be cumbersome, but they are crucial in assuring that the download you have received is the one you intended. You want to be sure that you are moving to a more secure setup as opposed to a less secure one.

Safer communications: What to do when you can't trust your communications channels

If you believe your communications are being targeted, you must stop using the communications services/accounts that you believe are compromised immediately. Create a new account and remember not to re-use your existing usernames, passwords or email accounts as you seek help.

*Note: If you are unable to set up PGP email with Thunderbird or OTR with Pidgin or Adium, **Mailvelope** [https://www.mailvelope.com/] for email and **Cryptocat** app for chat [https://crypto.cat/] in Firefox or Chrome are fast and simple ways to set up more secure communications in an emergency.*

The following important recommendations can help you to set up new channels of secure communication:

- After you've moved to a new device, create a new account using a new, secure password. *Under no circumstances should you re-use an account or a password you have previously used.* Find tips on creating a strong password here. [https://ssd.eff.org/your-computer/protect/passwords]
- Unless your threat model includes surveillance by very well resourced governments such as the USA, the UK, China or many governments listed in Google's transparency report, using Google products may afford you a degree of protection. Google tools (especially using Google tools on Chrome) can significantly increase security in these situations, and gives you access to more secure email, chat and voice/video conferencing. This security *only* helps 'inside' Google, i.e. Gmail to Gmail or Gchat to Gchat. It offers less protection if anyone forwards this information outside of Google, or a different email address then Gmail is added to a Gchat discussion.
- An alternative to Google is Riseup [https://help.riseup.net/], a volunteer group working to create democratic alternatives and practice self-determination by controlling our own secure means of communications. They offer services such as Gmail and Gchat. It is important to note that Riseup does not have the resources of Google. That said, depending on your situation, Riseup may be more appropriate.
- For end-to-end security, there are many tools with strong encryption you can use. Here are a few recommendations:
    - **Pidgin** [https://www.pidgin.im/] (PC) and **Adium** [https://adium.im/] (Mac) allow you to chat securely, with end-to-end encryption using OTR. Here is a guide to installing Pidgin with OTR: [https://securityinabox.org/en/pidgin_main].

- **Jitsi** can be used both for text chat as well as encrypted voice and video. Use this guide to set it up: [https://securityinabox.org/en/jitsi]. You can create an account for a secure voice/video call for free here: [https://ostel.co/]. Jtisi [https://jitsi.org/]
- **PGP** (PC and Mac) allows you to set up end-to-end encryption for your email. Here is a guide for using PGP with Thunderbird on your computer: [https://securityinabox.org/en/thunderbird_main].
- **Tor Browser Bundle** can be used to increase your security and privacy while visiting websites by bouncing your communications around a distributed network of relays run by volunteers all around the world [https://www.torproject.org/download/download-easy.html.en].
- A number of secure tools come pre-installed in TAILS.

Safer Communication on a smartphone

If you only have a smartphone, the following tools can protect your communication. Be aware that your phone is generally tied to your identity (through billing, account services or SIM card registration) and can reveal your location. These tools do not protect against this, they only encrypt the content of your communication.

Android

- **ChatSecure** by The Guardian Project [https://guardianproject.info/apps/chatsecure/] integrates with desktop chat Clients like Jitsi and Pidgin (using Gchat or Jabber/XMPP) and adds end-to-end encryption and the ability to send encrypted files, photos and audio.
- With **csipsimple** [https://play.google.com/store/apps/details?id=com.csipsimple] you can also make secure calls (such as from Ostel [https://ostel.co/]).
- **RedPhone** (for voice) and **TextSecure** (for SMS) by Open Whisper Systems [https://whispersystems.org] are good, but both parties must be on Android (with these tools installed) in order for these tools to work.
- These apps are in the Google Play store, the F-Droid repository [https://f-droid.org/repository/browse/] and available directly from the links above.
- **Orbot** by The Guardian Project and the Tor Project [https://www.torproject.org/docs/android.html.en] is an application that allows mobile phone users to access the web, instant messaging and email without being monitored or blocked by their mobile internet service provider. Orbot brings the features and functionality of Tor to the Android mobile operating system.

iPhone

Your iOS options are more limited, but the **ChatSecure** app on the iPhone is created in cooperation with the Android ChatSecure app and has similar features. **Onion Browser** [https://mike.tig.as/onionbrowser/] offers similar features to Tor and Orbot for iOS.

Trust

Whether you are helping someone remotely or seeking help from a third party, establishing trust is both very important and extremely complicated. You should presume an adversary

may have access to all your account details as well as your original communications when seeking help. This adversary has an obvious interest in intercepting your secure communications channel and providing specific, bad advice. Security tools have built-in ways to verify if the person you are talking to is actually the person you think you are talking to. When getting advice, compare it to concepts discussed on well-respected guides such as Security in a Box , resources at https://www.eff.org/ and https://pressfreedomfoundation.org/encryption-works
More information on the various technical aspects of trust can be found in the **Establishing Trust section p.30**.

Helpful resources

- Security in a Box; selecting and maintaining secure passwords https://securityinabox.org/en/chapter_3_1
- EFFs 'extensive' guidelines how to create a password

Account Hijacking

Are you having a problem accessing an email, social media or web account? Does an account show activity that you do not recognize? There are many things you can do to mitigate this problem.

Start by answering some simple questions:

- Which service are you having trouble with?
- Are you the only person who uses the account? Sometimes, multiple people have access to Facebook group pages, Wordpress blogs or email accounts. If multiple people have access to this account, first check that your friends or colleagues haven't changed permissions.
- What is the username and the URL of the account?
- Are you unable to access your account?
- Can you see someone else using your account?
- Did you get an alert or have friends/contacts received strange messages from you?
- What other evidence have you seen of the problem?

First steps to mitigate the problem:

If you still have access to the account

Move to a different computer - one that you consider to be safe or uncompromised. Log in and change the password on your account. Then move to the following steps:

- **Step 1:** Stop using this account for the exchange of sensitive information until you better understand the situation.
- **Step 2:** If possible, review the connection history/account activity (an available feature for Facebook, Gmail and other email platforms). Check to see if your account was used at a time when you were not online or if your account was accessed from an unfamiliar location or IP address.
- **Step 3:** Take a look at the account settings. Have they been changed? For email accounts, check for auto-forwards in email, possible changes to the backup/reset email address of phone numbers, synchronization to different devices, including phones, computers or tablets, permissions to applications or other account permissions.
- **Step 4:** Change the passwords for all your other online accounts that are linked to this one. For example, if you are looking at an email account and it is the recovery address for another account, change the password for that account.
- **Step 5:** Don't stop here! Follow the **important next steps below**

If you no longer have access to the account:

Follow the recovery procedures of the different providers. Note that different services have different ways to reset the password on your account. Some will send you a link to change your password using your recovery email address, while others reset it to your last

password. In the reset case it is important to change your password immediately after regaining access to your account. If these steps do not work and your account is being abused, contact one of the organizations listed above for possible support in shutting the account down.

Don't stop here! Important next steps:

If you suspect that someone else has access to your account, complete the following steps:

- **Step 1:** Answer the following questions for yourself: Who might have access to your account (friends, co-workers, spouse, children)? What devices (computer, phone, tablet) have you used to access the account? In what physical locations have you accessed these accounts (home, office, cybercafe, wifi network)?
- **Step 2:** Do you use the same password on other accounts? If so, perform the same checks on those accounts. Create new, unique passwords for each one.
- **Step 3:** Think about what you use this account for. Does it hold sensitive information? This could include your contacts, information about your location or the content of your messages. If you think this information could put your contacts at risk, inform them that your account has been compromised.
- **Step 4:** Repeat the review of the connection history/account activity - at least once a week for a month - to ensure that your account does not continue to show strange activity. If it continues to show strange activity, proceed to the malware section.

Take extra precautions against attackers:

Enable 2-factor authentication on this account, if it is available for the service you use. This is a process that requires you to confirm your identity on an alternate device (usually a mobile phone) when logging into an account. Google, Facebook, Twitter and WordPress support 2-factor authentication.

- Google: https://support.google.com/accounts/answer/180744?hl=en
- Facebook ('Login Approvals'): https://www.facebook.com/settings?tab=security
- Twitter ('Login Verification'): https://support.twitter.com/articles/20170388-using-login-verification
- WordPress: http://en.support.wordpress.com/security/two-step-authentication/

It should be noted that enabling 2-factor authentication on Google will force you to use custom per-application passwords for applications like Thunderbird, Jitsi, Pidgin and any other application that isn't connecting via the web interface. These can be set up in the account settings on the web.

Investigate

It is good to understand why your account was hijacked. Who do you think might be interested in targeting you or your organization? Is this threat related to your work? In the section on **Helpful Resources p.13** there are links to guides that give you tips and tricks on how to prevent digital emergencies and be proactive in your digital security.

Helpful resources and links:

Security in a Box: https://securityinabox.org/en/chapter_7_2
Threat models and Surveillance Self Defense: https://ssd.eff.org/ (Surveillance Self Defense is currently in the process of being updated, expected Autumn 2014)

Devices Seized

Is your device lost? Has it been stolen or seized by a third party? In any of these incidences it is very important to get a clear picture of what happened, what kinds of data and accounts may be vulnerable as a result and what steps must be taken to prevent the leaking and misuse of your information, contacts and accounts.

Start by answering some simple questions:

What happened?

- What sort of device are you missing? A computer, mobile phone, tablet or an external hard drive?
- When and where did you lose the device?
- How did you lose the device? Was it stolen by another person, taken by a state authority or did you simply lose track of it?
- Is the device still missing?

What kinds of security protections did the device have?

- Was the device protected by a password or other security measures?
- Which operating system was running on the device? Was this a legal version, or was it an illegal, jailbroken or rooted version?
- Does the device have full disk encryption turned on?
- What state was your device in when it was lost? Were you logged in? Was the device on but password-locked? Was it sleeping or hibernating? Completely turned off?
- Do you have remote access to the device?

What was on the device?

- **Make an inventory** of the different types of sensitive information that was on your device. Examples include email, chat history, social media, contacts (email, Skype, chat, etc.), files, location data, credit card data and more.
- What sort of base software was it using, i.e. Windows, OS X, Android, iPhone?
- Did you use encryption tools for email or chat (such as PGP and OTR)?
- **What accounts does this device have access to?** This can be email, social media, chat, IM and banking accounts that the device can access, browsers that have saved passwords to account, cookies that show your internet browsing history, authentication tokens such as fingerprint on iPhone 5 and accounts that use the device for secondary authentication.
- Do your accounts have saved passwords and/or automatically log in? This is common for email, Skype and other chat programs, or if you save your passwords in your web browser instead of a password manager like KeePass [https://securityinabox.org/en/keepass_main]

First steps to mitigate the problem:

If your device is still missing

If your device is lost or seized by a third party and you did not get it back, the first steps to take are the following:

- **Step 1:** When your device has access to accounts (email, social media or web account) remove the authorization for this device for all accounts. This can be done by going to your accounts online and changing the account permissions.
- **Step 2:** Change the passwords for all accounts that are accessible by this device.
- **Step 3:** Turn on 2-factor authentication for all accounts that were accessible by this device. Please note that not all accounts support 2-factor authentication [See 2-factor notes from 'Account Hijack' section].
- **Step 4:** If you have a tool installed on your lost devices that allows you to erase the data and the history of your device, use it.

If you get your device back

If your device was lost, taken by a third party or had to be handed over at a border crossing but you have it back, be careful as you do not know who has had access to it. Depending on the level of risk you're facing, you may want to treat the device as if it is now untrusted or compromised. Ask yourself the following questions and assess the risk that your device has been compromised:

- How long was the device out of your sight?
- Who potentially could have had access to it?
- Why would they want access to it?
- Are there signs that the device has been physically tampered with?

For more extensive threat modeling assistance see the Surveillance Self Defense Guide.

If you have lost contact with your device for an extended period of time and you feel there is a chance that something has been installed on it, please consider the following:

- **Computer:** reinstall the OS from scratch and recover all documents from the last backup and scan all your documents and files with antivirus software. For more guidance on this, see **cleaning up your device p.18** in the malware section.
- **Phones and tablets:** Depending on your level of risk and the circumstances under which your mobile phone or tablet was taken, it may be advisable to not use it again. If possible, migrate all of the data off of your phone or tables and purchase a new one. If you cannot change devices but you suspect it might be compromised, take precautions and do not use your phone or tablet for sensitive communication or opening sensitive files. Do not take it with you when going to sensitive meetings or have it with you when discussing sensitive topics.

Don't stop here! Important next steps:

Whether your device is still lost or you have it back, complete the following steps:

- **Step 1:** Think about what you used this device for - is there sensitive information on this device, such as your contacts, location or the content of your messages? Can this data be problematic for someone?
- **Step 2:** Inform your network. Inform the key and high-risk contacts you work with privately. If you feel comfortable doing so, post a list of potentially compromised accounts on your website or a social media account.
- **Step 3:** Do you use the same password on other accounts or devices? If so, perform this process on those accounts. They may also be compromised.
- **Step 4:** If possible, review the connection history/account activity of all accounts connected to the device (available feature on Facebook, Gmail and other email providers). Check to see if your account was used at a time when you were not online or if your account was accessed from an unfamiliar location or IP address. See the **Account Hijacking section p.11** for further details.
- **Step 5:** Check the account settings of all accounts connected to the device. Have they been changed? For email accounts, check for auto-forwards, possible changes to the backup/reset email address of phone numbers, synchronization to different devices, including phones, computers or tablets, and permissions to applications or other account permissions.
- **Step 6:** Repeat the review of the connection history/account activity - at least once a week for a month - to ensure that your account does not continue to show strange activity. If the history/account activities continue to show strange activity, proceed to the malware section.

Take extra precautions against attackers:

Prevention is the key to mitigating the risk of having your device seized, lost or stolen. However, simple actions can protect the data on your device if it is seized. Think about encryption, passwords, pin code locks for cell phone backups, tools that allow remote data wipes, installation of alert software in the case of theft**.** Prey Anti-Theft is a useful cross-platform and open source device tracking tool [https://preyproject.com/].

Investigate

If your device has been stolen or seized by a third party, it is good to understand why this has happened. Who do you think might be interested in targeting you or your organization? Is this threat related to your work? In the section on **Helpful Resources p.16** there are links to guides that provide tips and tricks on how to prevent digital emergencies and be proactive about your digital security.

Helpful resources

Security in a Box: https://securityinabox.org/en/chapter_7_2
Threat models and Surveillance Self Defense: https://ssd.eff.org/ (Surveillance Self Defense is currently in the process of being updated, expected Autumn 2014)

Malware

'Malware' is **mal**icious soft**ware** that facilitates an unauthorized takeover of your device by another user, government or third party to perform surveillance functions such as recording keystrokes, stealing passwords, taking screenshots, recording audio, video and more. While most malware is designed for and utilized by criminals, state-sponsored actors have increasingly adopted malware as a tool for surveillance, espionage and sabotage. Malware is used to gain control of devices. It exploits access to the device to send out spam, seize banking, email or social media credentials, shut down websites and collect vital information from journalists, human rights defenders, NGOs, activists and bloggers. If you suspect a malware infection on your device here are some things you can do:

Start by answering some simple questions:

- Are you sure this is not account hijacking or a compromised password, see **Account Hijacking p.11**
- What are your **indicators of compromise**, see below?

What is an 'indicator of compromise' anyway?

There are many reasons why you may think your device has been infected with malware; these are called 'indicators of compromise.' They may include the following:

- You opened an attachment or link that you think may have been malicious
- Your webcam LED turns on when you are not using the webcam
- Your accounts have been compromised multiple times, even after you have changed the password

You may also have reason to suspect your device is infected with malware if:

- Your device was seized and then returned
- Someone broke into your home and may have tampered with your device
- Some of your personal data has been made public and it could only come from your personal computer
- Your group is being targeted by a government, law enforcement, or an actor with equivalent capabilities

First steps to mitigate the problem:

After confirming that it is not an account hijacking and there are clear indicators of compromise there are two avenues of approach: getting your devices clean or understanding the attack and then cleaning your devices. Your first priority may be to get your computer 'clean' and usable again. Finding out what has happened to you and who has targeted you may be less important to you. However, it can be very valuable to gain understanding of your adversary, their technical capabilities and whether or not the potential attacker (a government entity or other third party) is known to use internet surveillance technology. If understanding the attacker and the attack is relevant to you, it is essential that collecting and analyzing information on a potential malware infection happens before you engage in 'cleaning' your computer. For information collection and analyzing of

malware continue to the **section recommended steps for first level analyst p.19** otherwise, proceed to the section below.

'Cleaning' your device

When you have chosen to clean your device without understanding the malware and attack first please keep the following in mind:

1. There is no quick fix to clean up malware from you computer. Even after completing the following steps a very sophisticated malware infection may still be present. These steps are sufficient to remove most of the malware you are likely to encounter unless you are being targeted by a very advanced attacker.
2. If you believe that you are being targeted by a state actor and indicators of compromise persist after cleaning up the virus detected through the steps below, disconnect it from the internet, turn off the device, unplug it, if possible remove its battery and seek the help of a security professional.

Anti-virus

Anti-virus software can be an effective first response to protecting a device from a significant percentage of malware. However, anti-virus software is generally considered ineffective against targeted attacks, especially by state-sponsored actors. Nevertheless, it remains a valuable defensive tool against non-targeted, but still dangerous, malware. Below is a non-exhaustive list of options:

- Microsoft Safety Scanner (Windows): http://www.microsoft.com/security/scanner/en-us/default.aspx
- F-Secure: http://www.f-secure.com/en/web/home_global/online-scanner
- Kaspersky: http://www.kaspersky.com/security-scan
- ClamXav (Mac OS X) : http://www.clamxav.com/
- TrendMicro: http://housecall.trendmicro.com/
- ClamAV (Windows and Linux) : http://www.clamav.net/lang/en/

When you run anti-virus software, ensure that it is up to date. If a virus is detected the following steps are recommended.

- **Step 1:** Ensure that your anti-virus software is up to date
- **Step 2:** Take a screenshot of the message
- **Step 3:** Continue with the recommended steps to remove the virus
- **Step 4:** Following the guidelines in the Safer Communication section above, send the screenshot to a person with security expertise

Don't stop here! Important next steps:

If you suspect a state sponsored attack or want to know more about the attack and attackers, it is important to gather as much forensic information as you can; please proceed to the **section on recommended steps for first level analyst p.19**. In certain computers you can swap the hard disk, keeping the infected hard disk safe for forensic analysis and enabling computing with a new disk.

- Back up your files and reinstall your operating system; it is not possible to be sure the virus has been completely removed. After installing one malware, the attacker usually installs others; therefore, it is always recommended to reinstall the operating system after performing a thorough wipe of the hard drive. If possible, investigate whether replacing your hard drive is an option.
- After reinstallation of the operating system you will want to have access to your files again. Be aware that malware could have infected your documents. After reinstalling your operating system, you should take the following steps:
- If possible, retrieve your documents from the back up you made prior to the malware infection.
- If you do not know when your device became compromised with malware, or if you suspect specific attachment and documents to be infected with the malware, there are several things you can do:
- Download all of your executable files again from a trusted source
- If the attack vector has been identified by an technical expert and the malware is clearly infecting other documents, one option could be to upload and open them in Google Docs and re-download them from there. In most cases opening a suspicious document in Google Docs is probably a good recommendation. The document will not infect your computer and it will remain editable.
- Another option is to copy the documents onto a USB key and open them on CIRCLean. The malware will not be copied, but the documents will be transformed to an image or pdf, a read only and non-editable format.

Recommended first steps for a first-level analyst

The following recommendations should only be implemented by a person with some security expertise. If you do not have the necessary expertise to follow the instructions below, ask a specialist for help. If possible, communicate with them via secure channels using the guidelines in the Safer Communications section.

The first steps to take:

- If one of the indicators of compromise is an email, gather the headers: [https://www.circl.lu/pub/tr-07/], and analyze them: [https://support.google.com/mail/answer/29436?hl=en]. Google also provides a simple tool that does this automatically: https://toolbox.googleapps.com/apps/messageheader/
- If possible, securely obtain the malware itself and look it up on Virus Total with the hashes to see if the file has already been uploaded [https://www.virustotal.com/].
- If the file is not confidential, you can also upload it on Malwr and analyze the result [https://malwr.com/].
- If the suspicious file comes from a link, get the full URL and run it in:
    - http://urlquery.net/
    - http://wepawet.iseclab.org/

What is next?

Step 1: Information collection for further analysis

The following information is critical for any further analysis, by you or by anyone else. It is recommended to collect most - and if possible all - of the information below for further analysis:

- Information on the system (hardware, OS details, including version and update status)
- Location of the victim and system localization (source IP, country, language of the user)
- List of users sharing the same device
- In case of suspicious email: full headers
- In case of a link: the full link, timestamp and screenshot
- It would also be useful to have a dump of the webpage, and a packet capture of the connection to it
- Memory dumps, see tutorial on memory dumps by Circl here https://www.circl.lu/pub/tr-22/#memory-acquisition
- Disk images, see tutorial on disk images by Circl here: https://www.circl.lu/pub/tr-22/#disk-acquisition
- Results from tool of integrity check (if used)
- Evaluate possibility of remote forensics and if so, establish proper channel of communication

Step 2: Malware analysis
If you do not have the skills to process this information, pass it on to a trusted, trained malware expert or one of the following organizations:

- EFF; https://www.eff.org/ info@eff.org
- Citizen Lab http://citizenlab.org/ info@citizenlab.org
- CIRCL http://www.circl.lu/ info@circl.lu

Take extra precaution against attackers

Malware is potentially the most dangerous attack against an activist, as it provides easy access to account information as well as extensive personal and project related documentation. There is no single or simple method to protect yourself from malware, but you can make yourself a more difficult adversary.

Keep in mind, however, that specialized and targeted malware will not be detected by even the best anti-virus software. Steps 1 and 2 make you safer against older malware, but only by changing your behavior will you improve your resilience.

- **Step 1:** Regularly check for updates to all of your software, especially your operating system and your browser
- **Step 2:** Install and configure an anti-virus program (see above) and make sure it updates automatically. Some anti-virus programs will stop after their trial period expires without warning.
- **Step 3:** Change your own behaviors. Email and chat attachments are common 'attack vectors' where a compromised computer of a friend will automatically try to send malicious attachments to the owner's entire address book. Ask people to send documents in plain text where possible and *never open unexpected attachments* without carefully verifying that the sender intended to send it! Tibet Action's 'Detach

from Attachments' provides further suggestions [https://tibetaction.net/knowledge/tech/attachments/]. Using a third party service like Google Docs to open office documents and spreadsheets can also let you see and edit the content with a much lower risk of a malware infestation.

- **Step 4:** Further protection can be provided by adding plugins to your browser such as HTTPS Everywhere [https://www.eff.org/https-everywhere] or NoScript for Firefox [http://noscript.net/].

Investigate

If your devices have been compromised by a targeted attack, it can be valuable to understand why you've been attacked and by whom.

Why you've been attacked: Who do you think might be interested in targeting you or your organization? Is this threat related to your work? In the section on **Helpful Resources p.21** there are links to guides that give you tips and tricks on how to prevent digital emergencies and be proactive about your digital security.

By whom: What are your adversary's technical capabilities? Is the potential attacker (a government entity or other third party) known to use internet surveillance technology. In the section on **Reports on State-sponsored Malware attacks** below, there is more information on the different ways in which governments have used malware for targeted attacks.

Documentation: It will be difficult to remember specifics such as the time and date when you clicked on a suspicious link. Therefore, we recommend keeping a notebook next to your computer to make notes of the time, date and strange things that have happened and are happening to your device. In some cases experts have been able to identify a specific type of malware by correlating the time of the attack with unique characteristics or **a possible indicator of compromise p.17**.

Reports on State-sponsored Malware attacks:

- Syria reports: https://www.eff.org/deeplinks/2013/12/social-engineering-and-malware-syria-eff-and-citizen-labs-latest-report-digital
- Vietnam report: https://www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal
- Report FinFisher https://citizenlab.org/2013/04/for-their-eyes-only-2/
- Report Blue Coat https://citizenlab.org/2013/07/planet-blue-coat-redux/
- Report HackingTeam https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/

Helpful resources

- Detach from Attachments: https://tibetaction.net/knowledge/tech/attachments/

- Google's Chrome browser and the open source version, Chromium, provide excellent information about suspicious websites
- More on Viruses and Spyware https://securityinabox.org/en/chapter_1_2

DDoS mitigation

A threat faced by many independent journalists, news sites and bloggers is having their voices muted because their website is down or defaced. In many cases, this maybe an innocent and frustrating problem, but on occasion, it may be due to a 'denial of service' attack or a website takeover. This section of the Digital First Aid Kit will walk you through some basic steps to diagnose potential problems. If your site is under a denial of service attack, some immediate options for next steps are suggested.

In general, it is important to know that there are many reasons why your website can be down. Most often this is due to programming errors or technical problems at the company that hosts the site. Sometimes, other things like legal challenges can cause a host to turn a site off as well. Finding the problem and possible solutions to your website's problem can be cumbersome if you do not have hosting expertise. Therefore, when possible, the best first step is to contact a trusted person who can help with your website (your webmaster, the people who helped you set up your site, your internal staff if you have them and the company that hosts your site).

It is good practice to **contact your webmaster and the site host** after investigating these common challenges below**!** The problem you face may not have been reported on their status page, may be a temporary problem, or the site host may not yet be aware of the problem. A good relationship with your service providers goes a long way - be clear and polite and share the results of your investigation using these questions to help them quickly troubleshoot the problem.

Start by answering some simple questions:

Basic information

- Who built your website? Are they available to help?
- Who is your web hosting provider? This is the company that provides the server where your website lives. If you do not know, you can use a tool like this: http://www.whoishostingthis.com/ to help.
- Do you have your account log in details for this hosting provider?
- Where did you purchase your domain name? In some cases this is also your website host, but it could also be another company.
- Do you have the log in details for the domain name service? If not, finding these is your first step to recovering your site
- Who else knows or may have access to these account details?

Diagnostic information

There can be different reasons why your website is down. This can range from network to policy, hosting, blocking, software, defacement and performance problems. The section below explains what each of these problems is and how to diagnose which problem you are facing.

- **Is your web host working, but your website is unavailable?** Check http://www.isup.me/ - your site might be up, but you can't see it. This is a ***network problem***. Your own iinternet connection could be having problems or be blocking your access to your site. This could also indicate that your account has been disabled: **Are you seeing a message from your web hosting provider?** You could have been taken offline for billing, legal, copyright or other reasons. This is a ***policy problem.*** First, make sure your billing information is up to date and that there is no outstanding balance on your hosting services or your domain name. If the message is due to a legal issue, the resources provided by EFF, while focused on US copyright laws, are a good place to learn more: https://www.eff.org/issues/bloggers/legal/liability/IP.

- **Is your site not loading at all?** Your hosting company may be having problems, in which case you may be facing a ***hosting problem***. Can you visit the website of your hosting company? Note that this is **not** the admin section of your own site, but that of the company or organization that hosts your site. Look or search for a 'status' blog (e.g. status.dreamhost.com); also search on twitter.com for other users discussing downtime at the host - a simple search like '(company name) down' can often reveal whether others are having the same problem.

- **Can you visit other sites with similar content to your site?** Try visiting websites related to yours or covering similar issues. Also try using Tor [https://www.torproject.org/projects/gettor.html] or Psiphon [https://psiphon.ca/products.php] to access your site. If this helps, you have a ***blocking problem*** - you are still online for other parts of the world, but are being censored in your own country.

- **Are you seeing error messages?** This could be a ***software problem***. You should reflect on any recent changes you or your team may have made and contact your webmaster. Sending your webmaster a screenshot, the link of the page you are having problems with and any error messages you see will help them figure out what might be causing the problem. You might also copy the error messages into a search to see if they are easily fixed.

- **Are you seeing a website that is not yours? Are you receiving a warning from your browser about malware on your own site?** This could be a ***defacement problem.*** See below for next steps; you will need to work with your web hosting provider and review the **Account Hijacking section p.11**.

- **Is your site loading intermittently or unusually slowly?** Your site may be overwhelmed by the number and speed of requests for pages it is receiving - this is a ***performance problem***. This could be 'good' insofar as your site has become more popular and it simply needs some improvements to respond to more readers - check your site analytics for a long-term pattern in growth. Contact your webmaster or hosting provider for guidance. Many popular blogging and CMS platforms (Joomla, Wordpress, Drupal and others) have plugins to help cache your website locally and integrate CDNs, which can dramatically improve site performance and resilience. Many of the solutions below can also help performance problems.

First steps to mitigate the problem:

When you are suffering from a Denial of Service attack

If the above diagnoses do not help (or you are experiencing a severe ***performance problem***, your site may be the victim of a **'denial of service' attack**, where a malicious user (or users), try to view the website repeatedly and rapidly (using automated tools), and in doing so crowd out legitimate readers. Sometimes it's one 'attacker' trying to do this to your site, which doesn't usually cause much of a problem - unless you pay for bandwidth. More common is the 'Distributed' denial of Service (DDoS), where an attacker uses thousands of machines under his control to targets a site.

- **Step 1:** Contact a trusted person who can help with your website (your webmaster, the people who helped you set up your site, your internal staff if you have them and the company that hosts your site).
- **Step 2:** Work with the company you bought your domain from (like EasyDNS, Network Solutions, GoDaddy) and change the 'Time to Live' or TTL to 1 hour. This can help you redirect your site much faster once it comes under attack (the default is 72 hours, or three days). This setting will often be found in 'advanced' properties for your domain, sometimes part of the SRV or Service records. [Network Solutions: http://www.networksolutions.com/support/how-to-manage-advanced-dns-records/] [GoDaddy: http://support.godaddy.com/help/article/680/managing-dns-for-your-domain-names]
- **Step 3:** Move your site to a DDoS mitigation service. See https://github.com/OpenInternet/MyWebsiteIsDown/blob/master/MyWebsiteIsDown.md#mitigation-services for a full list. To start:
    - Deflect.ca [https://www.deflect.ca/]
    - Google's Project Shield [https://projectshield.withgoogle.com/en/]
    - CloudFlare's Project Galileo [https://www.cloudflare.com/galileo]
- **Step 4:** As soon as you have regained control, review your needs and decide between a secure hosting provider or simply continuing with your DDoS mitigation service.

When you are suffering from a Website Defacement

- **Step 1:** Verify that this is a malicious takeover of your website. An unfortunate but legal practice is to buy recently expired domain names to 'take over' the traffic they had for advertising purposes. It is very important to keep payments for your domain name in order.
- **Step 2:** If your website has been defaced, first regain control of your website login account and reset its password, see the **Account Hijacking section p.11**. for help.
- **Step 3:** Make a backup of the defaced site that can later be used for investigation of the defacement.
- **Step 4:** Temporarily turn off your website - use a simple landing page or 'parked' page.
- **Step 5:** Determine how your site was hacked. Your hosting provider may be able to help. Common problems are older parts of your site with custom scripts/tools

running on them, out of date content management systems, and custom programming with security flaws.

- **Step 6:** Restore your original from backups. If neither you, nor your hosting company have backups, you may have to re-build your website from scratch! Also note that if your only backups are at your hosting provider, an attacker may be able to delete those when they take control of your site!
- **Step 7:** Move to a DDoS Mitigtion service or secure hosting provider (see a list of secure hosting services below on p. 28). Deflect.ca can support you in protecting your site from online attacks. CloudFlare can also block many common attacks. Secure hosting providers such as VirtualRoad/Qurium go to great lengths to detect and prevent such attacks.

Don't stop here! Important next steps

Don't wait until you have been attacked! All of the services listed below will work quickly to help you recover during or after an attack, but you can protect yourself now, before any attack happens! This can reduce costs by lowering your bandwidth usage and keeping you online during an attack. Once you've been hit, it can take up to three days for the internet to 'find' you at your new, protected address - so in almost every case, it's much better to **be prepared and get started now**.

1. **Secure Hosting Providers** require you to move your website completely to their servers - you're changing hosting providers. Many of them can help you through this. The benefits of this include the hosted solution often providing many other protection features in addition to DDoS mitigation; the downside can be cost (depending on what you currently pay) and control - you need to be able to trust your domain host, as they have a lot of control over your website.

   Pros:

   - Provides one central service for most, if not all, your website needs
   - Provides protection services for DDoS, hacking and spam attacks
   - Often includes many secondary services and consulting, and even limited legal defense in some cases
   - Full support teams are often on staff to help

   Cons:

   - You must host your website with the service
   - You must trust the service to manage your site and defend your rights
   - These services are often much more expensive (but you don't have to pay other hosting / DNS services anymore!)

2. **DDoS Mitigation services** let you continue hosting your site wherever it is, and just change how others on the internet find and access it - this is generally much easier to set up. These services have servers around the world that, essentially, get out in front of your website and absorb or ignore malicious traffic. They 'mirror' and serve constantly-updated copies of your site. These services are easy to set up and you

maintain complete control of your website and hosting setup. One challenge with proxied services is that very complex websites can sometimes experience problems with non-admin user logins and complex interactive/javascript area. Please discuss these with your webmaster and the proxy service as most can be resolved.

Pros:

- Lower cost (often with a free level)
- Quick and easy to set up
- You don't have to change your existing website host
- You can change or quit the service at any time

Cons:

- Fewer support options
- Focused primarily on just mitigating DDoS attacks - does not necessarily include help with malware or spammers.
- SSL (encrypted) traffic will be briefly decrypted and re-encrypted by the proxy server to pass it from their proxy to your server.

3. Choose a specific provider - for any service, you must be comfortable with the provider. This relates to trust, but also understanding their business model: Is it fee-for-service? If there's a free version, does it receive less support than a paid alternative? Is it funded by governments? It is best to cover as much detail up front as possible to avoid surprises down the road.

For all services ask yourself the following questions:

- How is the company/organization structured and sustained? What types of vetting or reporting are they required to do, if any?
- Consider what country/countries they have a legal presence in and which they would be required to comply with law enforcement and other legal requests
- What logs are created, and for how long are they available?
- Are there restrictions regarding the type of content the service will host/proxy, and could they have an impact on your site?
- Are there restrictions on the countries where they can provide service?
- Do they accept a form of payment you can use? Can you afford their service?
- Secure communications - you should be able to log in securely and communicate with the service provider privately.
- Is there an option for two-factor authentication, to improve the security of administrator access? This or related secure access policies can help reduce the threat of other forms of attacks against your website.
- What type of ongoing support will you have access to? Is there an additional cost for support, and/or will you receive sufficient support if you are using a 'free' tier?
- Can you 'test-drive' your website before you move over via a staging site?

Questions for secure hosting services

- Do they offer full support in moving your site over to their service?
- Are the services equal to or better than your current host, at least for the tools/services you use? Top things to check are:
- Management dashboards like cPanel
- Email accounts (how many, quotas, access via SMTP, IMAP)
- Databases (how many, types, access)
- Remote access via SFTP/SSH
- Support for the programming language (PHP, Perl, Ruby, cgi-bin access...) or CMS (Drupal, Joomla, Wordpress…) that your site uses

Questions for DDoS Mitigation services:

- If you use SSL (also known as HTTPS or secure web traffic), ask how they manage SSL. In some configurations, it may be easiest to share your private SSL key. If you do so, you need to have a high level of trust in the service provider, as they can 'impersonate' your site (indeed, this is what you are asking them to do by providing a proxy!)
- Ask about how administration /editorial logins and pages are managed
- Talk about any interactive parts of your website (users who log in, comment, admin/editorial needs, complex interactive pages/javascript/animations) - different proxy services manage these differently; you will need to test these before switching completely.

Specific Mitigation Services

Specific services are listed at https://github.com/OpenInternet/MyWebsiteIsDown/blob/master/MyWebsiteIsDown.md#mitigation-services with extensive notes. Please note that the list provided is not a complete listing of services; there are many more. However, these services all represent good starting points, as they have been used by other members in the independent media / human rights / free speech communities. For immediate coverage, here are options:

Secure Hosting Services:

- Qurium (formerly Virtual Road) [https://www.qurium.org/]
- The Positive Internet Company [http://www.positive-internet.com/services/vip-hosting]
- Greenhost [https://greenhost.net/]

DDoS Mitigation Services:

- Deflect.ca [https://www.deflect.ca/]
- Google's Project Shield [https://projectshield.withgoogle.com/en/]
- CloudFlare's Project Galileo [https://www.cloudflare.com/galileo]

Take extra precaution against attackers

Even if you have not experienced a Denial of Service attack, this guide offers steps to prepare for one, hopefully preventing any downtime at all. Go straight to the **Responding to**

a Denial of Service Attack section p.25 to investigate common solutions you can implement now, before being attacked. At the **Helpful Resource section p.29** you can find guides to keep your site alive.

- **Backups**: It's always good to ensure you have backups (that you store somewhere other than the same place your website is!). Many hosts and website platforms include this as part of their service, but it's best to also have additional, offline copies.
- **Keep up to date**: If you are using a Content Management System (CMS) such as WordPress or Drupal, check to make sure that your website technology is updated to the latest software, especially if there have been security updates. If you are using custom software, consider moving to a CMS that receives regular updates.
- **Monitoring**: There are many services that can constantly check on your site and email or text you if it goes down. This Mashable article lists ten popular ones. Be aware that the email or phone number you use for monitoring will be clearly associated with managing the website. [Mashable article: http://mashable.com/2010/04/09/free-uptime-monitoring/]

Investigate

If you have been the victim of a **'Denial of Service' or Defacement attack**, it can be valuable to understand why you've been attacked and why now.

Why you've been attacked and why now: Who do you think might be interested in targeting your website or your organization? Have you recently posted something controversial, could this threat be related to your work or does your website receive a lot of traffic and did your domain name expire? Why now? Could a recent change to your website have made you a target for Denial of Service attacks or Defacement attacks? In the section **on Helpful Resources p.29** there are links to guides that give you tips and tricks on how to prevent digital emergencies and be proactive in your digital security.

Helpful resources:

My Website is Down: https://github.com/OpenInternet/MyWebsiteIsDown
Keep your site alive: https://www.eff.org/keeping-your-site-alive
Security in a Box: https://securityinabox.org/en/chapter_7_2
Threat modeling, Surveillance Self Defense Guide: https://ssd.eff.org/risk/threats

Establishing Trust

In the secure communication chapter we mention some basic ways to begin to establish trust between someone seeking help and someone helping out. This section addresses how to add a technical layer of trust onto that, and understand the tools that help you maintain a secure conversation with only the person you think you're conversing with. It's important to note that while this section is rather technical, do the best you can - it is better to use encryption tools than to not use them!

Encryption tools like OTR ("Off The Record") and PGP ("Pretty Good Privacy") provide many benefits. Encrypted messages or files with OTR or PGP are protected from anyone peeking at them or tampering with them from when they leave your computer until they reach their destination. The problem, though, is knowing for certain if their destination is the 'right' one.

To use encryption tools like these, you must know the right address to send the encrypted message to - this is not just an email account or IM nickname, but requires more specific information - the encryption 'key' that goes with that account. Most of this is managed by your computer, but it is important for you to provide the final sign-off! Theoretically, if you were trying to establish secure communications with someone, an attacker could replace the specific encryption information with their own and read your communication. To defend against this, there are a few tricks.

Website Trust

Secure websites (those starting with HTTPS) have a system where browsers rely on a limited number of trustworthy companies to manage this. This makes it relatively easy for users, but if any of these companies are compromised (which has happened!) or are willing to cooperate with a government that may be a threat to you, the entire trust network becomes a problem (this same model is also used for a specific type of email security which is called S/MIME).

Trust in Communication Tools

For email, chat and secure phone calls, it is a bit more 'direct.' The ideal situation is that you meet someone in person to exchange the fingerprint information. There is no risk of someone 'intercepting' and changing this in a face-to-face meeting! Obviously that's not always possible. Different tools have different ways around this problem. Security in a Box has an entire chapter devoted to private communications. [Security in a Box https://securityinabox.org/en/chapter-7]

Chat: 'OTR'

In chat or instant messaging, the current standard for trust is called OTR, or Off The Record. This is not the same as 'off the record' messaging in GChat, which only means that Google does not store a permanent log of the conversation. OTR provides the basic benefits above (secured end-to-end and proof against tampering), but notably also provides an additional layer of security - each conversation session is protected separately. This means that if someone is able to store all of your private chat conversations, breaking the encryption of one chat provides no ability to read any of the other chats. This also allows a degree of

'deniability,' i.e while your conversation is protected and authenticated, there is no way to prove that any of the messages came from you as opposed to someone else. OTR works in Adium, Jitsi and Pidgin. [Adium: https://adium.im/] [Pidgin: https://www.pidgin.im/] [Tutorial on Pidgin: https://securityinabox.org/en/pidgin_main] [Jisti: [https://securityinabox.org/en/jitsi]

To benefit from all of this, however, you must find a way to 'authenticate' the person you are chatting with. You only have to do this once per device for each secure contact (and you can use apps like KeySync to help). The key to linking this digital trust with a person you know is through a shared secret - you can call each other and directly compare a code unique to your accounts, or use a question-and-answer method where you know only this specific person would know a secret word you've agreed on or a specific piece of private information. [KeySync: https://guardianproject.info/apps/keysync/]

Resources

- Authentication in OTR: https://securityinabox.org/en/pidgin_securechat
- OTR Technical details: https://otr.cypherpunks.ca/

Email: PGP

PGP (or Pretty Good Privacy) and its open source equivalent, GPG (Gnu Privacy Guard) allow you to encrypt emails and files for yourself or to send to others. With plugins like Enigmail for Thunderbird or GPGOL for Outlook, you can use PGP very effectively to protect the contents of your email (though not the subject, or who you're emailing with). [Tutorial on Enigmail: https://securityinabox.org/en/thunderbird_main] [GPGOL: http://www.gpg4win.org/]

To send a PGP encrypted email, you do not need your own PGP keys. PGP Keys come in pairs, a public one and a private one. The public one is like a house address that anyone can know but only someone with the 'private' key can access the account to receive messages sent to that address. By the same magic of PGP, only the person at that address (with the private key) can send messages out from that address (which can be verified by the public part of the key). See the resources listed below for more in-depth discussions on how PGP works.

The problem, of course, is finding the public key 'address' - there are digital phonebooks for PGP keys where you can search for emails or names [https://sks-keyservers.net/i/#extract and https://pgp.mit.edu/ are popular] - but there is no central authority guaranteeing that these keys belong to the right person. It's completely possible that someone has uploaded their own key and even a fake email address, impersonating someone else.

Again, the trick is to verify that the key is correct using another method - many people will exchange slips of paper with their key 'fingerprint' (see some at the top of this document associated with email help-desks!), or post them on their twitter profiles or web pages. The problem is that this only works for a small community of friends, not on a global internet scale.

For people who are relatively safe and can be public about their contact network, you can 'sign' the PGP keys of other people you have met and verified. This helps fix the trust problem by creating a 'web of trust,' i.e. if you have verified someone's key and you trust them to verify the keys of others, you can also trust any key they have signed off on.

Generally, however, this is not a huge problem as long as you have reasonable trust that you have the right key and right email address of the person you want to communicate with, and treat any unexpected changes in keys and email addresses with suspicion.

Resources

- https://pressfreedomfoundation.org/encryption-works#pgp
- https://www.cryptoparty.in/brief#crypto

Encrypted Voice: ZRTP

ZRTP is in many ways similar to OTR, in that it changes for every conversation, protecting the history of your communications. ZRTP is the standard in fully encrypted voice calls (using Jitsi, RedPhone, or Silent Circle). It requires you to read aloud a short series of characters to the person you're speaking with in order to authenticate the call using your voice in combination with these unique characters.
[Jisti: https://securityinabox.org/en/jitsi] [Redphone: https://whispersystems.org] [Silent Circle: https://silentcircle.com/]

Resources

- https://jitsi.org/Documentation/ZrtpFAQ#faqHow
- https://silentcircle.com/web/faq-zrtp/?#7

Helpful resources

Resources related to digital emergencies

- EFF https://www.eff.org/
- Digital Defenders Partnership www.digitaldefenders.org
- Front Line Defenders http://www.frontlinedefenders.org
- Internews https://www.internews.org/
- Freedom House http://freedomhouse.org/
- Access https://www.accessnow.org/
- CPJ https://www.cpj.org/
- RSF http://en.rsf.org/

Digital security guides

- Security in a Box https://securityinabox.org
- Surveillance Self-Defense https://ssd.eff.org/
- Information security for journalists https://www.cpj.org/reports/2012/04/information-security.php
- Communications Security: https://help.riseup.net/en/security
- Short 'How To' Mobile Security Guide https://guardianproject.info/howto/
-

Guides on Secure hosting and DDoS mitigation

- My Website is Down; Documentation and guides for withstanding DDoS Attacks https://github.com/OpenInternet/MyWebsiteIsDown

- If you are currently researching how to build your website to be resistant to attacks that might take it offline, you should first read through this guide by the Electronic Frontier Foundation: https://www.eff.org/keeping-your-site-alive

- AccessNow provides a much more in-depth guide with many more resources and mitigation techniques in English, Farsi, Arabic and Russian. Visit https://www.accessnow.org/policy/docs and click on DoS on the right side, or download a copy from https://s3.amazonaws.com/access.3cdn.net/3fd9faf32feb878cf7_krm6iy7bo.pdf

Resources related to Non-digital emergencies

- **Front Line Defenders**: provides support to Human Rights Defenders who are faced with an emergency http://www.frontlinedefenders.org/emergency

- **S.A.F.E Initiative**: integrated safety trainings that combine and address safety through the lens of digital identity, physical awareness and psychosocial care to at-

risk media practitioners. An IREX initiative. http://www.irex.org/project/safe-securing-access-free-expression

- **Media Legal Defence Initiative**: support to journalists, blogger and independent media under legal threat http://mediadefence.org/get-help

- CPJ: provides direct assistance to journalists at risk and their families http://cpj.org/campaigns/assistance/

- CPJ: journalists security guide https://www.cpj.org/reports/2012/04/journalist-security-guide.php

Glossary

- **DDoS / Distributed Denial of Service Attack:** A 'Denial of Service' attack is where a malicious user (or users) crowd out legitimate users of a service such as a website or a chat server. Sometimes it's one 'attacker' trying to do this to your site, which doesn't usually cause much of a problem - unless you pay for bandwidth. More common is the 'Distributed' Denial of Service (DDoS), where an attacker uses thousands of machines under his control to targets a site.

- **DNS Record:** The DNS record is like the master contact list of the phone book of the internet. All website servers are identified by a series of numbers and/or coded letters (the IP Address) - Google.com is 74.125.228.69, for example. By changing this record, you can give out a different IP Address for a website, i.e. a new hosting provider's address or a proxy for your original website.

- **Domain Name:** The human-readable name of your website - Google.com, for example.

- **End-to-end encryption**; means that messages or files leave your device encrypted and remain encrypted until they reach the rights address (a specific user).

- **Hibernate**: A process by which the computer will attempt to use the least amount of energy while providing the ability to boot up quickly. Like the sleep state, the system shuts down the display, hard drives and remotely connected devices, but will continue providing enough power to the computer to start quickly. It does this by writing the content of the memory to a file on the disk. On some computers the hibernate state can lower the security of the system. See also: Sleep

- **IM:** Instant Messaging. Examples of Instant Messaging are services like Google Chat and Facebook Chat, or any service using the XMPP (Jabber) method.

- **Nameserver:** When a browser wants to find a website it will first contact a name server. This tells the browser to connect the domain name (Google.com) to it's internet address / IP Address (74.125.228.69) via it's DNS Record (above). By changing the DNS record at a name server, you can 'point' the browser to a different server.

- Technically speaking the browser still checks with /etc/hosts before going to DNS, that's how one can block access to FB on their computer by routing facebook.com to another IP address. It is also useful for accessing some websites blocked through DNS blocks.

- **Sleep:** The operating system shuts down the display, hard drives and remotely connected devices off but will continue providing enough power to the computer to start quickly. Unlike the Hibernate state, the content of the memory is not written to disk.

- **SSL:** See explanation Transport Layer Encryption or Wikipedia [https://en.wikipedia.org/wiki/Secure_Sockets_Layer#Description]

- **SRV or Service record:** A Service record or SRV record is the record in the Domain Name System that defines the location, (the hostname and port number) of servers for specified services.

- **Threat modeling**: a way to make a assessment of the threats you are facing, the origin from the threat and the assets you are trying to protect. The threat can vary depending on your location, what you do and who you are working with.

- **Transport Layer Encryption**: are cryptographic protocols (Transport Layer Security (TLS) and Secure Sockets Layer (SSL) designed to provide secure communication channels over the Internet.

- **Vetting:** is the process of performing a background check on an individual or an organization before engaging in a financial, service or other type of relationship with them.

- **Website host:** The server where your website and its files/databases are stored.

- See also: https://securityinabox.org/en/glossary