Digital Security Guide for Journalists[1]

October 2017

1. Introduction

The Internet and other digital means of communication provide vastly enhanced access to information and serve as one of the primary vehicles for enjoying freedom of expression. Similarly, for the practice of journalism, the benefits of the Internet and digital communications more broadly are enormous. The Internet has dramatically increased the resources available to journalists for research, the means by which they can contact and communicate with sources, and the avenues to distribute content and engage in discussion with their audiences.

At the same time, journalists have faced, and will continue to face, a number of threats in the online world. The digitalisation of communications has brought with it new threats for journalists, such as massively increased powers and means of surveillance (by both State and non-State actors). This can be done, among other things, through location tracking, data mining and/or the interception of communications. This has proven to be a particular challenge in the content of protecting the identity of journalists' confidential sources of information.

Another risk is growing levels of online harassment, especially on social media platforms. Online harassment has no precise definition, but has been characterised by the Pew Research Center as having one of the following six elements: being called offensive names, being subjected to intentional attempts to embarrass you, being physically threatened, being stalked, being harassed for a sustained period and being sexually harassed.[2]

---

[1] Drafted by Portia Karegeya, Legal Officer, Centre for Law and Democracy.

[2] Maeve Duncan, *Online Harassment,* Pew Reaserch Center, 22 October 2014, p. 5. Available at: http://www.pewinternet.org/2014/10/22/part-1-experiencing-online-harassment/#demographics-of-online-harassment.

Online harassment has a particularly gendered aspect as women in general tend to face greater levels of harassment online, often of a violent and sexual nature. A 2014 Pew Research Centre survey of online harassment found that young women were more likely than others to experience the more severe forms of harassment, in particular online stalking and sexual harassment, as well as physical threats and sustained harassment.[3] Another iteration of this survey in 2017, came up with similar results: while men are somewhat more likely to be harassed online than women, women are far more likely to be the targets of sexual harassment online.[4]

Studies focusing on journalists have also found that intimidation is experienced at roughly equally rates by females and males except when it come to sexual harassment which is experienced more often by females.[5] The Representative on Freedom of the Media of the Organization for Security and Co-operation in Europe (OSCE) has echoed this sentiment reporting that "female journalists, bloggers and other media actors are disproportionally experiencing gender-related threats, harassment and intimidation on the Internet which has a direct impact on their safety and future online activities."[6] In Kenya, it was found that this could result, in extreme cases, in women journalists ceasing to work as journalists for a period of time or even withdrawing entirely from the Internet.[7]

To address these problems, journalists, of all genders, should take steps to protect themselves. This is especially the case given that both digital attacks themselves and the entities that carry them out can be difficult to identify without high levels of technical expertise.[8] Ultimately, there is no way to guarantee absolute protection from a truly dedicated attacker – and female journalists may have to take extra steps to protect themselves from certain forms of online harassment – but good digital security practice can make a huge difference. This guide aims to provide journalists, in an accessible format, with the tools they need to protect their own digital security, as well as that of their colleagues and sources.

---

[3] *Ibid.*

[4] Maeve Duncan, *Online Harassment,* Pew Reaserch Center, 11 July 2017. Available at: http://www.pewresearch.org/fact-tank/2017/07/11/key-takeaways-online-harassment/.

[5] Elana Newman, *et al.*, "Online abuse of women journalists: Towards an Evidence-based Approach to Prevention and Intervention" in OSCE, Representative on Freedom of the Media, *New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists,* 2016, p. 49. Available at: http://www.osce.org/fom/220411?download=true.

[6] Recommendations following the Expert Meeting New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists, 17 September 2015, in OSCE, Representative on Freedom of the Media, *New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists,* 2016, p. 5. Available at: http://www.osce.org/fom/220411?download=true.

[7] ARTICLE 19 and AMWIK, *Women Journalist's Digital Security* [sic], May 2016, p. 4. Available at: https://www.article19.org/data/files/medialibrary/38757/Women-Journalist's-Digital-Security-Kenya-2016.pdf.

[8] Jennifer R. Henrichsen, *et al.*, *Building Digital Safety for Journalism: A survey of selected issues*, UNESCO Series on Internet Freedom, 2015, p. 14. Available at: http://unesdoc.unesco.org/images/0023/002323/232358e.pdf.

2. Threat Modelling and Risk Assessment

As a first step in ensuring digital security, it is important for journalists and news organisations to engage in threat modelling and risk assessment of potential security threats. The objective should be to avoid over- or under-estimating threats and, instead, to identify properly the risks of surveillance, harassment and the possible capture of one's digital activities, and to take appropriate steps to guard against them.[9]

The Electronic Frontier Foundation (EFF) recommends that people ask the following five questions when creating a threat model:[10]

1. *What do I want to protect?*

   Consider the information and assets you have which are of value and need protecting. This may include your location, contact lists, devices, and files and documents. Also, list and consider where and how this information is stored, who has access to it and the ways access to the information could be limited.

2. *Who do I want to protect it from?*

   Thoroughly consider which persons or entities may want to target you or your information. This may include individuals, corporations or State actors.

3. *How bad are the consequences if I fail?*

   Consider what the goals of any digital attackers may be. For example, if you are reporting a story for which you have obtained a video, someone may want to delete that video from your devices. That might be more or less important to the success of your story.

4. *How likely is it that I will need to protect it?*

   Consider the likelihood or risk of an attack actually occurring. For example, even though a phone company would normally have access to your phone records the likelihood that they would use those records to harm you is limited. In other words, consider which threats are more likely to happen and which threats are of low probability.

[9] Della Kilroy, The Storyful Podcast: Digital Security – How Journalists and Activists Can Be Protected Online, Storyful, 31 January 2017. Available at: https://storyful.com/blog/2017/01/31/the-storyful-podcast-digital-security-how-journalists-and-activists-can-be-protected-online/.
[10] EFF, Surveillance Self-defense: Assessing Your Risks. Available at: https://ssd.eff.org/en/module/assessing-your-risks.

5. *How much trouble am I willing to go through to try to prevent potential consequences?*

   Consider the options you have to help guard against digital attacks and any technical, financial and social constraints that you may face in terms of implementing those options. Some threats may just be too difficult to guard against.

   A consideration here will be the capabilities of potential adversaries. Individual hackers, private companies and public actors may all have varying levels of interest in and capacity to compromise your data. The State normally has the greatest capabilities of all.

Threat modelling is not a one-time process but should be practised if and when the context and situation in which the journalist finds him- or herself changes.[11]

3. Passwords

Many of our digital accounts and services contain a great deal of personal information and data that may be vulnerable. Passwords are an important way of locking these services to protect them against access by outsiders.

a) Strong Passwords

It is very important to create strong passwords. An unfortunate challenge here is that while passwords may be difficult for a human to remember, they can be very easy for a computer to crack. Three recommended rules of thumb are:

1. Use a mixture of random letters, numbers and special characters.
2. The longer the better, preferably 12 characters or more.
3. Refrain from using the same password for multiple sites/services.

When creating passwords, the use of a *passphrase* made up of three or more random words is recommended. These have the advantage of being easier to recall and difficult to hack due to their length (for example, cowplantfridgeshoes).

To increase the level of randomness to your passphrase, you can also use what is known as the Diceware method. This is a method for picking passphrases that uses dice to select words at random from a list called the Diceware Word List.[12] Each word on the list corresponds to a five-digit number made up of digits

[11] *Ibid.*
[12] Dice-Indexed Passphrase Word List. Available at: http://world.std.com/~reinhold/dicewarewordlist.pdf

between one and six. In order to engage in this method of choosing a passphrase you need one or more dice (simple dice found in board games or sold separately at toy or hobby stores will do). Either roll one die five times, roll five dice once, or any other combination you desire. Once you have a five-digit number, look it up on the Diceware word list and select the corresponding word as part of your passphrase. Repeat the process to select as many words as you wish to put in your passphrase, the longer the better.[13]

b) Password Managers

Password managers are online tools that allow you to manage the multiple passwords that most people are bound to have across multiple platforms. Passwords managers require you to create a master password (the only one you have to remember, so it should be strong), which allows you to enter the password manager which, in turn, is a sort of encrypted vault which contains all your other passwords. Nowadays, password managers provide various options such as syncing across multiple devices, existing on a single device that logs into your accounts for you, or making sure you do not use the same password in too many places.[14]

Some effective password managers include:

- LastPass
- KeePass
- Dashlane
- Roboform 8
- 1Password

c) Two-Factor Authentication[15]

Enabling two-factor authentication for your online accounts is one of the simplest and best ways to promote online security. Two-factor authentication requires that, in addition to a password, one additional 'factor' or piece of data must be provided before you will be allowed into the account. This normally takes the form of a unique code sent to you via text, email or a particular app. Password managers such as LastPass, noted above, incorporate two-factor authentication as part of their security options. Major online services – including Google, Yahoo, Facebook, Twitter and Dropbox – all offer two-factor authentication.

Authy is an interesting two-factor authentication application:

---

[13] See: www.diceware.com.
[14] Allan Henry, *The Five Best Password Managers*, Lifehacker, 22 August 2017. Available at: https://lifehacker.com/5529133/five-best-password-managers.
[15] Google, 2-Step Verification. Available at: https://www.google.com/landing/2step/.

Instead of a code sent via text or email, which can be vulnerable to hacking or surveillance, the Authy application is downloaded to your device and then generates two-factor authentication codes automatically, offline, without Internet or cell service, relatively safe from surveillance or hacking. Furthermore, even if you lose your device, as long as you reinstall Authy on another device and login to your account you will be able to continue to generate codes for all the services you have registered to your Authy account. Furthermore, all your Authy-registered two-factor accounts are backed up on an encrypted cloud, so that your data would be protected even if the Authy servers were hacked.

4. Email Encryption

Email is the most common means of communicating digitally, alongside various forms of social media and mobile applications. A sophisticated, highly secure way to protect email communications is to encrypt them. Encryption, when applied to email and other digital files and communications, digitally encodes the information so that it is meaningless to anyone who does not have what is often called a 'secret key', which decrypts it.

Pretty Good Privacy (PGP) is a technology for encrypting emails and files, making it harder for hackers to access them. It allows you to make sure your emails are only able to be read by the persons for whom they were intended, with the recipient needing to use a password to decrypt them. PGP also allows you to digitally sign your email, providing proof of who sent it.

Installing PGP is an involved process. The EFF provides detailed instructions for how to install PGP for both Windows and OS X.

5. Protection from Common Hacking and Phishing

One of the common methods that hackers use to obtain personal data is phishing. A phishing attack usually takes the form of an email which appears to be sent from an official website, such as a bank, that contains a link which, if followed, will ask you to enter personal information, such as a password. The email may also ask you to download a document or install software. Doing so will lead to the installation of malicious software (know as malware) on your device. The attackers can then use that malware to access your device remotely and steal your information or spy on you.

Here are some tips to defend yourself against phishing attacks:

- Do not click on links sent to you via email that you were not expecting to receive. If you are suspicious, use alternative means to verify that the email was sent by the sender. For example, call your bank or the individual who supposedly sent you the email.
- Install software updates as soon as possible. Hackers rely on software bugs to engage in their phishing schemes; keeping software updated lowers this risk.
- Irrespective of how professional an email looks, do not trust emails asking for personal information unless you know they are from a trusted source.
- Use password managers with auto fill. When you install a password manager and save your various passwords within it, it will generally automatically fill a password into those save accounts for you unless you set it to do otherwise. If you follow a link to a page and your password manager does not automatically fill it in, that is a clue to double check the site you are visiting. Furthermore, pay close attention to the URLs of the links you receive. They may have spelling errors or strange top-level domains (top-level domain refers to the last part of a web address, such as '.com'). For example, "www.transferwise.com" may appear as "www.*tras*ferwise.com" or "www.transferwise.*cam*". Note also the subtle and easily missed lack of a dot after 'www' in "https://*wwwtransferwise*.com". In addition, the 'L' in gmail.com may be replaced with a capital 'i' to trick the eye, as in '*gmaiI*'.
- Open any suspicious documents in Google Drive. This converts the document into an image or HTML, which prevents it from installing malware on your device.
- Avoid logging into websites via Facebook, Google or Twitter. Many online services offer the option of logging into the service via your social media accounts. Illegitimate websites can use this to collect personal data and passwords. Instead of doing that, create a new, dedicated account for that website.

As a general rule, avoid providing unnecessary personal information. If you must, provide non-personal (false) information and use a disposable email address to register with websites you only want to use a few times. The website www.sharklasers.com provides a service that generates disposable email addresses.

Finally, make sure you are familiar with the privacy settings and security capabilities of the social media services you use. Here are privacy guides for some of the most common platforms used by journalists:

- Facebook
- Twitter
- Linkedin

6. Secure and Anonymous Internet Browsing

If your Internet browsing is not secure, then it is not private. Cookies, most simply described as small pieces of data automatically stored by websites on your computer in order to track your user preferences, are a fundamental component of web browsing. It is now commonplace for cookies not only to store data about your user experience but also to track data about your individual online behaviour. The information stored by cookies is highly valued by marketing companies which use it to build personalised profiles and better target their advertising. This data is collected over long periods of time and often distributed without your knowledge and consent, meaning that there is no way of knowing if it may end up in the hands of actors who want to use your data for nefarious ends.

Public Wi-Fi is particularly insecure. Even if a network is password protected, others using that network may be able to spy on your web browsing and, in this way, potentially collect a large amount of personal information about you. There are a number of ways to promote security while browsing. From among the most popular browsers – namely Chrome, Safari, Internet Explorer and Firefox – Firefox has the best reputation for protecting user rights. The companies in control of the other browsers are known to have tracked their users' behaviour. As a result, it is recommended that you use Firefox as your default browser.

a) Browser Extensions

Browser extensions are free additions that can be added to your Internet browser which help to protect your browsing from hackers, State surveillance and corporate advertising. There are a number of extensions that you can add to browsers to increase the level of protection:

- Privacy Badger: EFF created this browser add-on to stop advertisers and other third-party trackers from secretly tracking your browsing behaviour. When it detects an advertiser who is tracking you, it automatically blocks their ability to load content to your browser. It is available for installation on Chrome, Firefox and Opera browsers.

- HTTPS Everywhere: This extension, also created by EFF, makes your browser automatically encrypt your browsing whenever possible. As a result, it also offers great protection against phishing attacks. Like Privacy Badger, it can be added to Chrome, Firefox and Opera browsers.

- uBlock Origin: This is an ad blocker extension that blocks advertisements while you browse, taking into account that advertisements are a great source of malware, viruses and undesired tracking. It can be installed on Chrome and Firefox.

- Disconnet.me: This extension blocks trackers from following your web activity, allowing for faster browsing. It is available for both Chrome and Firefox.

b) Tor Browser[16]

Even if one were using all of the above tools, advanced hackers, State actors and Internet service providers would still be able to find out your location based on your computer's personal Internet Protocol (IP) address and the information being sent back and forth to your computer. No extension can protect you from this. Therefore, if you wish to be totally anonymous as you browse, you should consider using the Tor Browser.

The Tor browser operates through the Tor network, which ensures that the origin of your web communications cannot be tracked by bouncing them around the world and through different layers of encryption. The Tor browser is particularly useful for secure communication between journalists and sources for whom anonymity is of the utmost importance, such as political dissidents or whistleblowers. The Tor browser not only provides anonymous browsing but also enables users to set up and use websites which are only accessible through the Tor network. However, because it uses anonymisation, browsing with Tor can be slower than with regular browsers.

An important caveat is that while Tor anonymises your activities, it does not make your communications private. You will not be protected if you engage in Internet activities that can identify you, such as making posts on or through your Facebook page, or emailing from your personal email account.

c) Virtual Private Network (VPN)

The best way to remain anonymous while using standard Internet browsers is to use a virtual private network (VPN) which encrypts your web traffic and prevents interception. When you use a VPN your web requests go through a VPN server, which encrypts your data before it reaches the wider Internet. Therefore, when you access a website, your request will appear to be coming from the VPN server, which may be located anywhere in the world, and not from your actual location. In addition to encrypting your data and protecting your personal information when you use public networks, using a VPN can also help you to avoid Internet censorship when you are connecting through a network that blocks certain websites.

[16] EFF, How HTTPS and Tor Work Together to Protect Your Anonymity and Privacy. Available at: https://www.eff.org/pages/tor-and-https.

Technically proficient individuals can set up their own VPN servers using open-source software, such as OpenVPN, or use free VPN add-ons that can be added to their browsers.[17] Many individuals also pay a fee to subscribe to a VPN provider of which there are very many options.

VPNs offer great protection against surveillance while using public networks but they do not protect your data from the VPN provider itself. The VPN provider may be able to see your traffic and there is nothing to prevent a VPN provider from collecting your personal data. It is, therefore, important to chose your VPN carefully, including by taking note of the location of the provider, and finding out about what laws they are subject to and their privacy policies. This can help you understand which information is likely to be turned over to State actors by the provider, should a request for it be made. A provider may also be able to access your IP address while you are using the service. When you wish to avoid revealing your IP address you can use the Tor browser to connect to your VPN.[18]

Some recommended VPN providers are:

- AirVPN
- Feral Hosting
- CyberghostVPN

In order to establish a VPN, you have to install what is called a VPN client on your computer which communicates with your VPN provider. Once installed, you can simply click on your client and all your Internet activity will automatically start to be routed through your VPN server. Like VPN providers, you have to pay for some VPN clients but many are free and work reliably. The VPN provider AirVPN comes with its own free client. Other recommended clients include:

- Viscosity
- Tunnelblick (free for Mac)
- OpenVPN (free for Windows)

d) Tails

Using the Tails operating system is the ultimate anonymity option as it goes beyond just the web browser. Tails is a privacy and security focused Linux-based operating system that can be installed at any time on any computer. The use of Tails can be particularly helpful for activists and journalists to avoid surveillance and to access the Internet without compromising their location and data. Tails can

[17] Preston Gralla, *5 great free VPNs for Chrome, Firefox, mobile, and beyond*, IT World, 4 August 2014. Available at: https://www.itworld.com/article/2696891/security/5-great-free-vpns-for-chrome--firefox--mobile--and-beyond.html.
[18] EFF, Surveillance-Self Defense: Choosing the VPN that's Right for You. Available at: https://ssd.eff.org/en/module/choosing-vpn-thats-right-you.

be installed on a USB or DVD and used on any computer whether it is a Linux, Windows or Apple based.

A big advantage of using Tails, in addition to its portability, is that it is amnesic so that it does not store any data between uses and no identifying information is left behind. In addition, all Internet activity is routed through the Tor network, HTTPS Everywhere is preinstalled and a PGP email client is also included to facilitate the sending of encrypted emails.

As with all security tools and software, if you use Tails, make sure that you are using the latest version. While Tails provides you with greater security, it is not completely invulnerable. For example, Tails does not automatically encrypt your documents and cannot protect you if your computer has already been compromised.[19]

7. Device Loss or Seizure

You should take precautionary steps to prevent your data being accessed or compromised in case your device is lost, stolen, or temporarily confiscated. In addition to securing all your online accounts and services using strong passwords and two-factor authentication where possible, it is important to encrypt your computer's hard-drive.

OS X for Mac comes with its own encryption software called File Vault 2. Windows 10 also encrypts your hard drive by default but if you have earlier versions of Windows you can download the encryption software Bitlocker,[20] to do the same thing. You can also decide to encrypt your files manually using PGP.[21]

If your device is stolen or lost, your data could be completely lost. To avoid this, it is recommended that you back up your data on an external hard-drive that is also encrypted. As a third and final line of defence, since an external hard-drive may also be stolen or lost, files can be saved to an encrypted cloud. A number of cloud storage services work just like Dropbox and Google Drive but have increased security as they have built-in encryption. A few suggestions include:

---

[19] Noah Kelly, A DIY Guide to Feminist Cyber Security. Available at: https://hackblossom.org/cybersecurity/#tails. A full list of Tails' vulnerabilities can be found at: https://tails.boum.org/doc/about/warning/index.en.html.

[20] Chris Hoffman, How to Set Up BitLocker Encryption on Windows, How-To Geek, 5 October 2017. Available at: https://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/.

[21] For a more detailed discussion of hardware encryption, a useful article from a digital expert is: Micah Lee, Encrypting Your Laptop Like you Mean It, The Intercept, 27 April 2015. Available at: https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/#osx.

- SpiderOak
- Tresorit
- Mega

You should also consider seriously whether some of your information is simply too sensitive to record or store digitally regardless of the technology you are using. In addition, always delete any critical information that you do not need in digital format from all of your devices.

If, after being temporarily separated from a device, for example because it is seized at a border crossing or elsewhere, you are worried that it might have been tampered with, it is a good idea to restore the device from a backup including a reinstallation of the operating system. With a smartphone, depending on the circumstances and level of risk it was exposed to, you might even consider getting rid of the phone and replacing it with a new one, to which you can migrate your data from a backup.

8. Phone Protection

Smartphones may be compromised in many different ways. The GPS function on smartphones that many social media applications use can give away your location. Leaving your phone Wi-Fi enabled can also leave you vulnerable to attack, as a hacker using a nearby network could collect your metadata even when you are not active online. As a result, it is best to disable the Wi-Fi and location settings on your phone whenever you do not need to use them.

The best way to protect the information contained in your smartphone is to encrypt it and download the tools you need to browse anonymously.

a) Mobile Browsing Privacy

As with desktop browsers, it is recommended that you download and use the mobile browser developed by Mozilla Firefox, available for both iOS and Android devices. On Android devices, the Firefox mobile browser also allows you to install all of the privacy extensions discussed above. On Apple devices, the Firefox mobile browser not only blocks trackers, advertisers and minimises surveillance, but also lets you extend its privacy features to other apps on your device.[22]

It is better to use the official mobile applications for websites which have created them rather than logging into those websites through the default browser on your device, which is less secure.

[22] Noah Kelly, A DIY Guide to Feminist Cyber Security, explains: "To enable these features in Safari, go to Safari under Settings, click 'Content Blockers', and enable Firefox Focus". See: https://hackblossom.org/cybersecurity/#mobilebrowsing.

b) Secure Mobile Messaging

The top recommended tool for secure messaging via smartphones is the open source software application called Signal. Signal offers end-to-end encrypted phone calls and messaging of text, videos and pictures. It completely encrypts the content of what is sent so that all anyone conducting surveillance on the cellular network could see is who sent and received the text and when it was sent, but not what was sent. The WhatsApp messaging application also offers end-to-end encryption but the added benefit of Signal is that your messages are also encrypted locally on the phone, so that if anyone else gains control of your phone they would need to decrypt both your application and your phone in order to view any stored messages. EFF provides instructions on how to install and use Signal on both Android[23] and iOS[24] devices.

c) Mobile Device Encryption

A positive development is that privacy concerns have led the producers of Apple and Android devices to encrypt their devices by default, securing the data contained on the phone from hackers. In addition, devices now offer greater levels of security through the use of passcodes[25]or fingerprint Touch ID. Most recently, Apple has also developed a facial recognition option on its newest devices to keep others out should your device be lost or stolen. As with passwords, it is recommended that passcodes be six characters or longer.

The EFF provides an in depth guide on how to best encrypt your iPhone,[26] and the Android blog Greenbot does the same for Android devices.[27]

9. Other Resources and Digital Guides

- EFF, Surveillance Self-Defence

[23] EFF, Surveillance-Self Defense: How to: Use Signal for Android. Available at: https://ssd.eff.org/en/node/93/.
[24] EFF, Surveillance-Self Defense: How to: Use Signal on iOS. Available at: https://ssd.eff.org/en/module/how-use-signal-ios.
[25] Passcodes are a string of characters that function as passwords do but which are specifically designed to gain access to a mobile device such as a tablet or smartphone.
[26] EFF, Surveillance-Self Defense: How to: Encrypt Your iPhone. Available at: https://ssd.eff.org/en/module/how-encrypt-your-iphone.
[27] Patrick Nelson, How to turn on Android encryption today (no waiting necessary), Greenbot, 19 September 2014. Available at: https://www.greenbot.com/article/2145380/why-and-how-to-encrypt-your-android-device.html.

This guide is a great general resource about online security that provides a basic overview of digital surveillance and how to avoid it, tutorials on how to install helpful tools and software, and detailed guides about specific situations.

- Committee to Protect Journalists, CPJ Journalist Security Guide: Covering the News in a Dangerous and Changing World

  The 'Technology Security' section of this guide provides advice on understanding the threats journalists face when protecting communications and securingdata.

- Tactical Technology Collective and Front Line Defenders: Security in-a-Box – Digital Security Tools and Tactics

  This digital security guide outlines the basic principles of digital security and offers step-by-step instructions to help install and use the most essential digital security software and services. It also offers tailored 'Community Guides' advising specific groups of people on how to protect themselves against digital threats faced uniquely by them. These guides include tailored advice on tools and tactics that are relevant to the needs of those particular groups (for example, Guide for LGBT activists in Sub-Saharan Africa).

- Privacytools.io

  This website provides information about global mass surveillance and provides tools to protect against it such as lists of VPN providers, browser testing tools and add-ons.

- We Fight Censorship, Online Survival Kit

  This guide "offers practical tools, advice and techniques that teach you how to circumvent censorship and to secure your communications and data" and aims to provide readers "with the means to resist censors, governments or interests groups that want to control news and information and gag dissenting voices."

- Digitaldefenders.org, Digital First Aid Kit

  This guide "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."

- Hack*Blossom, A DIY Guide to Feminist Cybersecurity

  This guide aims "to be a comprehensive and accessible introduction to some of the most valuable cyber security tools available." The guide provides advice on how to maintain anonymity, avoid hacking, and protect data online and on various types of devices.

10. Glossary[28]

Add-on

"A piece of software that modifies another software application, changing how it works or what it can do. Often add-ons can add privacy or security features to web browsers or email software. Some add-ons are malware, so be careful to install only those that are reputable and from official sources."

Commercial VPN

"A commercial Virtual Private Network is a private service that offers to securely relay your Internet communications via their own network. The advantage of this is that all of the data you send and receive is hidden from local networks, so it is safer from nearby criminals, or untrusted local ISPs or cybercafes. A VPN may be hosted in a foreign country, which is useful both for protecting communications from a local government, and bypassing national censorship. The down side is that most of the traffic is decrypted at the commercial VPN's end. That means you need to trust the commercial VPN (and the country where it is located) not to snoop on your traffic."

Cookies

"Cookies are a web technology that let websites recognize your browser. Cookies were originally designed to allow sites to offer online shopping carts, save preferences or keep you logged on to a site. They also enable tracking and profiling so sites can recognize you and learn more about where you go, which devices you use, and what you are interested in – even if you don't have an account with that site, or aren't logged in."

Cryptography

[28] The definitions in this glossary are all taken from the Electronic Frontier Foundation's Surveillance Self-Defence Glossary. Available at: https://ssd.eff.org/en/glossary.

"The art of designing secret codes or ciphers that let you send and receive messages to a recipient without others being able to understand the message."

Decrypt

"Make a secret message or data intelligible. The idea behind encryptionis to make messages that can only be decrypted by the person or people who are meant to receive them."

Encrypt

"To apply encryption technology to any sort of information or communication. This transforms the information or communication mathematically so that it seems meaningless, but can still be restored to its original form by a person or device that possesses the right secret key. This limits who can access the information because without the right secret key, it should be impossible to reverse the encryption and recover the original information. Encryption is one of several technologies that make up the field called cryptography"

End-to-end encryption

"End-to-end encryption ensures that a message is turned into a secret message by its original sender, and decoded only by its final recipient. Other forms of encryption may depend on encryption performed by third parties. That means that those parties have to be trusted with the original text. End-to-end encryption is generally regarded as safer, because it reduces the number of parties who might be able to interfere or break the encryption."

Key

"In cryptography, a piece of data which gives you the capability to encrypt or decrypt a message."

Malware

"Malware, is short for malicious software: programs that are designed to conduct unwanted actions on your device. Computer viruses are malware. So are programs that steal passwords, secretly record you, or delete your data."

Metadata

"Metadata (or "data about data") is everything about a piece of information, apart from the information itself. So the content of a message is not metadata, but who sent it, when, where from, and to whom, are all examples of metadata. Legal systems often protect content more than metadata: for instance, in the United States, law enforcement needs a warrant to listen to a person's telephone calls, but claims the right to obtain the list of who you have called far more easily. However, metadata can often reveal a great deal, and will often need to be protected as carefully as the data it describes."

Online harassment

"Offensive name-calling, intentional efforts to embarrass someone, physical threats, stalking, harassment over a sustained period of time or sexual harassment online."[29]

Operating system

"A program that runs all the other programs on a computer. Windows, Android and Apple's OS X and iOS are all examples of operating systems."

PGP

"PGP or Pretty Good Privacy was one of the first popular implementations of public key cryptography. Phil Zimmermann, its creator, wrote the program in 1991 to help activists and others protect their communications. He was formally investigated by the US government when the program spread outside the United States. At the time, exporting tools that included strong public key encryption was a violation of US law. PGP continues to exist as a commercial software product. A free implementation of the same underlying standard that PGP uses called GnuPG (or GPG) is also available. Because both use the same interchangeable approach, people will refer to using a "PGP key" or sending a "PGP message", even if they are using GnuPG."

Risk analysis

"In computer security, risk analysis is calculating the chance that threats might succeed, so you know how much effort to spend defending against them. There may be many different ways that you might lose control or access to your data, but some of them are less likely than others. Assessing risk means deciding which threats you are going to take seriously, and

[29] Maeve Dugan, *Online Harassment 2017,* Pew Research Center – Internet and Technology (Jul. 11, 2017), http://www.pewInternet.org/2017/07/11/online-harassment-2017/.

which may be too rare or too harmless (or too difficult to combat) to worry about. See threat modeling."

Threat model

"A way of narrowly thinking about the sorts of protection you want for your data. It's impossible to protect against every kind of trick or attacker, so you should concentrate on which people might want your data, what they might want from it, and how they might get it. Coming up with a set of possible attacks you plan to protect against is called threat modeling. Once you have a threat model, you can conduct a risk analysis."

VPN

"A virtual private network is a method for connecting your computer securely to the network of an organization on the other side of the Internet. When you use a VPN, all of your computer's Internet communications is packaged together, encrypted and then relayed to this other organization, where it is decrypted, unpacked, and then sent on to its destination. To the organization's network, or any other computer on the wider Internet, it looks like your computer's request is coming from inside the organization, not from your location. VPNs are used by businesses to provide secure access to internal resources (like file servers or printers). They are also used by individuals to bypass local censorship, or defeat local surveillance."