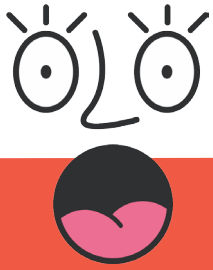
DIGITAL SECURITY

Training Kit

Kit#1

I LOST ACCESS TO MY EMAIL, FACEBOOK OR TWITTER USER ACCOUNT. WHAT SHOULD I DO IF SOMEONE STOLE MY LOG-IN INFORMATION AND I CAN NO LONGER LOG IN?



ONE DAY YOU SWITCH ON YOUR COMPUTER AND YOU CAN NO LONGER LOG IN TO YOUR EMAIL, FACEBOOK OR TWITTER ACCOUNT. YOU ARE SURE THAT YOU REMEMBER YOUR PASSPHRASE CORRECTLY AND YOU SUSPECT THAT SOMEONE ELSE HAS CHANGED IT.

WHAT YOU SHOULD DO

You need to double-check first of all that you are on the correct log-in page; that the link and interface you are seeing are genuine. Look carefully for slight variations in the URL. It might be useful to ask someone around you to check that the service you are trying to access is not out of order; this sometimes happens even to the biggest service providers.

Reset your passphrase. If you are unable to log in, proceed as if you forgot your passphrase and need to reset it. Almost all online services have at least one way to reset a passphrase and regain access to the account.

Email: Most email providers will allow you to reset your passphrase, and will send a reset link to a secondary email or a temporary log-in code to your mobile, or ask you to answer a series of security questions. Passphrase recovery options are different for each provider but instructions should be easy to find.

Facebook: Follow the "Forgot your password?" link and identify your account. Then you will be offered the chance to reset the passphrase either through an email to the email address associated with your account or through a text message to the mobile number associated with your account. (See Kit #3) If you no longer have access to those for any reason or the hacker changed the information in the account, you will have the option to submit a new email or phone number to be used instead, followed by asking your "trusted contacts" to help you in the process. Sometimes you have to wait 24 hours until you can access the account again. If you ultimately can't regain access to your account, you should consider reporting to Facebook that your account has been hacked.

Twitter: If you can't log in to your account, you can request a temporary log-in code to be sent to your email address or mobile phone via SMS. This temporary code is not reusable. You can also request a reset link to be sent to your email address by following the "Forgot password?" link on the Twitter log-in page.

While you are without access to your account, it is a good idea to have a person you trust to write to your key contacts and warn them that you are without access to your account and someone may be acting as an impostor.

HOW TO PREVENT FUTURE PROBLEMS

ONCE YOU RECOVER ACCESS TO YOUR SERVICE, DO THE FOLLOWING IMMEDIATELY:

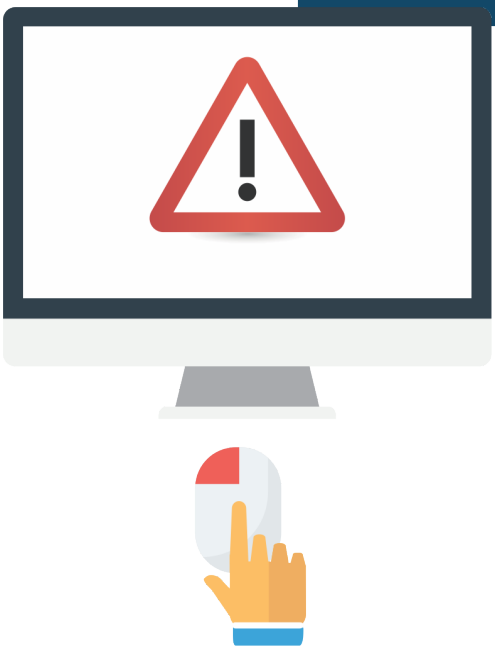
- Go to your account settings to change your passphrase and add a secondary email address.
- If you can, consider adding a mobile phone number, unless your government is known or suspected to work together with mobile operators to hijack people's accounts, in which case don't add your number. If this is not a concern where you live, having both a passphrase and mobile phone verification is called "two factor authentication" (2FA) and increases the security of your account.
- Go to your account's security settings and activate log-in alerts or log-in verification. On Facebook you can review a list of active sessions into your account and their locations. If you notice any unfamiliar devices or locations, click "End Activity" to end the session.
- Review the third-party applications that have been granted permissions on your account. On Facebook you can define your "Trusted Contacts" to help you with future lockouts.
- Check carefully all the accounts in your Facebook friend and Twitter following lists to make sure that you are not newly associated with any suspicious, unknown accounts. This is important on Facebook because depending on your privacy settings, your posts could now be visible to these accounts.

KEEP IN MIND

- The attacker will not always hack into your account and change the passphrase to lock you out. An attacker could gain access to your account to impersonate or survey you. You might not notice that you're a victim of hacking.
- Each time you log into your account you establish a new session and when you log out you end it. Always log out from sessions on a web browser. You need to keep an eye on active sessions and activities such as messages, posts, third-party applications and new friends to make sure everything is done by you.
- Common attacks on Facebook happen through malicious links that appear to be something they are not. These links might reveal your personal information or facilitate an adversary taking control of your account. Do not click or interact with any links or attachments that you get from untrusted people in your inbox, or suspicious links from your trusted contacts.
- Make sure you always use HTTPS when logging into your accounts. If you are connecting from your phone, try avoiding use of your phone's standalone application because you cannot control whether or not the connection is secure. Instead, connect to your social network's HTTPS URL via the browser on your phone.
- It is true that Facebook might be an efficient tool for organising, but always remember it is not a safe and secure platform. Your friends and contacts can be negatively impacted by flaws in your security practices and vice versa. Conducting activism online is therefore a great responsibility.

Where to find more help

- Manage **where you are logged into Facebook.**
- Recover a **lost or forgotten passphrase on Twitter** and find out if your **Twitter account is compromised.**
- Learn some safety tips for **social networking sites.**
- Find out if your **Gmail account has been hacked.**



IF THE CONTENT OF MY COMPUTER GETS CONFISCATED, I AM AFRAID IT WILL COMPROMISE MY SAFETY

MY COMPUTER MIGHT GET LOST, STOLEN OR CONFISCATED. IS THERE ANYTHING I CAN DO TO MINIMISE THE RISK THAT ITS CONTENT WILL COMPROMISE ME OR OTHERS?

COMPUTERS OFTEN GET LOST OR STOLEN AND CAN ALSO GET CONFISCATED BY AUTHORITIES WHO ARE AFTER YOUR DATA. YOUR DEVICES ARE VAULTS FULL OF SENSITIVE DATA. IF THIS DATA IS DISCOVERED BY SOMEONE UNTRUSTED, IT CAN DO A GOOD DEAL OF DAMAGE. FOR EXAMPLE, IF YOU MANAGE YOUR EMAILS USING AN EMAIL CLIENT SUCH AS THUNDERBIRD OR OUTLOOK IT'S LIKELY THAT THE PROGRAMME CONTAINS PRIVATE INFORMATION, SUCH AS YOUR FRIENDS' CONTACTS AND SENSITIVE MESSAGES. IF YOUR COMPUTER IS LOST, STOLEN OR CONFISCATED, THE NEW OWNERS GAIN ACCESS TO ALL THIS INFORMATION. WHAT CAN BE EVEN MORE DAMAGING IS IF THEY START ACTING LIKE IMPOSTORS, WRITING TO YOUR CONTACTS PRETENDING THAT THEY ARE YOU.

WHAT YOU SHOULD DO

Not much can be done once your computer is lost. So you should prepare your system and use your computer in such a way that in the eventuality of its loss, the leakage of contacts and other sensitive data is minimal.

- Use passphrases. As a most basic protection against information leakage due to an opportunistic (not targeted) theft or loss, use a desktop passphrase. Configure your device to require a passphrase when it is switched on, and activate a passphrase-protected screen saver or lock screen that automatically activates after five minutes of computer or device inactivity.

- Please keep in mind that this makes it difficult for someone with physical access to gain access to the data and applications on your computer or device, but circumvention of a passphrase is relatively easy for experienced technologists or law enforcement.

- Keep your user accounts safe. Don't let your browser store your passphrases. Don't store them in a text file on your desktop. Don't send them to yourself by email or SMS. Don't write them down on a piece of paper on your desk. Passphrases to your online user accounts need to be either in your mind or stored in an encrypted manner (see Kit #3).

- Protect your email. Make sure your email client permits you to passphrase-protect access to your profile. While this helps against a common thief, this won't stop computer experts who might be interested in getting to your data. If compromising the content of your emails poses a real threat to you, consider storing all data from your email client in an encrypted volume with TrueCrypt. [1] You can configure your mail client to prompt you for your passphrase the first time your client downloads new messages or sends messages. This can prevent someone from impersonating you.

- Encrypt sensitive files. Get into a habit of separating even mildly sensitive data from other data on your computer, and keeping sensitive data encrypted. Use a specific encryption software such as the free/libre and "available source" TrueCrypt to create an encrypted volume (disk-space) on your hard drive. Place your sensitive information in the encrypted volume. An encrypted volume is like a vault that can be opened only by you or others with whom you share the passphrase.

- Encrypt the device's drive. By using disk encryption, you guarantee that you are the only person who can access the content using the passphrase. At the level of the operating system, you can encrypt the entire computer, which protects everything while the computer is off.

Note that once the disk is decrypted and the computer is on or hibernating, the data is generally accessible until the disk is fully encrypted again (usually by switching the computer off).

- TrueCrypt works on Windows, Mac and GNU/Linux. Device encryption on Android and iOS can be enabled under device settings. If you are a GNU/Linux user you can encrypt during the installation process. It is extremely important to note that without your encryption passphrase there will be absolutely no way to access the data (which is the point; however, this potential loss of control of your own data is in itself a risk).

Where to find more help

- **Protect sensitive files on your computer.**
- Create and maintain secure passphrases.
- **Protect the content of your Mozilla Thunderbird email client.**
- **Learn about GNU/Linux operating systems.**
- Learn about TrueCrypt.

Note : In September 2015, critical security flaws were reported in TrueCrypt, the open source software for file and disk encryption. As a result, we are reviewing our advice and we support these recommendations for alternative tools for secure file storage.

Kit#3

I NEED TO KEEP MY PASSPHRASES SAFE

I KEEP ALL IMPORTANT PASSPHRASES IN MY PAPER AGENDA AND IN MY MOBILE PHONE AND MY BROWSER REMEMBERS ALL THE PASSPHRASES I USE ONLINE. THAT IS PROBABLY NOT SAFE. IS THERE A BETTER SOLUTION?

YOU'RE USING SEVERAL ONLINE SERVICES AND HAVE A DIFFERENT PASSPHRASE FOR EACH BECAUSE IT'S SAFER. YOU CAN'T REMEMBER ALL OF THEM SO YOU ALLOWED YOUR BROWSER TO REMEMBER THEM WHEN YOU FIRST LOGGED IN. YOU ALSO HAVE OTHER IMPORTANT AND SENSITIVE DETAILS TO REMEMBER, SUCH AS PINS, CREDIT CARD NUMBERS AND IMPORTANT PHONE NUMBERS. SINCE IT'S IMPOSSIBLE TO REMEMBER THEM ALL, YOU KEEP THESE NUMBERS AND PASSPHRASES ON PAPER AND IN A TEXT DOCUMENT ON YOUR DESKTOP. IF THE PAPER AGENDA IS LOST YOU'LL BE LOCKED OUT OF YOUR ACCOUNTS. IF SOMEONE GAINS PHYSICAL ACCESS TO YOUR COMPUTER OR MOBILE PHONE AND FINDS THE PAPER AGENDA, TOO, THEN GAINING ACCESS TO ALL OF YOUR ACCOUNTS IS TRIVIAL.

What you should do

There are a few options for good passphrase management and many poor passphrase management practices. Here is a list of what you should and shouldn't do.

Never store passphrases or other sensitive details in a text file on your desktop or in any other way that would permit intruders into your computer to easily find them.

Don't store passphrases in your browser's passphrase manager. Allowing your browser to "remember" passphrases to online services such as your email or Facebook account means that it stores your passphrases in a single unencrypted file that can be

easily recovered and read by anyone who gains access to your computer, either physically or remotely. For example, someone could get remote access via a malware programme. If this happens, see Kit #1: My email, Facebook or Twitter account was hijacked. From the browser settings menu, stop storing your passphrases, delete those that are already stored in your browser, and disallow the browser from ever asking you to store your log-in information again.

Install a standalone passphrase manager application. This allows you to easily copy and paste passphrases into online forms. The software is designed so that you never need to display the passphrase on your screen. And because you do not need to type them it protects you from some sophisticated monitoring techniques, particularly from shoulder surfing. If someone takes control over your computer, they won't be able to access any of this information without knowing the master passphrase to your passphrase manager application.

A recommended passphrase manager application is KeePassX for Windows, Mac and GNU/Linux. KeePassX is easy to use, doesn't need installation and can be moved around with USB storage. Some passphrase managers, including KeePassX, allow you to not only store passphrases, but also any type of text or file types as attachments that you can lock under the master passphrase.

To keep in mind

- Consider revisiting all your passwords and changing them to passphrases, which are longer and more secure.
- Consider changing all of your passphrases annually.
- Be aware that not even the use of standalone password managers can 100% protect you from password theft, particularly if your computer is infected by a sophisticated malware. However, the use of a password manager such as KeePassX significantly decreases the risk of such thefts.
- Create secure passphrases using Diceware.

Where to find more help

Learn more about creating passphrases that you can memorise.

See Kit #4. I need to carry around sensitive data in a secure manner.

Create and maintain secure passphrases.

Get started using KeePassX – Secure passphrase storage.

Use KeePassX in your browser, across your computers and on your phone

Kit#4

I NEED TO CARRY AROUND SENSITIVE DATA IN A SECURE MANNER

I HAVE SENSITIVE DATA THAT I NEED TO PHYSICALLY TRANSPORT BETWEEN TWO OR MORE PLACES. HOW DO I MAKE SURE IT STAYS SAFE?

YOU ARE ABOUT TO TRAVEL OR MOVE AROUND BETWEEN DIFFERENT LOCATIONS IN YOUR CITY FOR AN IMPORTANT MEETING, LIKELY WITHOUT INTERNET ACCESS. YOU NEED TO BRING WITH YOU SENSITIVE DATA THAT YOU AREN'T COMFORTABLE UPLOADING TO A SERVER OR OTHER ONLINE SPACE.

What you should do?

In order to move around with sensitive data, you will need to not only encrypt the data but obscure its very existence.

- Obscure the data physically. Consider transporting files on a small device instead of on your laptop. SD cards and USB drives can store a huge amount of data in a very small device. These devices can be hidden (and lost!) just about anywhere. Insert the SD card into an otherwise harmless electronic device if you or your bags must pass through a metal detector or x-ray, such as an empty (clean) mobile phone or camera.

- Once you've decided how you're going to transport the data, encrypt the data. TrueCrypt [1] or GPGTools can encrypt any directory or file (see Kit #2. If the content of my computer gets confiscated, I am afraid it will compromise my safety).

- Alternatively, encrypt the entire drive. Depending on what device or volume you will store your sensitive data in, consider encrypting everything, not just the sensitive files. If you do this, keep in mind that it may be more obvious that you are hiding something

- Obscure the data digitally. If you choose to secure your data in an encrypted volume with TrueCrypt, you can also make the volume "hidden", which can help you avoid the possibility of an adversary finding your files and asking or forcing you to reveal the decryption passphrase. Or, you might simply rename the

encrypted file to something unassuming like “My Music” and place it within a typical directory structure.

Keep in mind

- The way USB drives and SD cards store data in solid state means they are very reliable but also makes wiping data off of them difficult. Sometimes the only safe way to destroy the data to avoid eventual recovery is to literally destroy the device.
- Note that passphrase-protection of a directory or file is not encryption and is very easy to circumvent.
- If the device containing the sensitive data is discovered and accessed, an unusual operating system such as GNU/Linux or the immediate appearance of a full-disk decryption prompt may in and of itself reveal that you are hiding something. Sometimes it is best to use the hide-in-plain-sight tactic.

Where to find more help

- Use a persistent volume.
- Learn how to create hidden volumes with TrueCrypt.

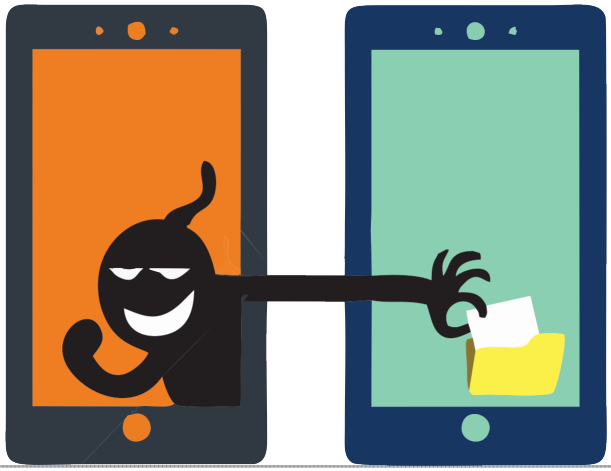
[1] Note: In September 2015, critical security flaws were reported in TrueCrypt, the open source software for file and disk encryption. As a result, we are reviewing our aadvice and we support these recommendations for alternative tools for secure file storage.

I NEED TO SECURE MY MOBILE DEVICE AND COMMUNICATION

I LIKE THE CONVENIENCE OF USING MY MOBILE DEVICE TO COMMUNICATE WITH FRIENDS, FAMILY AND COLLEAGUES ALIKE, BUT I'M CONCERNED ABOUT MY PRIVACY. IS THERE A WAY I CAN SAFELY USE MY PERSONAL MOBILE FOR SENSITIVE COMMUNICATIONS?

YOU ARE SECURITY CONSCIOUS AND WANT TO COMMUNICATE SECURELY WITH YOUR MOBILE DEVICE JUST LIKE YOU DO WITH YOUR LAPTOP. YOU MIGHT WANT TO HAVE ACCESS TO YOUR WORK EMAIL ON YOUR MOBILE, TO BE ABLE TO BROWSE THE WEB ON YOUR PHONE ANONYMOUSLY, OR EVEN CIRCUMVENT CENSORSHIP WITH YOUR MOBILE CONNECTION. BUT YOU'RE NOT SURE HOW TO DO ALL OF THESE THINGS IN A SECURE WAY OR WHAT TO AVOID.

Mobile smartphones are small, expensive and can contain a huge amount of information. Mobiles are not built with security and privacy in mind. Call logs, messages and geographic positions are shared with and stored by the mobile company, whom you must trust to implement good security practices and comply with local laws to protect your privacy. In most countries, the government, a possible adversary, can easily gain access to that data. Your mobile provider can also block services or censor content, again often at the request of the government.



What you should do

- Avoid standalone applications. Mobile apps such as Facebook and Twitter are not privacy-friendly. To install them, you must give them permission to access, and in some cases control, many other services on your device. You cannot control their method of connection and by default many use insecure HTTP connections, not HTTPS, to connect to the internet. Use your mobile browser instead.

- Protect your media. Its highly advisable not to store any sensitive images or videos on your device in the first place because many common applications have access to your gallery. ObscuraCam is a mobile app that can encrypt your images and videos.

- Lock your device and SIMs. Enable SIM and screen locks on your device. By doing this, it prevents an opportunistic thief or adversary with average technical skills from changing the SIM or accessing your content.

- Encrypt your device. Encrypting your relatively new Android or iPhone device and its data is a very easy and essential step to start with, and it protects the data in case of physical loss or confiscation. You just need to enable encryption and set a good passphrase to make sure your data is private and not accessible if the attacker has physical access to the device. Note that device encryption only protects your data as long as the device remains encrypted (usually when it is off). The encryption cannot protect devices that are on from data theft.

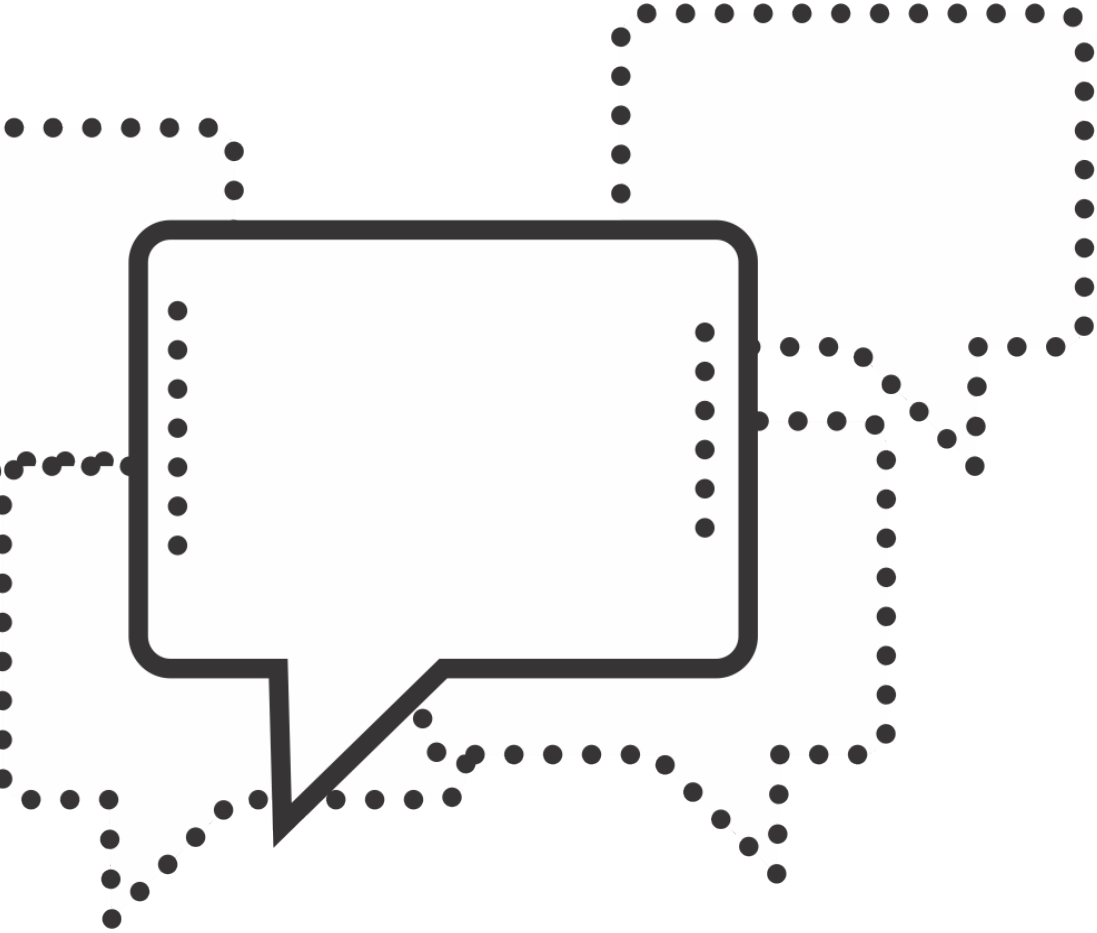
- Browse anonymously. You can use Tor on your mobile by browsing the web with Orweb. Or you could configure your entire device to route traffic through a VPN (See Kit #12. I need to access a blocked website anonymously).

- Email with caution. It is advised not to read or write sensitive email with your mobile and to never store your encryption keys (such as OpenPGP) on the device. You could create a separate email and private/public OpenPGP key pair for use exclusively on your mobile.

- Send and receive messages securely. With messaging, you are only as safe as the application you use. Instead of WhatsApp, Skype or Viber use Signal. Signal allows you to send messages and make encrypted voice calls.
- Speak confidentially. Keep in mind that the mobile's microphone can be turned on by applications. Even switching off the phone isn't good enough because the mobile phone provider (or the government via the provider) has the technical means to remotely activate the device. When talking about sensitive issues, take out the battery or keep the phone far away from you.
- Backup your data. Frequently backup the important data on the device such as your contact list.
- Revoke access. If your device was stolen, lost or confiscated you should immediately use a web browser to change the passphrases of the accounts you were logged into on your device. You can sign out of all active sessions on Facebook, Twitter and Gmail, for example.
- Remote wipe. If your device was stolen, lost or confiscated you might be able to remotely control your mobile device by sending some commands to wipe the data or locate its position, but such tools aren't always guaranteed to work and they depend on several variables such as the data connection on the mobile, GPS, network strength and whether the device is on. This capability is usually a feature of your device's operating system so look for setup and execution instructions from Android or iOS.

Where to find more help

- Learn about encrypting your iPhone.
- Read the basic Android security setup guide.
- Learn about Android apps such as Signal, Orbot and Orweb from The Guardian Project.



Kit#6

MY BLOG OR WEBSITE HAS BEEN HACKED OR ATTACKED

I WENT ONLINE TODAY AND DISCOVERED THAT OUR WEBSITE IS NO LONGER ACCESSIBLE! HOW CAN I GET OUR SITE BACK UP AND PROTECT IT FROM FUTURE ATTACKS?

YOUR ORGANISATION'S WEBSITE HAS UNDERGONE VANDALISM OR IS NOT ACCESSIBLE ANYMORE, OR YOU ARE SIMPLY WORRIED THAT BECAUSE OF AN UPCOMING CAMPAIGN OR ACTION, YOUR SITE WILL BE A TARGET OF REACTIONARY FORCES, EITHER STATE-SPONSORED OR AMATEUR. YOU NEED TO GET BACK OR KEEP CONTROL OVER YOUR BLOG OR WEBSITE AND ITS INFORMATION.

WHAT YOU SHOULD DO

You might need to reach out to your website developer or a technical expert if you're unsure why your website is inaccessible. You could start by opening a support ticket with your hosting provider or sending an email to someone at an organisation like APC who can help determine exactly what has happened. If you're concerned your site is being censored, use a web proxy or service like GreatFire (if censored in China) to verify where your site is (in) accessible. Once you figure out the problem, you can act.

If your site was vandalised, it's likely because someone gained access as a privileged user through a weakness in your site's security. You should:

- Log in and revoke access from untrusted users.

    1. If your log-in doesn't work and your site is hosted with a third-party service, read Kit #1. My email, Facebook or Twitter account was hijacked, and follow similar steps to try to regain access to your site's administration interface.

    2. If your log-in doesn't work and you host your own site, you should be able to regain access at the database/server level, depending on your site's platform. Because each platform and server set-up are so specific, you may need to turn to a technologist or support person at your web

host for help.

3. Restore the site with a recent backup.

4. Without a backup or tracked content revision of any kind, you may face data loss.

- If your site was taken offline by your provider, it may be because of government or other legal requests. Often your provider will notify you. You should:

  1. Comply with the content take-down request so that your full site can be restored.

  2. Appeal to your provider, explaining the political context of your work and asking them to restore your site. Challenge the request's legality (it's surprising how often these requests are illegitimate). You could employ the help of a lawyer.

  3. Move your site to a provider who is better aligned with the politics of your organisation and won't comply with such requests. If you don't already have access to a recent backup of the site files and database, you might have to go back to your existing provider and request a copy.

  4. If your domain name was hijacked through a hack or because your ownership lapsed, you should immediately begin an appeal process with the domain registrar to restore your access. These appeals can be followed through all the way up to domain-name governance according to ICANN's dispute resolution policies.

- If your site is under DDoS attack you should reach out to your provider, who has likely already taken steps to mitigate the enormous amount of traffic coming to your site. Your provider can give you details of the attack that can help you and a technologist determine the best course of action. If waiting for the attack to subside is not an option, you should:

1. Move your site or upload the most recent backup to a new server.

2. Change the DNS TTL ("time to live") setting to something short so that when you move the website, zone record changes propagate fast.

3. Get help putting the restored site behind DDoS protection such as Varnish (software) or Deflect.

4. If your site is being censored there may be no quick fix to restore access by users who are behind the filter or firewall. You should take some or all of these courses of action:

1. Set up mirrors. Mirroring a website means having copies of your website on different servers. Mirrors require some set-up and are usually precautionary measures in cases such as technical problems, censorship or targeted hacking.

2. Raise awareness about the censorship. Use social media to alert your users and freedom of expression activists to the site's censorship and give them a new URL with which they can still access the site.

3. Engage in campaigning and policy advocacy to lift the censorship.

4. Educate your users about circumventing censorship. Kit #12. I need to access a blocked website anonymously.

- You or a technical expert needs to inspect the server log files to see what has happened, otherwise the adversary may have uploaded and hidden a malicious "shell" file on your website, dumped your database, or created a system user on your server. Simply recovering the website is not enough if the server has been compromised.

How to prevent future problems

- Backup the site files and database. Frequent backup is an essential practice. If you are running a blog on a third-party platform such as WordPress or Blogspot (Blogger) you can export the whole blog to your computer any time. Do this monthly, at a minimum.
- If you host your own site, look to your web host to provide you with redundancy and backup options. How do they backup your site in case their infrastructure fails? How do you gain access to these backups? Does access to an automatic backup feature add extra cost to your monthly or yearly subs cription?
- Secure the website's platform. If you are hosting your own website, you need to ensure that your website's code is always up to date with the latest security releases. Once security vulnerabilities are known and updates are released for them, hackers also learn about these vulnerabilities and can exploit them to gain access to your website.

- Secure your server. If you are hosting your own website on a server, it is important to spend some time reading the security features and policies of the hosting company, especially when it comes to take-down requests and data storage policies. There are several APC member organisations that take a political approach to providing technical services to activists, including Colnodo (Colombia), GreenNet (UK), Jinbonet (South Korea), May First (USA), and Pangea (Spain).

- Protect your DNS. Domain registrars are commercial providers who, depending on their commitment to user privacy and data control, can be a weak point in your infrastructure. The government or another adversary could freeze your DNS. Or your control of your domain name could be a target for hackers. Make sure to use a trusted registrar like EasyDNS, keep your account secure and always renew on time.

- Secure traffic to the site. It is extremely important to enable HTTPS access to your site, at least for when you log in to the site as an administrator, but also for your users' privacy. TSL is an encryption protocol that establishes a secure channel between your computer and the server hosting your email or the website you're visiting. The secure channel requires you to validate the site's trustworthiness with a TSL certificate that you purchase from a certificate authority. Several certificate authorities like StartSSL.com issue free certificates to non-profits.

- Secure log-ins. Enable two-step verification for administrator or user access to your site. Configure the site to keep logs and monitor them for unusual activity by user accounts. Delete, ban or block user accounts and IP addresses that you don't trust.

- Enable log-in recovery. Set up all recovery options for yourself such as a secondary email address. As opposed to a corporate blogging platform, if you are hosting your own website then you will have more options such as adding a mobile number, recovery questions or a special PIN code.

- Prevent DDoS attacks. The best way to ensure a DDoS attack doesn't keep your website and potentially your other web

services like email from going dark, is prevention. Deflect is a free/libre and open source software tool and gratis service for progressive groups and organisations. You can sign up easily and at no cost, while maintaining control and access to your web stats.

Where to find more help

- Manage backups.
- Export your WordPress site.
- Export your Blogspot site.
- Get a free TSL certificate and learn about TSL from the project Let's Encrypt!.
- Learn about DDoS protection with Deflect.

Kit#7

I NEED TO USE A COMPUTER WITHOUT LEAVING A TRACE

I HAVE A PARTICULAR TASK THAT REQUIRES ME TO GO ONLINE IN A COMPLETELY DISCREET MANNER. WHAT CAN I DO TO HIDE MY ACTIVITY AND MY IDENTITY?

YOU MIGHT WANT TO VISIT SOME WEBSITES, CONDUCT RESEARCH, OR PUBLISH OR SEND INFORMATION ONLINE. WHETHER YOU USE YOUR OWN OR SOMEONE ELSE'S COMPUTER, YOUR ACTIONS PERFORMED ON THE COMPUTER AND THE ONLINE TRAFFIC YOU GENERATE COULD EXPOSE YOUR ACTIVITY AND YOUR IDENTITY. YOU NEED TO WORK WITHOUT LEAVING A TRACE AND IN A SECURE MANNER

What you should do

Even if you are very concerned about your anonymity, in some cases you might have to use a computer that is not yours and you want to do it in a safe manner without leaving any traces. You might also be using your personal laptop but you still prefer to avoid leaving traces of your activity.

Tails is a live operating system (OS) that you can use on almost any computer by booting (starting the computer) from a DVD, USB drive or SD card. A live operating system is a full operating system that uses the computer's hardware but not its software or drive storage. Tails is a special live OS that aims to preserve your privacy and anonymity by never storing data about your activity and forcing all internet connections through the Tor network. Tails comes with a set of programmes for web browsing, encryption, chatting and editing documents that are privacy-respecting by design.

The Tails website contains detailed and accessible documentation about how to download, verify and install Tails onto a DVD, USB drive or SD card that you can then use anywhere.

Keep in mind

If you are working in a sensitive environment, and you are in a public space, you might need to be aware of any CCTV/surveillance around you. That applies, for example, to using a computer in a cyber café or a library.

Always keep Tails up to date. The system should notify you if there are new updates, but it's advised to check their website frequently for announcements.

Where to find more help

- Learn about first steps with Tails.
- Learn about installing Tails onto a USB stick.
- Learn about Tails features and included software.
- Read an overview of Tor.

Kit#8

SOMEONE MONITORS EVERYTHING I DO ON MY COMPUTER

I THINK SOMEONE KNOWS WHAT I AM DOING ON MY COMPUTER BUT I DON'T KNOW HOW IT IS POSSIBLE. WHAT CAN I DO TO PROTECT MY PRIVACY?

YOU FOUND OUT THAT YOUR COMMUNICATION IS LEAKING TO PEOPLE WHO SHOULD NOT SEE IT. YOU NOTICED THAT SOME PEOPLE KNOW ABOUT PRIVATE DOCUMENTS YOU HAVE WRITTEN ON YOUR COMPUTER. YOU THINK SOMEONE HAS ACCESS TO THE CONTENT OF YOUR COMPUTER AND YOU DO NOT KNOW HOW IT IS POSSIBLE.

Your computer could be infected by a virus, trojan, spyware or other malicious software (malware) running without your knowledge. You may have downloaded a file, visited a web page, clicked on a link, used an infected USB drive, or opened an email that led to the malware. This might have given the malware's creator the control over your computer. Hardware such as a keylogger may be embedded and disguised within your device, which allows someone to capture your activity.

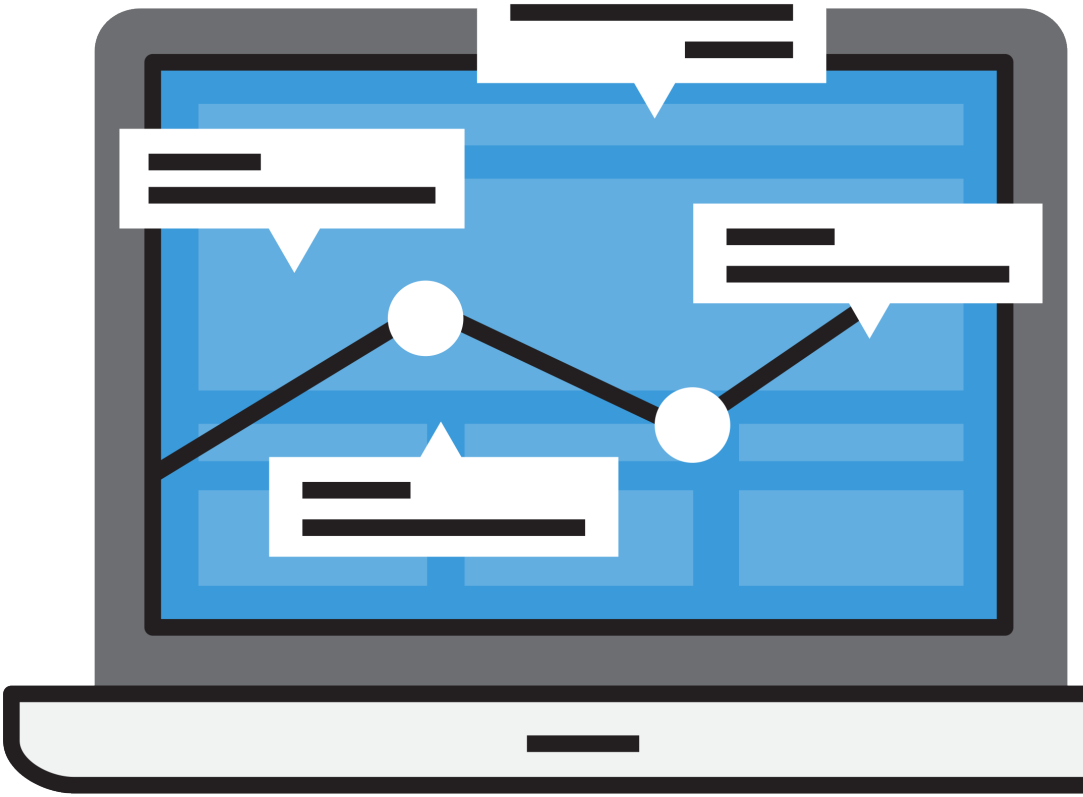
Untargetted malware can be used for advertising, theft, fraud, spamming, "psiphoning" off computational power, or pointless malice. However, you may also suspect that you have become a target of law enforcement, your employer, someone you live with or your partner, for example.

What you should do

First, make sure this is not a human error, which means that the information is not being disclosed by some other people whom you trust and with whom you share it. If you are positive it is not a human error, then:

Ask, "Who can have physical access to my device at home, work or elsewhere?" Protect the log-in screen with a passphrase or change your passphrase to a stronger one.

If you are using Wi-Fi to connect to the internet, make sure that the Wi-Fi connection is passphraseword-protected and not open to



anyone you don't know and trust.

Ensure that no one but you has access to your online accounts. See Kit #1. My email, Facebook or Twitter account was hijacked.

Make sure your anti-virus software is installed and properly updated. Do a full scan of your computer.

Make sure you have a working firewall in place.

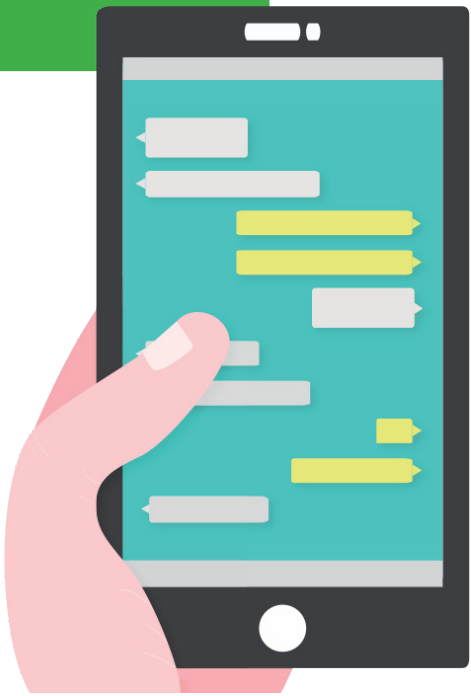
Do all you can to secure your communications such as always browsing with HTTPS and encrypting all of your emails.

If you suspect that someone can see documents that you do not send over the internet or other things you do/have on your computer, your computer is probably "hijacked" by someone who has full, remote access to your computer either via malicious software or a keylogger. At this extreme stage it is advised to stop using the infected computer and disconnect it from the internet and any media. Carefully migrate essential files (not your entire drive) to a brand new device with a fresh operating system.

Where to find more help

- Secure your own Wi-Fi network.
- Use anti-virus software.
- Use anti-spyware software.
- Use a firewall.
- Securely browse the web with HTTPS–Everywhere.
- Change the security settings of your Gmail account.

Kit#9



I NEED TO CHAT IN A SECURE MANNER

I NEED TO CHAT WITH SOMEONE WHILE NO ONE ELSE IS LISTENING OR MONITORING OUR CONVERSATION. I CAN ONLY SHARE INFORMATION WITH THEM IF I KNOW THAT NO ONE ELSE WILL FIND IT OUT.

YOU ARE PREPARING AN ONLINE MEETING WITH ONE OR MORE COLLEAGUES AND YOU NEED TO SHARE CONFIDENTIAL INFORMATION WITH THEM. YOU NEED TO BE SURE THAT NO ONE CAN ACTIVELY MONITOR OR PASSIVELY COLLECT THE CONTENT OR ANY OTHER INFORMATION RELATED TO YOUR CONVERSATION.

Chatting tools are like the rest of the communication tools we use on daily basis: they could be monitored and have different levels of risks. When using chatting applications, be aware that they are either:

- End-to-end encrypted, which means that only you and the receiver can read the messages and no one else can.
- Encrypted to the server, which means your connections to the service provider are secure but requires you to trust your service provider (Microsoft in the case of Skype, Google in the case of Hangouts).
- Not encrypted at all, which means that anyone watching your communication could see your messages in plain text.

You must also trust the application. The only way to judge the security of an application and verify its privacy claims is to review its code in an open and transparent manner. Applications that provide their code for community review, and comply with several other criteria, are classified as free/libre and open source software (FLOSS). FLOSS applications are generally trustworthy.

Most popular applications don't prioritise user privacy and security. While your contacts may be using these popular services, we recommend that you stop using Viber, WhatsApp, Facebook Chat, Google Hangouts and Telegram because they don't implement security measures transparently.

What you should do

Learn about the many options for secure chat applications from the list of resources below and choose the best solution for your needs. We recommend FLOSS applications that use end-to-end encryption.

Start by learning which applications and tools implement secure protocols and which do not from the Secure Messaging Scorecard.

Where to find more help

- Use Signal for Android.
- Use Signal for iPhone.
- Use Jitsi (xmpp) or Jitsi Meet.
- Use Cryptocat in your web browser (Note from the developer, 19 February 2016: I am temporarily suspending the Cryptocat service until the complete software rewrite that I'm working on is released. I promise you that this suspension is strictly temporary.).

I NEED TO SEND EMAILS THAT CANNOT BE TRACKED BACK TO MET

I HAVE TO SEND EMAILS THAT, IF LEAKED, WOULD PUT ME OR MY COLLEAGUES AT RISK. HOW DO I SEND EMAILS THAT CANNOT BE TRACKED BACK TO ME?

YOU NEED TO SEND ANONYMOUS MESSAGES THAT YOU DON'T WANT ANYONE TO BE ABLE TO LINK BACK TO YOU. YOU MIGHT NEED TO WORK ANONYMOUSLY. YOU NEED TO TAKE PRECAUTIONS NOT TO EXPOSE YOUR AND OTHERS' IDENTITIES IN CASE SOME MESSAGES ARE INTERCEPTED OR ONE OF YOUR COLLEAGUES' COMPUTERS IS CONFISCATED.

What you should do

There are many points along the message's way from you to the recipient that can expose your identity. Nevertheless, you can take some of the following precautions that make it very difficult to link the message back to you:

- Create an email account with a service that is openly committed to user privacy and does not store or disclose user or message details. Every email message travels through the internet with metadata to ensure its recipient receives it. Think of stamps of all the post offices through which a package travels. Some email providers deliberately delete message details about previous servers through which a given email has travelled. This is what you need. If your email provider is based in London, all that can be found from your message about your real physical location is that your messages travelled through London. Note that this is effective only if the email is intercepted after it reaches your email provider. Riseup.net is such an email provider.

- If your use is temporary, use a web-based anonymous remailer service but note that you should not have extended correspondence through an anonymous remailer. In fact, not all of them will even deliver messages back to you. Additionally note that even if you trust the service, you should access the remailer website with Tor Browser to anonymise your IP address.

- With an email client configured to use an email address that cannot be linked to your identity, use The Onion Router (Tor) application. If properly configured, it will pass your email communication through a chain of anonymising servers that will obfuscate the message's route between you and your service provider.
- Use an email client as a portable application to send and receive your emails from public computers. For example, you could install the email client Thunderbird on a USB drive. You can then write messages on your (or any other) computer, go to a public computer, plug your memory stick into a computer, open Thunderbird, and send your messages. Sending messages from a public computer has the advantage that the computer and IP address are not associated with you. It is advised in case of using public computers to use VPN or Tor before starting your web activity and communication. In all cases there are physical clues that can identify you even with a public computer such as CCTV footage or computer user logs at libraries.

Keep in mind

While using public computers can be useful to maintain your annonymity, you have generally no control over what kind of software, malware, keyloggers or remote administration applications run on such a computer. Have these possible threats in mind when using a public computer.

Where to find more help

- Read about Riseup's secure email and internet services.
- Learn about using the Tor Browser.
- Learn about Portable Thunderbird
- Tips on responding to suspected email surveillance.

Kit#11

I NEED TO SEND EMAILS THAT ONLY THE RECIPIENT CAN READ

HOW CAN I BE SURE THAT THE CONTENTS OF MY EMAILS ARE COMPLETELY CONFIDENTIAL?

YOU NEED TO SEND SENSITIVE INFORMATION TO YOUR COLLEAGUES OR FRIENDS, BUT YOU'VE HEARD THAT ONCE MESSAGES LEAVE YOUR COMPUTER THEY TRAVEL THROUGH A STRANGE NO-MAN'S-LAND WHERE YOU LOSE CONTROL OVER WHO MIGHT SEE YOUR COMMUNICATION. YOU HAVE A SUSPICION THAT SOMEONE IS EAVESDROPPING. IF THIS HAPPENS WHEN YOU'RE SENDING SENSITIVE INFORMATION, YOU AND THE PEOPLE YOU WRITE TO MIGHT GET INTO SERIOUS TROUBLE.

Once your email or chat message leaves your computer, it travels through many nodes or points along the way such as routers, servers and middle boxes where it can be intercepted, read and stored for future access. The internet's underlying infrastructure was built for openness and interoperability and therefore unfortunately does not guarantee privacy.

What you should do

You must make careful decisions about your email provider and the software you use if you want to make sure that your messages can't be read by anyone other than the intended recipient.

Encrypt your communication. This means that if an unauthorised person intercepts your messages, they'll see a sequence of letters and numbers that won't make any sense to them. To do so:

1. Rather than using your email provider's website for sending and receiving emails (using so-called webmail), you should switch to managing your messages in an encryption-enabled email client (application). This will store your messages on your computer, and will do so exclusively if you configure the client to use the POP protocol instead of IMAP. A recommendable and well-supported email application is

Mozilla Thunderbird.

2. If you install Thunderbird, you'll need to add the Enigmail extension to manage email encryption using OpenPGP.

3. 3Create an encryption key pair, which is both a private key that you never share with anyone and a public key that you will give to other people to send messages to you. You can have more than one key for several reasons and uses. Once you get started and are familiar with the process, you will find it easy. You just need to practise a little bit. Follow the links below for instructions on how to create and use your OpenPGP key.

4. 4Configure your email client to be able to properly encrypt and decrypt email messages, using the application that is most convenient for you. Links below will lead you to instructions on how to configure and use encryption in a Thunderbird email client.

5. 5Get the public keys of your correspondents. Encrypted communication is end-to-end, which means both sender and receiver have to be using the same encryption protocol. You can use OpenPGP with Thunderbird/Enigmail to communicate with someone who uses OpenPGP through another client such as Claws Mail, or through the K9+AGP mail client and OpenPGP manager on Android.

Keep in mind

- The message body and attachments of an email message can be encrypted. However, the other information that travels along with every email (including the subject, addressees, sender, dates and servers through which the message travels) is not encrypted.

- The email you encrypt can be decrypted only if the addressee has her/his own private OpenPGP key and knows the passphrase that allows her/him to use it. Consequently, anyone in control of her/his private OpenPGP key could read the message you sent.

- Encryption is illegal in some countries. Check whether this is the case in your country before you start using encryption, just to be aware.

Where to find more help

- Read introductions to public key cryptography and to mail encryption with OpenPGP.
- Learn more about email encryption.
- Learn more about how to use OpenPGP in Thunderbird with Enigmail.
- Tips on responding to suspected email surveillance.
- Learn about encryption-related laws in each country.

Kit#12

I NEED TO ACCESS A BLOCKED WEBSITE ANONYMOUSLY

I NEED TO CHECK OUT A WEBSITE THAT IS BLOCKED OR WHOSE CONTENT IS NOT LEGAL IN MY COUNTRY. IS THERE A WAY TO DO THIS WITHOUT DRAWING ATTENTION TO MYSELF?

YOU LIVE IN A COUNTRY THAT CENSORS CERTAIN WEBSITES AND ONLINE SERVICES, PREVENTING YOU FROM READING THEM WHEN YOU TYPE THEIR URL INTO YOUR BROWSER. IN OTHER CASES, WEBSITES ARE ACCESSIBLE BUT THEIR CONTENT IS ILLEGAL WHERE YOU LIVE. YOU MIGHT FACE FINES OR IMPRISONMENT IF YOU WERE FOUND TO HAVE ACCESSED THESE WEBSITES OR DOWNLOADED PARTICULAR CONTENT. OR YOU SIMPLY WANT TO VISIT A WEBSITE WITHOUT LEAVING A TRACE OR ALLOWING OTHERS "WATCHING" THE TRAFFIC TO KNOW.

What you should do

There are three options to access content that is censored, unavailable in your location or simply taboo. They differ in terms of the security and anonymity they provide to you, but also in terms of ease of use.

- The first is to use a virtual private network (VPN). VPNs enable a properly configured device to send and receive all data through another computer network. For example, if you are using a VPN to access https://apc.org, your computer first connects to the VPN, which then connects to https://apc.org on your behalf and sends back the result. When you connect to the internet through a VPN all your traffic and activities must be encrypted, so ensure that your VPN provider is implementing security properly. This encrypted "tunnel" protects you from surveillance and allows you to bypass censorship.

- With an onion routing network such as Tor, your traffic is bounced through at least three other anonymising nodes or points to your requested destination and back, providing

multiple layers of anonymity that effectively obfuscate your identity. The Tor Browser is an easy application to download and install and requires little to no configuration. Tor, however, is not secure. Unless you use HTTPS – and you should always use HTTPS – and email encryption, any node or point in the Tor network can see, store and disclose the full details of your communication. Tor is also notoriously slow.

- A web proxy is perhaps the easiest tool for quick access to a blocked website. Similar to a VPN, you simply navigate to a proxy website and type in the URL that you wish to access. The proxy (an intermediary server) fetches the site for you and returns it, often with ads and other unwanted code embedded. It is not recommended to access websites regularly using a web proxy. And never use your regular browser to access a site with a proxy since your web browser contains data about you, called a fingerprint, such as your history and session cookies.

Keep in mind

- Although your traffic is secured between you and the VPN, the VPN provider must be trusted because they can see, store and disclose the details of your traffic.
- While Tor provides anonymity, it does not secure the content of your communications from eventual eavesdroppers.
- Do not trust a VPN or the Tor network with your communications. Always use HTTPS when browsing and OpenPGP encryption when sending emails while connected to a VPN or Tor. If you can't use HTTPS to visit some sensitive websites or don't have OpenPGP encryption set up for your email client, then you shouldn't use Tor or an untrusted VPN, period.
- Whatever precautions you take to anonymously browse blocked or illegal content, your browser is configured by default to remember your browsing history. So in the case that your computer is seized or hacked, the intruder can easily check which websites you've visited. If this is a concern for

you, configure your browser in such way that it doesn't record browsing history.

Where to find more help

- Learn about how to bypass censorship.
- Learn about extending your Firefox browser security.
- Learn about Tor.
- See an interactive illustration of how HTTPS and Tor make you both secure and anonymous.
- Learn about Riseup VPN and about TunnelBear VPN.
- Assess whether using a VPN will give you the protection you need.
- Disable browsing history in Mozilla Firefox.
- Temporarily disable browsing history in Chrome.

Kit#13

I AM FACING ONLINE ABUSE

SOMEONE OR MANY PEOPLE ARE STALKING AND BLACKMAILING ME, AND SENDING ME DEATH AND RAPE THREATS. I FEEL UNSAFE BOTH ONLINE AND OFFLINE. PLEASE HELP!

ONLINE VIOLENCE IS VIOLENCE AND THE STRATEGIES TO COMBAT TECHNOLOGY-ENABLED VIOLENCE ARE AS DIVERSE AS THE TACTICS BEING USED TO SCARE AND SILENCE YOU. YOU NEED TO PROTECT YOURSELF AND YOUR ASSOCIATES FROM THE ONLINE ABUSE AS WELL AS, IN SOME CASES, WORK WITH LOCAL GROUPS OR AUTHORITIES TO DEAL WITH AND REPORT ON OFFLINE THREATS AGAINST YOU

Violence against women (VAW) such as sexual harassment, domestic violence and sexual violence is extended, perpetrated and exacerbated in various ways online, but ICTs can be helpful for women to find help, connect with others and take action. With technology-related violence against women, be it cyber stalking, blackmail or hate speech, every situation is different. You may feel helpless, but you can take action.

Cyber stalking is a technologically enabled attack on a person for reasons of anger, revenge or control. It is much more likely that women will experience stalking than men, and more often this is done by an intimate partner. Sometimes this type of violence may also involve physical assault.

Cyber stalking includes harassment, humiliation and embarrassment of the person targeted; harassing family, friends and employers to isolate the person; tactics to make the target fearful; taking on the identity of the other person; constant surveillance and monitoring of activities and location (e.g. using Facebook notifications to find out where the person is going, using spyware, activating GPS).

What makes cyber stalking difficult to address are factors such as stalker anonymity; law enforcement's assumption that a stalker located far away will not travel to follow up on threats; and the stalker encouraging online friends to participate in the harassment, thus increasing the person's distress. Further, cyber stalking is not

recognised in law in many countries, which means survivors of cyberstalking have no legal recourse.

Blackmail is the act of threatening to reveal damaging information about a person to the public, family or associates unless that person buys the blackmailer's silence. The damage can be in the form of harm to reputation, well-being, employment, or in some contexts, to physical safety. Online sexualised blackmail is where blackmailers may steal, fake or use private and often sexualised images or correspondence and threaten to publish or distribute them without consent. The price demanded may be money or physical and emotional control of the person being blackmailed. In the case of what is known as "revenge porn" (where private sexualised images or videos are published online without consent but without financial motive), the price seems to be pure humiliation and degradation of women. It can happen in many ways, from government surveillance for power, to manipulation of photos to humiliate, to images stolen for financial gain, to videos taken without consent, to partner surveillance, to images taken of violence and kept as a way to control someone.

Remember that blackmail is unacceptable and you have rights (PDF): a right to freedom of expression, a right to privacy and freedom from defamation, a right to freedom from violence and a right to protect your artistic work.

What you should do

Here are some strategies you can use to respond and protect yourself. However, this is not an exhaustive list. Do remember that it is not your fault and we recommend talking to trusted people in your life about this for help.

- Install a firewall, secure your Wi-Fi and turn off Bluetooth. Wi-Fi hotspots and Bluetooth connections can reveal your location and make it easier for people to hack your phone. When using public Wi-Fi, your line of defence is your firewall. A firewall will defend you from untrusted connections from the internet and local networks, which could let hackers and viruses access your computer. A firewall is the first programme on a computer

that sees incoming data from the internet and the last programme to handle outgoing information.

1. For your home connection, make sure the connection is protected by WPA2 security. WEP (another encryption standard used for securing Wi-Fi networks) is child's play for hackers.

2. Choose a very strong password for the Wi-Fi connection.

3. Install a firewall.

4. Switch off your Bluetooth connection.

- Get an alternative SIM card. If a stalker can obtain your mobile number, they may harass you through SMS messages and phone calls. They may use it in combination with GPS to reveal that they know your location. Consider an alternate SIM card for private calls.

  1. Turn your phone off, switch out SIM cards and restart your phone.

  2. Don't forget to switch out the private card when you're finished.

  3. Keep the private SIM in a safe place.

- Disable GPS on your phone. GPS may tell you what coffee shops are nearby, but it can also let others know where you are. The majority of smartphones have GPS chips that can geo-locate the phone in seconds.

  1. Only enable GPS settings when you need them.

  2. Turn them off by navigating to Settings > Privacy > Location.

- Disable the GPS on your mobile camera. Photos have information embedded in their properties that include when and where you took them (if your camera or phone have a GPS). It can also be possible to decipher the location based on what's in the image. This geographic info can be embedded

in photos pinpointing exactly when and where the photo was taken. Together with the content, it can be easy to discern where you live, work or play.

1. On an iPhone, go to Settings > Privacy > Location, and disable the option of “Camera”.

2. On Android, go to the camera application. Under settings, turn “Location Tag” to “Off”.

- Protect your phone with a passphrase. If your phone is not password protected, anyone who gets their hands on it can access your information. Password hacking is common, and the more a stalker knows about you, the more likely they are to guess your passwords. Passphrase protection will keep your data safer if you lose your phone or someone tries to use it without your permission.

  1. For more information refer to Kit #3: I need to keep my passphrases safe.

  2. Reset your passphrases regularly.

- Protect your computer and phone from spyware and malware. Malicious applications may contain spyware. The more capabilities your smartphone has, like GPS, the more those extras can be used to spy on you. Malware and spyware are used to track, record and watch what you do online.

  1. Install trusted anti-malware such as Spybot.

- Maintain privacy on social media. It’s very easy to glean information about where you live, the places you visit regularly and the people you care about from posts and pictures. Your friends might also unintentionally reveal information about you.

  1. Create a different email account for site registration. This will help avoid spam, and your personal email won’t be revealed if the online service doesn’t have gaood privacy practices.

  2. Leave optional fields blank. When registering online, only

fill in the required fields and leave certain identifying information such as birthdate blank.

3. Use a profile photo that doesn't identify you. Choosing images that also protect your location can keep you from being recognised or found.

4. Choose a screen name that isn't personal. Many people have screen names that do not give away identifying characteristics. You might want to consider a user name that is gender-neutral.

5. Check your privacy settings. Services such as Facebook change their privacy policy all the time, so check in regularly to make sure you are sharing the information you want to share only with people you trust. Some sites have options for you to test how your profile is being viewed by others. Learn more about social networking privacy settings.

6. Refer to Kit #1. My email, Facebook or Twitter account was hijacked.

- Use a secure chat option that is not incorporated into mainstream social networking services, preferably one that encrypts conversations. Many social networking sites offer chat options. This is one of the most insecure ways to communicate online. Online acquaintances can stalk you in chatrooms.

  1. Use Jitsi instead of Skype because it is more trusted.

  2. For your mobile phone consider Signal or Telegram. Be aware that both you and the person you are talking to should be using the same encrypted service.

  3. Refer to Kit #9. I need to chat in a secure manner.

- Switch off your webcam and place a sticker or piece of paper over the camera on your laptop or mobile phone. Stalkers use spyware to access webcams and film people without their knowledge or consent.

You can also denounce stalkers and seek redress. Here are some suggestions how you can do this.

Where to find more help

- Take Back the Tech (TBTT) Safety Toolkit
- Learn about Cyber stalking, Blackmail and Hate Speech
- How to talk to survivors
- What privacy and anonymity have to do with tech-related VAW
- What data storage has to do with tech-related VAW
- Zen and the art of making tech work for you