DIGITAL SECURITY AND PRIVACY

FOR ACTIVISTS & HUMAN RIGHTS DEFENDERS OPERATING IN AFGHANISTAN
SEPTEMBER 2022

AFGHANISTAN DEMOCRACY AND DEVELOPMENT ORGANIZATION
(ADDO)

Table of Contents

AFGHANISTAN DEMOCRACY AND DEVELOPMENT ORGANIZATION (ADDO)

Afghanistan Democracy and Development Organization (ADDO)[1] is a non-governmental organization registered in the Ministry of Economy in Afghanistan in 2014. ADDO has been working in Southern, Northern, and Central Afghanistan, including Kabul. The Vision of ADDO is to create a society where the rule of law, democracy, and respect for human rights are the cornerstones of society's governance and where target communities have attained a sustainable level of social and economic self-autonomy. The Organization's goal is to advance democratic principles and human rights through strengthening Afghan citizens' capacities, engaging in advocacy work and research, and promoting a more favorable image of Afghanistan abroad. In both rural and urban parts of Afghanistan, ADDO is engaging with policymakers, CSOs, women's rights groups, and youth organizations to strengthen democracy through training, research, monitoring of legislation, advocacy, capacity building, and preservation of human rights and freedoms.

ABOUT THE MANUAL

This manual was developed using the most recent information on digital security and safety. This is a helpful user guide for all Afghan activists and human rights defenders operating in Afghanistan and beyond the borders. As this manual has been shortened, we have made an effort to avoid including unnecessary details that can confuse the readers. As an alternative, we offered links for every subject covered under each summarized topic. There are many helpful websites that can provide more information on any of the subjects covered in the manual. For more updated and helpful information, the readers can explore any of the websites. This manual was made possible by the generous support of ACCESSNOW. ADDO appreciate ACCESSNOW for their funding support and opportunities. The contents and opinions expressed herein are not the responsibility of ACCESSNOW and do not necessarily reflect its views. ADDO would welcome any comments on the content of this manual (including the correction of any mistakes).

[1] http://addo.org.af

LIST OF ACRONYOMS

- AES - Advanced Encryption Standard
- BYOD – Bring Your Own Device
- GMIC - Government Media and Information Center – Afghanistan
- HTTPS - Hypertext Transfer Protocol Secure
- IDS - Intrusion Detection System
- IoT - The Internet of Things
- ISP - Internet Service Provider
- NSA - National Security Agency
- OS - Operation System
- PC - Personal Computer
- RFID - Radio Frequency Identification
- SSL - Secure Sockets Layer
- SMS - Short Message Service
- UDHR - Universal Declaration of Human Rights
- VPN - Virtual Private Network

1. DIGITAL SECURITY AND PRIVACY

Undoubtedly, we use computers, smart phones, and the Internet to seek, store and exchange information. Therefore, security in a digital world relates to our information security. We must protect our information where it is stolen, restricted, compromised, and damaged. In an idle system, everybody has an equal opportunity to access and disseminate information. However, some governments control the flow of information, and while they want, they impose restrictions on the information. The other problem is that internet users will experience malicious individuals who create viruses for computers and smart phones and hack into their systems to cause damage and stole valuable data.

Now confusion rules our digital world. We hopefully say that nothing is certain. However, everything can possibly happen. We send an email, text someone, send documents on social media communication tools, and or write a document, but we never consider the outcomes of the insecurity. Undoubtfully, we can't be confident players in the digital environment. We have to be fully aware of our potential and weaknesses in the new age of information highways and technology which emerges. We must be aware and have the skills to survive and accomplish our daily work on the internet safely.

Some countries pass legislation and introduce new technologies to have more surveillance power. For example, the ECHELON[2] project is introducing a global surveillance system that is able to record and process our communication on telephone, internet, and satellite. As a result, the right and ability to access information from internet connection points have been restricted. The governments were not ready to give the right to their citizens, took advantage of that, and restricted the rights to free access to the internet. Several country-specific filtering systems have been developed to restrict and block internet information considered inappropriate and or against the country's laws.

Global Internet restrictions and surveillance are on the rise. As general online freedom has decreased, governments all around the world are stepping up their Internet restriction and surveillance efforts. There has been a decline since June 2014 in online freedom in over half of the 65 nations analyzed. France, which imposed a law in the wake of the Charlie Hebdo attacks, saw one of the worst decreases. Iran, Syria, and China are listed as the nations with the strictest limitations on online freedom. In total, 14 nations passed legislation to increase government

[2] The Five Eyes, also known as Australia, Canada, New Zealand, the United Kingdom, and the United States, are the five signatory nations to the UKUSA Security Agreement and manage the monitoring program.

surveillance. Private enterprises in 42 of the 65 countries were compelled to delete or restrict internet information because critical remarks regarding governmental authority were more likely to result in censorship. Additionally, a lot of governments adopted increasingly strident attitudes against technologies for online anonymity and encryption[3].

China introduced a "Great Firewall," which routes all international communications. The Great Firewall functions through proxy servers at official gateways. The Ministry for Public Security was able to identify individual users and the contents, define the rights, and finally monitor traffic into and out of the country at these gateways[4]. Now, the "Great Firewall" in China is transforming an entire generation[5]. Following that, China introduced the "Golden Shield." It was an ambitious successor to the previous system. The Golden Shield relies on a national internet and is separated from the global internet. The Golden Shield Project was supposed to keep a database of every internet user and utilize it to aid in maintaining national security. In essence, it was a technique for widespread spying in China[6]. China has built surveillance intelligence in the network, which allows it to see, hear and think. Now content filtration moved from national levels to millions of information and communication devices in public places and citizens' homes. Finally, the Golden Shield is equipped with incredibly complex technology.

These limitations restrict our capacity to use the Internet and travel across borders in our pursuit of knowledge and communication. Additionally, they violate a number of the Universal Declaration of Human Rights (UDHR) provisions that guarantee everyone's right to privacy and freedom of expression.

Techniques for surveillance and monitoring have moved from the control of intelligence officers to hardware and software systems run by both commercial businesses and governmental organizations.

Before, someone who was deemed a threat to national security was being spied on. Because of the monitoring and filtering mechanisms that our governments have set up on the Internet, we are all now suspects. The technology doesn't always distinguish between users since it watches for specific phrases in our email, messages, and web searches, and when it detects them, it alerts surveillance teams or disables our communications.

One of the final lines of defense for online privacy is encryption. It allows us to encrypt our communications so that only the intended recipient may read them. Even the Internet's architecture includes a layer of encryption to support safe financial transactions which is called

[3] https://www.reuters.com/article/cybersecurity-report-idINKCN0SM1NJ20151028
[4] https://www.techtarget.com/whatis/definition/Great-Firewall-of-China
[5] https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385
[6] https://basecreative.co.uk/

Secure Sockets Layer (SSL)[7]. This technology encountered fierce criticism in many nations when it started to be used to secure non-financial information. The US government initially wanted to outlaw all SSL encryption whose complexity was greater than their ability to decrypt it[8]. All encrypted emails will likely be gathered for additional examination by a global monitoring system like ECHELON (or any other), just because they were encrypted in the first place. Therefore, every attempt at privacy will be interpreted as a desire to conceal something.

There are specific threats faced by activists and human rights defenders in their own countries. They frequently become the subject of surveillance and restrictions. Their ability to exercise their right to free speech is regularly restricted.

They often face severe punishments for carrying on with their work. For them, the digital age has been both a benefit and a curse. On the one hand, they are now more connected to their global colleagues, and the speed of communications and reports of human rights abuses can quickly become viral. The Internet is being used to mobilize people, and many social initiatives have shifted online, particularly during COVID-19. In addition, the digital divide has kept many activists and defenders in less developed countries from participating in the global dialogue and outreach because they lack access to computers or the Internet. The insecurity of their mobile devices increase daily.

Emails do not reach their intended recipients, social media pages are hacked, Internet connections are patchy, social media communication tools are severely monitored, telephone conversations are heard, computers are seized, and viruses ruin years of work. These issues are typical and well-known. The growing interest of authorities in online publishing is another frequent occurrence. When "unwanted" content comes from an activist and a human rights defender, the authorities swiftly retaliate. They are actively looking through online news sites, social media pages, and blogs.

The Digital Divide, Digitally Facilitated Repression, Violations in the Name of Security, Systemic Cyber Vulnerability, and Digital Insecurity are just a few of the challenges that continue to exist for activists and human rights defenders around the world.

By being familiar with computers, smart phones, and Internet operations, activists and human rights defenders can better protect their work. Therefore, they will be more successful at defending their own rights and advancing the rights of others they are attempting to help.

2. GOVERNMENT SURVEILLANCE

[7] https://www.ssl.com/faqs/faq-what-is-ssl/
[8] https://www.ssl.com/blogs/june-2020-security-roundup/

Governments are investing more in high-tech equipment to track the online activity of their citizens. The increasing use of social media surveillance, when combined with an alarming rise in the number of nations where social media users have been detained for their online legal activity, threatens to reduce the room for civic activism on digital platforms. Many governments monitor their citizens' online behavior, as do their intelligence services. Your Internet Service Provider (ISP) is privy to everything you do online, and authorities can force it to turn up your data[9].

Social media surveillance is another challenge for activists and human rights defenders. It entails the collection and handling of private information gleaned via online communication tools, frequently through the use of automated software that enables the real-time gathering, management, and analysis of substantial volumes of metadata and content. Social media monitoring cannot be dismissed as less intrusive because it is more extensive than spyware, which intercepts conversations by focusing on the devices of particular people. These digital platforms are used by billions of people worldwide to connect with friends and family, interact with loved ones, and express their political, social, and religious opinions. The information that is gathered, created, and inferred about users of these services, even when they rarely interact with them, is of enormous value to advertisers as well as, increasingly, to law enforcement and intelligence organizations. Governments have deployed professionals to monitor social media speech for a long time, including by setting up phony accounts to communicate with actual users and access networks. Iranian authorities have bragged about their 42,000-strong army of volunteers who keep an eye on online speech. On the website of the Cyber Police (FATA), any citizen may report for duty. Similar to this, China has hired hundreds of people to comb through the internet and alert the authorities to any questionable accounts or content. Chinese agents actively collaborate with major companies to keep an eye on people online. Approximately 364 million Chinese users' social media accounts, communications, and shared files were found in an unsecured database that was being used by security researchers for manual law enforcement tracking. The Chinese government has access to user information and metadata through a complicated web of regulations, which makes it easier for authorities to identify and penalize individuals who publish sensitive content[10].

Afghanistan, as it is today, is very different from the country where the internet was outlawed in 2001. Cell towers were built nationwide by the government, which the United States supported. According to market research company Statista, the number of mobile phone users increased from just one million in 2005 to over 22 million in 2019. According to experts, 70% of people have access to a cell phone.

The Taliban, who formerly ruled Afghanistan by outlawing the internet, have used social media as a potent weapon to quell opposition and disseminate their views. They are using thousands of Twitter accounts, some official and some anonymous. They show the technological prowess that

[9] https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance
[10] https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance

the militants have developed over the course of years of warfare, providing a sneak peek at how the Taliban might utilize those resources to control Afghanistan. The citizens, social media users removed their pictures, posts, and even cancel their accounts as Taliban spread fare. Both Facebook and Twitter have pledged to take action to protect accounts. Social media accounts of participants in anti-Taliban campaigns had been deleted. Without the time and outside assistance, the Taliban today would find it difficult to block messages from the outside, as China and Russia do[11].

Many Afghans, especially those whose livelihoods or personal status make them targets for the Taliban, started frantically deleting or editing their social media accounts or online presence as the Taliban started searching people for phones and houses for any weapons. They do this because they know the Taliban follow a regional trend of social media surveillance to consolidate power over perceived dissenters. While the Taliban have been known to utilize social media for narrative control and surveillance, the previous U.S.-backed administration had dabbled with similar strategies, periodically ordering the shutdown of messaging applications like WhatsApp and Telegram in the country[12].

Now as an activist and human rights defender, you might be the target of government surveillance if you use social media frequently, speak at conferences, or are outspoken about your engagement with civil society organizations. This is especially true if you have publicly called for reform, supported human rights, or exposed potential corruption or human rights violations. Uncomfortably, targeted surveillance doesn't require that you have committed a crime. Governments utilize a variety of sophisticated cyber tools to spy on a variety of professionals, including journalists, academics, and even government officials themselves. This practice occurs everywhere. Authorities have been known to access devices through surveillance techniques, retrieve contacts, find passwords, track messages and phone calls, and interfere with the activity of activists. Governments have exploited the data gathered through surveillance methods to malign activists, portray them as criminals, and concoct accusations to have them jailed.

3. PROTECTING YOUR INTERNET CONNECTION

Because your Internet Service Provider (ISP) manages your internet traffic, it can keep track of everything you do online. Your ISP may be able to view your files, emails, passwords, online purchases, and even the questions you ask your smart speaker. What's worse is that your ISP may gather enough information about you to correlate your numerous activist activities, perhaps assisting law enforcement in compiling evidence against you. ISPs assert that they do not share your information with outside parties. However, they may be required to turn over your

[11] https://www.nytimes.com/2021/08/20/technology/afghanistan-taliban-social-media.html
[12] https://www.mei.edu/publications/how-digital-rights-are-key-protecting-afghans-under-taliban

information to governmental and law enforcement authorities. For example, ISPs in Australia are required to give the federal police access to user surfing data. Some of that information is kept for as long as two years.

For secure connections, use a Virtual Private Network (VPN). Here are some VPNs having anti-censorship track records:

- TunnelBear: https://www.tunnelbear.com/download
- VPNGate: https://www.vpngate.net
- ProtonVPN: https://protonvpn.com
- Mullvad: https://mullvad.net/en/download/
- Bitmask: https://bitmask.net

Your best option is to think about spending money on a reliable VPN to fight the intrusiveness of ISPs VPNs. Then, when you go online, a VPN will give you a private, secure connection and assist in making your online behavior anonymous. Multiple layers of security are used by VPNs and are relatively simple to set up, such as:

3.1. USE ENCRYPTION

Strong 256-AES (Advanced Encryption Standard)[13] encryption is used to protect your connection with premium VPNs. This stops nosy people from monitoring or spying on your online behavior. The websites you visit and the services you use won't be visible to your ISP or other outside parties as a result[14].

3.2. CHOOSE A VPN WITH NO-LOGS POLICY

Choose a VPN that strictly adheres to the no-logs rule so that it cannot store any of your user data on its servers. Your browsing history and personal details are included. The VPN won't have anything to turn over to the police if they ask for any information about you[15].

3.3. MASK IP ADDRESS

[13] The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government.
[14] https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard
[15] Please see: 3. protecting your internet connection

Many thousands of servers are located around the world in larger VPNs. Your actual IP address is hidden when you connect to one because of the VPN IP address. Doing this makes it impossible for anyone to link your online activities to you[16].

3.4. DON'T TAKE THE RISKS OF A FREE VPN

Numerous free VPNs claim to shield your online privacy and critical information. Many of them have significant drawbacks and risks, such as:

- Limitations on the amount of data you can utilize and the number of devices you can protect third-party trackers included in their program minimal server options;
- Internet connection lag when using a VPN;
- Adware and hidden malware; and
- Appearing in pop-up adverts that claim your data is shared with third parties.

3.5. CIRCUMVENT ONLINE CENSORSHIP

You probably can't access specific news websites, apps, or social media if you reside in a country with severe online restrictions. However, you can connect to servers in countries where certain websites and apps aren't blocked by using a reliable VPN. You can access geographically restricted content and neutral resources and even coordinate your activity online by shifting your digital location. However, it's wise to research which VPNs are most effective in your area because not every VPN can access all blocked content.

3.6. ENHANCE SECURITY

Premium VPNs can be used on the most popular desktop and mobile operating systems. Even smart TVs, routers, and a few other linked gadgets can use them.

3.7. ACCESS THE INTERNET ANONYMOUSLY, USE THE TOR NETWORK

[16] https://www.expressvpn.com/go/what-is-my-ip/hide-my-ip-1?category=DSA&subcategory=All&lang=en&gclid=Cj0KCQjw08aYBhDlARIsAA_gb0fTCTXscDgpdFV8XemQ8uB2NtWkbDmoNe4WDZ5CzEs9EekoMhkdolYaAsN3EALw_wcB

A fantastic approach for activists to access the internet safely and anonymously is through Tor (The Onion Router)[17]. All your internet activity and data while connected to the Tor network is encrypted multiple times, making it impossible to identify you from any of it.

To maximize privacy and protection, we advise combining a VPN with Tor. Prior to connecting to Tor, you should connect to a VPN (VPN over Tor). By doing this, the Tor node won't be able to see your home IP address, and you will benefit from all the privacy safeguards offered by the Tor network. Using a VPN over Tor has additional advantages, such as:

Your home network cannot identify that you are using Tor because of the encrypted traffic from your VPN. In locations where Tor is restricted, a VPN can give you access to the network. You won't be able to be tracked by your VPN when using the Tor network. Your VPN adds an extra degree of security between you and any bugs that may exist in the Tor browser.

3.8. USE PUBLIC WI-FI SAFELY

The traffic that passes across an open Wi-Fi network is typically not secured, making it an obvious target for online snoops. This makes using public Wi-Fi risky. It is crucial that you take precautions if you must engage in activism-related activities on a public network.

Please keep in mind while using a public Wi-Fi:

- Encrypt your data using a VPN to render your internet activity impenetrable and impossible to track;
- Visit only HTTPS[18]-secured websites;
- If you're using a public computer, make sure to log out of all your accounts;
- Keep your firewall turned on for further virus defense;
- Use a personal portable router to manage your network connection;
- Never join unreliable networks;
- Don’t join a network without a password protection;
- Don’t enable automatic Wi-Fi connection for your devices;
- When not in use, never keep your Bluetooth or Wi-Fi connected; and
- Using public Wi-Fi, don’t distribute or upload private information or documents.

[17] https://www.vpn-mentors.com/best-vpn-for-tor/?keyword=tor%20network&geo=9000786&device=&cq_src=google_ads&cq_cmp=10810894927&cq_term=tor%20network&cq_plac=&cq_net=g&cq_plt=gp&gclid=Cj0KCQjw08aYBhDlARIsAA_gb0dJGmeR8Q3oUBfjrPFFXETlP7Y_LVDmhi7yzJanyxrLAK7gKNviMjAaAkI6EALw_wcB

[18] https://www.cloudflare.com/en-ca/learning/ssl/what-is-https/

4. PROTECTING YOUR COMPUTER

There is a ton of private and valuable information on your computer. You presumably use a variety of computers every day, including a laptop, tablet, smartphone, home desktop, and office desktop. Your bank information, emails, files, images, videos, and other digital communications are all stored on these devices. The first step in protecting all of your online devices and data is to secure your PC.

The majority of the activists own computers with Microsoft Windows as their operating system. The most widely used variations are Windows 11[19], 10[20], and 7[21]. Your computer needs to have a secure operating system to be protected from online attacks. In search of vulnerable PCs lacking certain security upgrades, thousands of hackers are continually checking IP addresses. Weekly security updates should be installed on all Windows versions, even if the computer is brand new. If you permit it, the majority of Windows versions will perform this patching automatically.

Activists rely on the internet to check their emails, run campaigns, join movements outside their geographical areas, join online meetings, study online, participate in social media, and carry out other crucial operations—despite the presence of surveillance by government authorities and computer hackers. Yet even at huge organizations with advanced security safeguards, we frequently learn about significant computer intrusions. Use below standard instructions to safeguard your computers and sensitive information in them:

4.1. ACTIVATE A FIREWALL

Activate the firewall before accessing the internet. A firewall acts as a wall between a network and the outside world, providing basic security. Sometimes a firewall is a standalone server, other times, it is a router, and still other times, it is computer software. A firewall, in whatever physical shape it takes, controls network traffic entering and leaving the system. In conjunction with a firewall, a proxy server is frequently used to mask the IP address of the internal network and display a single IP address to outsiders. The perimeter is protected by firewalls and proxy servers, which analyze traffic and stop it from going somewhere that has been forbidden by the administrator. An intrusion detection system (IDS) is frequently used to supplement these two security measures. An IDS merely keeps track of traffic and searches for any unusual activity that would point to an attempted breach.

[19] https://www.microsoft.com/en-ca/software-download/windows11
[20] https://www.microsoft.com/en-ca/windows/get-windows-10
[21] https://www.microsoft.com/en-ca/software-download/

4.2. INSTALL ANTIVIRUS SOFTWARE

Numerous well-known antivirus programs are available for Windows-based PCs. Your computer is protected from malicious software and unauthorized code by antivirus programs like Avast, Bitdefender, Panda Free Antivirus, and Malwarebytes. Malware and computer viruses are pervasive. Viruses might be the main reason your computer runs slowly or erase important files, or they may be less obvious. Antivirus software monitors every activity and runs continually. This applies to each time you access a file from the internet, run the software, or open a document. All new files are scanned by the application, and any ones it finds suspicious are quarantined. Usually, you will then be prompted to take action. When customizing your antivirus program, there are two very crucial factors to take into account. The first step is to confirm that updates are being applied to your antivirus solution. Making ensuring there is just one antivirus product installed on the computer is the second crucial component. If you have more than one antivirus program installed, they will compete with one another for control of your computer. You can find top 10 antivirus for 2022 here: https://www.antivirussoftwareguide.com/best-windows-antivirus

4.3. INSTALL AN ANTISPYWARE PACKAGE

Spyware is a specific kind of software that covertly watches and gathers data from individuals or organizations. Some spyware logs each keystroke in order to access passwords and other sensitive financial data. All computer activity can be monitored by spyware programs, and third parties can access this data in a variety of ways. The most typical technique uses a Trojan horse. Additionally, if you are simply browsing a certain website, malware may start to download in the background.

Luckily, there are numerous software programs available that are intended to find and eliminate spyware, just as there are numerous spyware applications accessible. Although antispyware focuses solely on this threat, it is frequently included in popular antivirus packages from companies like Webroot, McAfee, and Norton. Real-time security is provided by antispyware products, which examine all incoming data and stop threats. Additionally, these applications are frequently affordable. The best course of action you can take to prevent spyware from infecting your computer is, of course, to never download anything from the Internet that does not originate from a very reputable and trusted website. Most current antivirus programs either come standard with antispyware or offer it as an optional addition. You can find top 10 antivirus including antispyware for 2022 here: https://www.antivirussoftwareguide.com/best-windows-antivirus

4.4. USE COMPLEX PASSWORDS

Using computers effectively requires using strong passwords. A strong password is the most important component of any system when it comes to digital security. The most frequent way that

hackers and attackers target your information systems is via cracking passwords, according to history. Use a password manager, such as Dashlane[22], Sticky Password[23], LastPass[24], or Password Boss[25]. Have a strong window password, but don't depend on Windows passwords to keep your information secure. They are quickly destroyed. Instead of using a short, obvious password, it is preferable to write down your passwords and save them securely. Use a different password each time and ensure secure passwords that are not closely connected to your interests or way of life. Never divulge or disclose your key passwords to anyone. Every three to six months, change your passwords. Keep in mind that a variety of free online tools are available to help you find your Windows password, wireless network encryption, and pretty much any other kind of computer password you might have.

4.5. UPDATE YOUR OS, APPS, AND BROWSER

It's not too difficult to upgrade your operating system and antivirus software. This feature is already activated by default on current products. However, it's possible that some of the software programs you've placed on your computer aren't getting security updates. Web browsers, Java[26], Adobe Reader[27], and many other programs fall under this category. The updating of these programs is essential. You might have already noticed that Adobe Reader prompts you to update the program each time you open a PDF file. Certain upgrades fix the flaws that make it possible for malicious software to attack these programs.

Install any new operating system updates immediately. Most updates come with security patches that stop hackers from accessing and using your data for their own purposes. Apps are no different. Web browsers of today are getting more and more intelligent, especially in terms of privacy and security. In addition to applying all fresh updates, remember to check your browser's security settings. For instance, you can increase your online privacy by using your browser to stop websites from tracking your movements. Alternately, use one of these secure web browsers.

4.6. IGNORE SPAM[28]

The majority of readers have probably heard of spam. Spam is unsolicited, undesired email that is distributed to several recipients. Although it is frequently utilized for marketing purposes, it is also

[22] https://www.dashlane.com
[23] https://www.stickypassword.com
[24] https://www.lastpass.com/features/password-generator
[25] https://www.passwordboss.com
[26] https://www.java.com/en/
[27] https://www.adobe.com
[28] https://www.malwarebytes.com/spam

capable of being abused for much darker ends. For instance, spam is a typical method for a virus or worm to spread. In order to steal the recipient's identity, spam is also used to send emails that tempt them to visit phishing websites. In essence, spam is at best a nuisance and at worst a delivery method for malware including spyware, viruses, worms, and phishing attacks. Therefore, be alerted when opening attachments or clicking links in emails from someone you don't know. Spam inbox filters are getting better at catching the most obvious spam. However, more sophisticated phishing emails that impersonate your friends, colleagues, and reliable organizations (like your bank) have grown popular, so be alert for anything that seems or sounds suspicious.

4.7. BACKUP YOUR COMPUTER

Having a backup of your data is essential in case hackers manage to break in and destroy your system. Always make sure you can recover as quickly as you can if you experience a data loss or incident. Start with the backup programs included with Windows File History[29] and macOS Time Machine[30]. These utilities can also be used effectively with enough capacity on an external backup hard disk.

The assumption that "nothing will go wrong" frequently takes precedence over the necessity of making a backup copy of your computer's contents. We count on both ourselves and our technology to prevent forgetting, losing, or harming information.

Think about the kind, volume, and frequency of your information's backup. You can have a copy of all your data and documents on iCloud[31] and Dropbox[32], but you may want to carry about a USB memory stick with a copy of everything else. A server computer in your organization needs regular backups of the software and system settings in addition to the documents that users keep on it.

4.8. SHUT YOUR COMPUTER DOWN

Many organizations are constantly "all systems go," especially those that run web servers. However, if you're not running a sophisticated internet-based organization, turn your computer off at night or for extended periods of time while you're not using it. Shutting down your computer removes any connection a hacker may have made with your network and stops any potential harm from happening because leaving your computer on makes it more apparent and a target for hackers.

[29] https://support.microsoft.com/en-us/windows/file-history-in-windows-5de0e203-ebae-05ab-db85-d5aa0a199255
[30] https://support.apple.com/en-ca/guide/mac-help/mh35860/mac
[31] https://support.apple.com/en-ca/guide/mac-help/mh35860/mac
[32] https://www.dropbox.com

4.9. SECURE YOUR NETWORK

Most routers do not ship with the greatest levels of security enabled. When configuring your network, access the router and enter a password using an encrypted, safe setup. This stops hackers from accessing your network and changing your settings.

4.10. PUT TWO-FACTOR AUTHENTICATION TO USE

Your primary defense line against computer hackers is a password, but adding another layer increases security. Many websites allow you to set two-factor authentication, which increases security by requiring you to provide a number code in addition to your password when logging in. This code is sent to your phone or email address.

4.11. YOU MAY USE ENCRYPTION

Encryption can stop hackers from accessing any of your data, even if they are able to access your network and files. You can encrypt any USB flash drive that contains sensitive information, encrypt your Windows or macOS hard drive with BitLocker[33] (Windows) or FileVault[34] (Mac), and utilize a VPN to secure web traffic. Only make purchases from secure websites; you can tell them apart right away by the "HTTPS" in the address bar and the closed-padlock icon.

5. PROTECTING YOUR SMARTPHONE

The use of mobile devices over computers increased daily. Threats to the security of mobile devices are increasing. On more than 1 million user devices, Kaspersky discovered about 3.5 million pieces of malware in 2014. Kaspersky's in-lab detection algorithms processed 360,000 malicious files per day by the end of 2017. Additionally, 78% of those files were malware programs, amounting to a daily detection rate of over 280,000 malware files, many of which are aimed at mobile devices. Here are some mobile device threats and predictions for the future[35].

5.1. UNSECURED WI-FI

[33] https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview
[34] https://support.apple.com/en-ca/HT204837
[35] https://www.kaspersky.com

When wireless hotspots are accessible, nobody wants to use up their cellular data, yet free Wi-Fi networks are frequently insecure[36]. Three British politicians who consented to participate in a free Wi-Fi security experiment, were readily compromised by cyber specialists[37]. Their VoIP chats, PayPal transactions, and social media accounts were all compromised and hacked. Use free Wi-Fi on your mobile device carefully for safety. Additionally, never use it to access private or confidential services, such as banking or credit card details.

5.2. NETWORK SPOOFING

In high-traffic public spaces like coffee shops and airports, hackers put up phony access points—connections that appear to be Wi-Fi networks but are traps. To entice people to connect, cybercriminals give the access points familiar names like "Free Airport Wi-Fi" or "Coffeehouse." Even attackers need users to register for an "account," replete with a password, to access these free services. Hackers can access users' email, e-commerce, and other secure information since many users use the same email and password combination for several services. Never give out personal information when connecting to any free Wi-Fi, in addition to exercising caution. And always create a special password anytime you are prompted to do so, whether it be for Wi-Fi or any other program[38].

5.3. PHISHING ATTACKS

Mobile devices are the target of the majority of phishing attacks since they are constantly on. Because they frequently check their email in real-time, reading and opening emails as they arrive, mobile users are more exposed. Due to the lower screen sizes, email programmes on mobile devices display less information, making users more vulnerable. For instance, unless you extend the header information bar, an email may just show the sender's name even after it has been opened. Never click on links in emails you don't recognise. Let the response or action items wait till you are at your computer if the problem is not urgent. Here are some more information about phishing attacks and how to prevent them: https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

5.4. SPYWARE

Although many mobile users are concerned with malware sending data streams back to hackers, spyware poses a more immediate threat. Users should often be concerned about spyware

[36] https://whatismyipaddress.com/unsecured-network-2
[37] https://securityaffairs.co/wordpress/38510/cyber-crime/3-uk-politicians-hacked-Wi-Fi.html
[38] https://www.techtarget.com/searchsecurity/definition/IP-spoofing

deployed by partners, coworkers, or employers who want to monitor their movements and behavior rather than malware from unknown attackers. Many of these programs, often referred to as stalkers, are made to be installed on the target's smartphone without their knowledge or consent. This type of application requires slightly different handling than other malware due to how it enters your device and its goal. Thus a thorough antivirus and malware detection suite should use specialist scanning techniques[39].

5.5. BROKEN CRYPTOGRAPHY

When app developers utilize ineffective encryption techniques or improperly deploy strong encryption, cryptography can become broken. To hasten the app development process in the first scenario, developers may choose to employ well-known encryption techniques in spite of their acknowledged security flaws. Because of this, any determined attacker can take advantage of the flaws to break passwords and get access. In the second case, programmers employ extremely safe algorithms but leave additional "back doors" accessible that reduce their efficacy. For instance, the hackers may not be able to guess the passwords, but if developers introduce bugs in the code that let attackers change high-level app features—like sending or receiving text messages—they might not even require passwords to cause issues. Before apps are released, it is the responsibility of companies and developers to enforce encryption standards[40].

5.6. IMPROPER SESSION HANDLING

Many apps employ "tokens," which let users execute many operations without having to re-authenticate their identities to support ease of access for mobile device transactions. Tokens are created by apps to identify and validate devices, just like passwords are for people. With each access attempt or "session," secure apps create new tokens that should be kept private. The Manifest claims that inappropriate session handling happens when programs unintentionally share session tokens, such as with malicious actors who can then pose as genuine users with them. This frequently happens as a result of a session that is still active after the user leaves the app or website. A cybercriminal would have unrestricted access to the website and other related areas of your employer's network if, for instance, you logged into a workplace intranet site from your tablet and forgot to log out when you finished the assignment[41].

5.7. WHAT THREATS TO MOBILE SECURITY WILL EMERGE NEXT?

[39] https://www.malwarebytes.com/spyware
[40] https://knowledge-base.secureflag.com/vulnerabilities/broken_cryptography/broken_cryptography_category.html
[41] https://owasp.org/www-project-mobile-top-10/2014-risks/m9-improper-session-handling

Despite becoming a favorite target for hackers, mobile security is not given the same priority as network and PC security. Even inside the mobile ecosystem, security investment was chronically underfunded in comparison to mobile app development, according to a Harvard Business Review analysis. As our reliance on mobile devices increases, the value of data also rises, which gives hackers more incentive. Be on the lookout for additional threats targeted at the following three major impact areas in addition to the mobile security dangers we just discussed[42]:

SMiShing[43]: Cybercriminals use SMiShing, a technique similar to phishing scams, to try to get users to download malware, click on harmful links, or reveal personal information. Instead of email, a SMiShing attack is launched through text texts.

BYOD[44]: As high-level access to personal mobile devices is made available to corporate users, smartphones and tablets are essentially taking the place of desktop computers for many business operations. Personal mobile devices, however, don't provide the same level of integrated security or control as the desktop PCs owned by the enterprise that they are replacing.

The Internet of Things (IoT)[45]: Because the variety of smart devices is expanding so quickly, from RFID chips to thermostats and even household appliances, it is not always possible for users or antivirus programs to keep an eye on them. Because of this, IoT devices are a desirable target for hackers who utilize them as points of entry into bigger networks[46].

6. PROTECTING YOUR PASSWORD[47]

Your passwords are the most frequent method a computer hacker will use to harm you. Online companies frequently require us to update our login information and select passwords that adhere to tight security standards. When the password you wish to use is too short and lacks a special character, a number, and a capital letter, this might be frustrating. Although security instructions may be inconvenient, they are there for your protection. You must comprehend the significance of secure passwords before we offer simple answers to these needs. While setting your password:

- Don't depend on Windows passwords to keep your information secure. They are quickly destroyed.

[42] https://www.securitymagazine.com
[43] https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it
[44] https://www.freshbooks.com/hub/other/what-is-byod?ref=&campaignid=16988866217&adgroupid=&targetid=&crid=&dv=c&geo=9000786&ntwk=x&source=GOOGLE&gclid=Cj0KCQjw08aYBhDlARIsAA_gb0csfHZJ8sfHlpNIE7kwIyt5Th03upAvoO25MO8M-xwJTmXzipAZfSUaAnnPEALw_wcB
[45] https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT
[46] https://www.kaspersky.com
[47] https://www.ibm.com/docs/en/zos/2.4.0?topic=security-what-is-password-protection

- Make passwords that are at least eight characters long. A succinct sentence can also be used as your password.
- Instead of using a short, obvious password, it is preferable to write down your passwords and save them securely.
- Make your password up of symbols, capital letters, small letters, and digits.
- Use a different password each time.
- Use secure passwords that are not closely connected to your personal interests or way of life.
- Never divulge or disclose your key passwords with anyone.
- Every three to six months, change your passwords.
- Keep in mind that a variety of free online tools are available to help you find your Windows password, wireless network encryption, and pretty much any other kind of computer password you might have.

6.1. PASSWORD ATTACKS[48]

Many of us make use of the security functions offered by well-known software programs. You can use a password to secure a file or software from companies like Microsoft, Quicken, Adobe, and others. Microsoft Office programs like Microsoft Word are a typical illustration of this. This word processor offers a security feature that allows you to password-protect any document. Anyone attempting to open the document will be prompted for the password, and until the proper password is entered, no content will be seen in the document. Only honest people will be kept out by this security measure, which is merely a layer. The password can be taken using one of two techniques.

Using computers effectively requires using strong passwords. Whether it's an email account, network login, or online banking, they serve as a security barrier by authenticating access to the necessary service. You are allowed to use various passwords for various accounts. This makes getting in more challenging. Because of this, in a technical sense, the information your passwords defend should be as secure as the priciest safe. A strong password is the most important component of any system when it comes to digital security. The most frequent way that hackers and attackers target your information systems is via cracking passwords, according to history.

6.2. PROFILING

Profiling entails generating an educated estimate about the individual who has the password by gathering facts and personal data about them. Our passwords typically represent something that is simple for us to remember, such as our birth year, a special someone's name, our hometown,

[48] https://securityboulevard.com/2022/05/what-is-a-password-attack-in-cyber-security/

our favourite football team, etc. These and other like facts are taken into account by the profilers. They might notice the books on your bookcase if they have access to your office. Since there are so many passwords you can remember that are difficult to memorise and have no connection to you. However, the most popular approach to breaking into a system that remains incredibly effective for determined hackers is password guessing by knowing personal information about the user.

6.3. SOCIAL ENGINEERING

Through ingeniously crafted scenarios and questions, many people have been duped into disclosing their passwords. It may take the form of a phone call from your ISP, who claims to be doing server upgrades and needs your password to make sure you don't lose any email in the process. Someone could pretend to be a coworkers from a different division of your company and ask for the password to the shared email account on the grounds that the owner is presently ill and needs to send things quickly. This practice is called social engineering. It is still a viable way for hackers to try to break into a system[49].

6.4. DICTIONARY ATTACKS

A dictionary attack entails inputting every word in a dictionary as a password in order to gain access to a password-protected computer, network, or other IT resource. A dictionary attack can also be used to try to decipher a communication or document that has been encrypted. A list of potential passwords will be used in this assault to attack the document. A number of sets of dictionaries are available for free online download, and this list is known as a dictionary[50].

6.5. BRUTE FORCE ATTACKS[51]

In most cases, this attack will be finished in under five seconds. This approach does not rely on a pre-loaded list of potential passwords. Instead, it will try each password—including ones with letters, numbers, and special characters—that is possible. Although it may seem unachievable, keep in mind the enormous processing power that is currently available on every computer. The application is defaulted to try passwords with four to ten characters because the majority of passwords do not have less than four characters.

[49] https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering
[50] https://www.hypr.com/security-encyclopedia/dictionary-attack
[51] https://www.kaspersky.com/resource-center/definitions/brute-force-attack

6.6. CREATING A STRONG PASSWORD

We now know that passwords like "apple," "Michael," and even "banana4" are insecure. Online services need more secure credentials because of this. Most websites will require a password that is at least eight characters long and contains a number and a special character. Some will insist on a capital letter as well. It could be challenging to come up with a password that is both simple to remember and fits these criteria. I advise using a series of passwords with a straightforward structure. Assume you have chosen to update the password for one of your online banking accounts and that you must comply with the password's security standards. If you must include "apple" in the password, think about using "Orange23$%18No." There are many ways to create passwords that are both hard to guess and simple to remember. Password managers are the best options. Please see 4.4. USE COMPLEX PASSWORD for password managers. Use a password manager, such as Dashlane[52], Sticky Password[53], LastPass[54], or Password Boss[55].

Your password is frequently the first and most crucial assurance of the protection of your data. It functions as the entrance to your home. It's like leaving the door open all night to use a poor password or none at all. Perhaps nobody will enter, or perhaps someone will steal everything you own. Be very careful about how you construct your passwords and where you store them.

1.1. PASSWORD AUTO SAVE

The majority of programs and operating systems try their best to make using them simple. Offering an auto-saving option for passwords is one way that web browsers and other apps accomplish this. For instance, most web browsers will ask you to save the password when you connect to a website and enter into an online account. You've given the browser permission to save the password on your computer when you select this option and input your password. Numerous programs have been developed to retrieve these passwords from this unencrypted data. Here, there is an easy fix. Never let software save your passwords on its own. You can modify this if your web browser currently logs you in when you visit a website automatically after you've given it permission to save your password. I will describe how to erase your passwords from Internet Explorer, Mozilla Firefox, Google Chrome, and Safari, even if I am unable to pinpoint how to do this for every application. The top four web browsers for Windows and Mac are listed here[56].

[52] https://www.dashlane.com/
[53] https://www.stickypassword.com
[54] https://www.lastpass.com/features/password-generator
[55] https://www.passwordboss.com
[56] https://www.techadvisor.com/article/745824/is-it-safe-to-store-passwords-in-your-web-browser.html

1.1.1. INTERNET EXPLORER (IE)[57]

Select "Tools" from the menu bar, and then select "Internet Options." This will bring up a new window with a number of choices. Click the "Delete" button under "Browsing History" on the "general" tab. Your temporary files, history, cookies, saved passwords, and data from web forms will all be deleted as a result.

1.1.2. MOZILLA FIREFOX[58]

Click "Tools" and then "Options" in the menu bar. You should see a section labeled "Passwords" under the "Security" menu. A new window will open when you click "Saved Passwords," displaying all of the saved passwords on that computer. You can delete any saved passwords by clicking "Remove All." When finished, click "Close" and, in the "Options" window, uncheck "Remember passwords for sites."

1.1.3. GOOGLE CHROME[59]

Click "Settings" on the menu bar located in the top right corner of the screen. This will bring up a new page with a number of choices. Click "Show advanced settings" at the bottom of the page after scrolling there. More options, including a section for passwords, will load as a result. "Manage stored passwords" can be selected. You'll be able to do this to remove your passwords from storage. To safeguard yourself from numerous password attacks in the future, uncheck the box next to "Offer to keep passwords I type on the web" after you are done.

1.1.4. SAFARI[60]

Select "Preferences" from the menu after clicking "Safari" in the menu bar. A new window containing numerous options will pop up. You may see all of your saved passwords by selecting the "Passwords" option. A "Remove All" button can be found at the bottom of this window. When you click this, the saved passwords are deleted.

1.2. AUTO LOGIN

Operating systems also provide you the choice of saving your password and logging in automatically. This is both incredibly useful and quite risky. This might be acceptable if your

[57] https://www.microsoft.com/en-ca/download/internet-explorer.aspx
[58] https://www.mozilla.org/
[59] https://www.google.com/chrome/
[60] https://www.apple.com/ca/safari/

computer is the only one in use and the system is locked away in a location that only you can access. But if other people occasionally have access to your computer, that might be dangerous. All of your documents and private information are stored on your computer. Nothing prevents someone from stealing your data if your computer automatically logs in as you do when you turn it on. By enabling a password on your user account, you can make this more challenging.

7. PROTECTING YOUR WEBSITE PRIVACY

7.1. BROWSERS[61]

Your internet connection information and online activity are regularly collected by web browsers. Regularly a standard web browser is gathering and saving data about your connection and online activities. It sends the following data to the websites you visit:

- you IP address;
- Your device's type;
- your browser's name;
- your cookie settings;
- Your browser's add-ons;
- The clicks and movements of your mouse;
- Your location and time zone; and
- Your screen resolution and battery level are some additional fundamental details.

The majority of this data may seem unimportant, but when aggregated, it yields a singular digital fingerprint that websites may use to recognize and monitor you online. Your browser fingerprint will be visible to websites and third-party analytics even if you have removed your cookies (little data files that websites store on your device), history, and cache or are using an incognito/private window. This might establish clear connections between you and your activism. You might believe that all it takes to prevent tracking is a simple change to your browser's privacy settings. In fact, this might increase the uniqueness of your browser fingerprint.

7.2. THE BEST BROWSER FOR PRIVACY MAINTENANCE [62]

There are several browsers available. The best are the following seven, but the most secure one is Firefox compared with Chrome, Edge, Safari, Opera, Brave, and Internet Explorer.

[62] https://www.mozilla.org/en-CA/firefox/browsers/compare/

7.3. How to use a browser safely

7.3.1. CLEAN & CLICK

With a single click, shut down every browser you currently have. This includes form data, cookies, cache, passwords you've already saved, and your browser's and download history.

7.3.2. PUBLICITY BADGER

Block trackers and instantly recognize suspicious activity on the websites you visit. Anything against user consent is blocked.

7.3.3. VPN CYBERGHOST

You can hide your IP address with the help of a VPN service. It doesn't keep any activity logs and also disables all online tracking.

If you don't want to switch web browsers, there are other ways to reduce tracking and data storage on your online activity, such as: Limiting the number of cookies you accept; configuring your browser to block tracking ads and invisible trackers, and routinely clearing your cache and cookies to reduce your risk of being tracked.

These procedures are useful, but they won't significantly change the fingerprint of your browser. As was previously noted, changing a few settings may actually make your browser's digital fingerprint appear even more distinctive to the websites you visit.
Utilizing the Tor network is a good approach to reduce the chance of your browser being fingerprinted. No matter what device or operating system is being utilized, every Tor user should have the exact same browser fingerprint. You can use the Tor Browser or modify a browser to access the Tor network.

7.4. PREFERRED AND SECURE BROWSERS FOR ACTIVISTS

7.4.1. BROWSER TOR

With the assistance of pre-configured security mechanisms and relay servers, Tor, arguably the most well-known privacy-focused browser, prevents unauthorized snooping.

7.4.2. EPIC[63]

The default option for privacy is on. The browser will disable cookies, trackers, and advertisements when using the private search engine DuckDuckGo. Your login information, browsing history, and other information are also not stored.

7.4.3. FIREFOX

Thanks to privacy protections that guard you against tracking, viruses, and cryptominers, it's one of the safest browsers out there. Additionally, it is frequently updated to help control threats.

7.5. SEARCH ENGINES

Your every internet move is tracked by Google and other search engines[64]. They frequently and may transfer user data to third parties. How much information Google and other search engines have about you might surprise you. They gather a ton of information to provide targeted adverts and customize your web browsing.

7.5.1. WHAT GOOGLE KNOWS[65]

7.5.1.1. ABOUT YOU

Google is aware of your name, age, gender, facial and voice recognition data, fitness information, political views, and religion. How it knows, through the process of registering for Google, Google Search, Google Fit, and Google Assistant

7.5.1.2. WHERE ARE YOU

Google is aware of your current location as well as your past, present, and future whereabouts. Your mode of transportation and location queries are also known to Google. How it knows, through Waze and Google Maps

7.5.1.3. WHO YOU SPEAK WITH

Your discussions, appointments, images, movies, and anything else you've posted to Drive are all known to Google. Sensitive data, including march routes, boycott or strike planning, correspondence, and petitions, may all be accessible to Google. How it knows, through Google Drive, Google Calendar, Google Hangouts, and Gmail

[63] https://www.epicbrowser.com
[64] https://www.lifewire.com/best-search-engines-2483352
[65] https://www.businessinsider.com/what-does-google-know-about-me-search-history-delete-2019-10

7.5.1.4. WHO YOU ARE

Google is aware of the books, articles, and movies you've read, watched, purchased, and searched. How it knows, through Google News, YouTube, Google Search, and Google Shopping Ads, Google Books

7.5.1.5. WHAT YOU SEARCH

Google is aware of the history of the websites you've visited, including any saved usernames and passwords.

7.5.2. HOW TO USE CHROME[66]

You should be aware that the majority of search engines can be forced to turn over your search and browsing history by law enforcement or government officials. Consider what this would entail for you as an activist if you frequently look up information about dissidents and government figures, as well as legal aid and international organizations.

We are aware that Google is the most popular search engine. But when it comes to tracking and collecting user data, it's one of the worst. The Associated Press recently discovered that Google continues to track your whereabouts even if you turn off the "Location History" option.

7.6. THE PREFERRED SEARCH ENGINES FOR PRIVACY

7.6.1. DUCKDUCKGO[67]

It is confidential and simple to use. Neither cookies nor user data are gathered by it. Additionally, it cleans the servers' IP logs. You can access DUKDUCKGO at: https://duckduckgo.com/?va=b&t=hc.

7.6.2. METAGER[68]

The German multilingual search engine places a strong emphasis on protecting user privacy and neither profiles nor collects data about its users. Use Tor to directly access MetaGer. You can access MetaGer at: https://metager.org.

[66] https://support.google.com/a/users/answer/9310344?hl=en
[67] https://duckduckgo.com/?va=b&t=hc
[68] https://metager.org

7.6.3. STARTPAGE[69]

It offers a comfortable but private surfing experience by using Google technology without tracking. Startpage does not record any user information or divulge it to outside parties. You can access Startpage at: https://www.startpage.com.

8. PROTECTING YOUR DATA PRIVACY

Activists frequently possess vital information, and many have access to a multitude of materials that might further their objectives. These assets, which are kept in the form of data, are susceptible to malicious attacks from all parties.

One alternative for safely keeping your data is on encrypted flash drives (memory sticks) or hard disks, but doing so may leave your information even more susceptible to theft, loss, or technological difficulties. The storage capacities of physical devices are also limited.

Cloud storage has become crucial as a result. Data in the cloud is also more sharable, which is crucial for activists who need to disseminate information to further their causes.

8.1. CLOUD STORAGE

The majority of significant cloud storage providers may be required to give law enforcement access to your data.

You have to be warned that your cloud storage provider offers data encryption doesn't imply your privacy is ensured. Adamant prosecutors may force huge cloud firms to collaborate, and encryption alone won't protect against this since some services have been known to exchange data and files with government spy organizations like the National Security Agency (NSA) in the United States.

8.1.1. HOW TO SECURE CLOUD STORAGE

By selecting a cloud storage provider that encrypts your files locally on your device before they are uploaded to the cloud, you can protect your cloud storage (as opposed to files that are encrypted in transit to the cloud). Keep in mind that providers may have access to encryption keys and may be able to decrypt your files or give them to the authorities if necessary.

[69] https://www.startpage.com

It is strongly advised that you manually encrypt your data before submitting them to a cloud service. So long as you never upload the encryption keys with your files, you will be the only one who has the key to decrypt your data.

There are several commercial and free encryption programs available, but make sure they are compatible with your devices and your cloud storage provider. Make sure the program uses end-to-end encryption, which ensures that your files are encrypted from the moment they leave your smartphone until you can access them once more.

8.2. SHARING DATA

The app Veracrypt (https://veracrypt.fr/) allows users to save encrypted containers (folders) on hard drives and online storages, Google Drive or Dropbox, which to outsiders look like normal or system files. This is done to ensure the security of your documents while being stored on your computer before uploading them for online sharing and storage. To prevent the program from attracting notice, choose to delete the application after using Veracrypt to encrypt a document like this even from the Trash Bin. For secure end-to-end encrypted alternatives for file sharing, see below choices:

- https://cryptpad.fr/drive
- https://ufile.io
- https://send.tresorit.com
- https://send.tresorit.com

9. PROTECTING YOUR SOCIAL MEDIA AND COMMUNICATIONS

9.1. HOW TO USE SECURE COMMUNICATION

Activists frequently exchange private information with other activists, groups, lawyers, and journalists. The greatest approach to conducting a truly private chat is face-to-face communication, but this is obviously not always possible.

It is best to use encrypted communication services like Signal, Wire, and Keybase when conversing online. In this method, end-to-end encryption is used to protect what you say.

Please be aware that Telegram has had data breaches and that end-to-end encryption is not by default enabled, with the exception of "private chats" and audio and video calls. Email service

providers may be compelled to give authorities your information. You may be exposed to murky social media privacy policies.

9.2. EMAILS

The majority of well-known email companies are quite secure and have strict mechanisms in place to guard against data leaks. These procedures, however, are not error-free and or fail-proof. It's unlikely that security measures will keep you safe if your email provider is required to turn over information in your emails by government authorities.

9.2.1. KEEPING YOUR EMAIL IDENTITY PRIVATE

You should take extra precautions to preserve your privacy to reduce the likelihood that governmental agencies will snoop through your correspondence. The most practical approach is to use a private email service like ProtonMail[70], Fastmail[71], or Zoho Mail[72] because encrypting emails takes time and effort.

Rise Up[73] and Aktivix[74], secure email services created for activists, are free since they are supported by donations. They may not, however, support as many saved emails as commercial providers, so you may want additional email management, such as achieving older emails in a secure cloud storage facility.

It's better to completely maintain your personal email accounts and email accounts for activism separately. This prevents an account that has your personal, identifiable information from being connected to the account(s) you use to plan events or interact with other activists.

9.2.2. EMAIL SAFETY

Phishing is a form of scam when online crooks or other snoops pretend to be reliable businesses or individuals you know, typically by email. The purpose is to con users into disclosing their private emails or other information. To convince you to download malicious software or click on links that appear to be legitimate, con artists may also entice you. Never click on links or downloads sent to you via email by an unknown sender. Make sure the email address is legitimate by double-checking it. Do not click any links in an email that informs you of a problem with a particular account. It's

[70] https://account.proton.me/login
[71] https://www.fastmail.com
[72] https://www.zoho.com/mail/
[73] https://account.riseup.net
[74] https://en.exp.activix.ca/users/sign_in

preferable to go straight to the service's website or app. Please be aware that any of these techniques could be used by bad actors that target activists to access your email accounts[75].

9.3. SOCIAL MEDIA

The companies behind the most well-known social apps and sites have been dogged by controversy, especially with regard to privacy and security, despite the fact that social media offers some of the most useful tools for activists — mass engagement for movements and causes, event promotion, or outreach and campaigning, for example.

For instance, the Cambridge Analytica controversy in recent years highlighted how Facebook permitted the collection of personal information from millions of users. Such privacy violations highlight how much information social media has about you. The information you disclose on these networks is obviously not as private as you might believe.

Geotagging is frequently used in social media to pinpoint your precise location. Facebook tracks more than just your location; it also logs your purchases, web searches, and contacts. The platform constantly asks for access to your contacts, call history, and SMS because of this.

9.3.1. IMPORTANT INFORMATION ABOUT FACIAL RECOGNITION

Pervasive and involuntary facial tagging raises the risk of surveillance. Facial recognition software is embedded into social media photo-sharing systems. Platforms are accumulating massive user face image collections. Social networking sites commonly provide face profile information to authorities. Once you upload a photo, it becomes the platform's property. There is no way to opt-out of the current face recognition systems. You're in, once you're in.

Your personal information isn't safe with Facebook or other social media platforms, as they have repeatedly shown. Your privacy is at stake the more personal information you post on social media. For well-known campaigners, choosing between participation and visibility is a two-edged sword.

9.3.2. CHANGE SOCIAL MEDIA SETTINGS

To guarantee optimal anonymity as an activist, you should always change your privacy settings from the platform defaults. You will be able to control who can see your profile, posts, location, photographs, and contact details, as well as whether or not people can tag you or find you in profile searches because of this.

[75] https://www.tripwire.com/state-of-security/featured/essential-tips-for-keeping-your-email-safe/

You could also improve the security settings on your social media accounts. You can configure two-factor authentication here, ban user profiles, and sign up for notifications whenever an unauthorized attempt is made to access your account.

9.3.3. SETTING UP A SECURE ACCOUNT ON SOCIAL MEDIA

If you want a secure account on social media:

- Never use your complete or true name.
- Use a different email address when you register than your real one.
- Give only the information that is required.
- Select a profile photo that neither physically nor through meta tags can be used to pinpoint you or your location.
- Set up two-factor authentication and select a secure complex password.
- Choose fictitious responses for the password recovery areas, then save your selections in a password manager.
- Install a browser extension that disables third-party cookies and trackers.

You might need to delve into the terms and conditions or privacy rules to properly comprehend your social media settings, which can be time-consuming and difficult.

The portions that explain how your data is used when it is given to third parties and how the platform reacts to demands from law enforcement are, it should be noted, the most crucial ones.

Also, keep in mind that privacy settings can change. Check for updates to determine whether any previously private information may now be shared, but also look for any new options that can give you more privacy control[76].

10. SECURITY AND SAFETY OF SOCIAL MEDIA PLATFORMS AND COMMUNICATION TOOLS

We outline some of the social media platforms and communication tools that are widely used in Afghanistan under this category. We refrain from going into detail on every one of these widely utilized platforms and tools. Facebook, Twitter, Instagram, TikTok, and YouTube are the most popular social media platforms in Afghanistan. Gmail, Yahoo, Messenger, WhatsApp, Viber, Telegram, Skype, Zoom, and Signal are the most popular social media communication tools. Under this title, we refrain from repeating the aforesaid important points in this manual. Please read through all of the chapters in this manual if you wish to utilize the social media platforms and

[76] https://www.mcafee.com/blogs/privacy-identity-protection/how-to-protect-your-social-media-accounts/

communication tools listed below in a secure manner and retain your privacy, as we won't be rehashing many of the important points from the other chapters.

10.1. SIGNIFICANT POINTS OF SOCIAL MEDIA PLATFORMS

10.1.1. Facebook

- Two-factor authentication helps protect your Facebook account. It is a security feature designed to safeguard your account and log in. How to activate: https://www.facebook.com/help/148233965247823
- You can control who can find you on Facebook. You can control the search engines and Facebook search. How to activate: https://www.facebook.com/help/1718866941707011
- You can turn off your location on Facebook. How to activate: https://www.facebook.com/help/275925085769221
- If you need more privacy on Facebook, lock your profile. How to activate: https://www.facebook.com/help/196419427651178
- Utilize a password manager and use a complex password. Randomly, change your password. Never use the same password across many websites. Useful password managers:

  https:/www.dashlane.com
  https://www.stickypassword.com
  https://www.lastpass.com/features/password-generator
  https://www.passwordboss.com
- Log into your Facebook account safely if using a computer that is not yours. You can use a Virtual Private Network (VPN) for more private use of internet. First, verify the security of the browser. Do not select remember the password option. Once you're finished, log out of the account.
- Be on the lookout for phishing assaults. Never let fraudulent accounts trick you into giving over your account sign-in information. They usually send out phony messages requesting a password reset.
- Change your password if your account has been compromised. Visit the help link if you are unable to change your password. More information: https://www.facebook.com/help/203305893040179
- Control your timeline, posts, and tags. How to do this: https://www.facebook.com/help/203305893040179
- Please do not leave your phone unlocked or give it to someone else. Facebook accounts are readily accessible on the majority of phones. Therefore, anyone who has access to your cellphone can access your account.

- Avoid phishing scams and clicking on any suspicious link. Instead, only click on a link after confirming its authenticity. More information: https://www.facebook.com/help/166863010078512

10.1.2. Twitter

- Two-factor authentication helps protect your Twitter account. It is an extra layer of security for your Twitter account. How to activate: https://help.twitter.com/en/managing-your-account/two-factor-authentication Please do not leave your phone unlocked or give it to someone else while you have two-factor authentication activated.
- Use a password manager. Create a complex password and change it repeatedly. Never use an old password and the same password for several accounts. Useful password managers:
  https:/www.dashlane.com
  https://www.stickypassword.com
  https://www.lastpass.com/features/password-generator
  https://www.passwordboss.com
- Manage your tweets, whether to be public or private. You can control the privacy of your tweets.
  https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public
  https://help.twitter.com/en/safety-and-security/public-and-protected-tweets
- Control your tweet location and hide your account country location.
  https://help.twitter.com/en/using-twitter/tweet-location
  https://help.twitter.com/en/managing-your-account/how-to-change-country-settings
- Log into your Twitter account safely if using a computer that is not yours. You can use a Virtual Private Network (VPN) for more private use of internet. First, verify the security of the browser. Do not select remember the password option. Once you're finished, log out of the account.
- If your account has been compromised, but you still can log in, you will be able to secure your account and stop avoided behaviors. If you are not able to log in to your account, go to help with a potentially hacked account. How to do this: https://help.twitter.com/en/safety-and-security/twitter-account-compromised
- By default, users can use your email address and phone number to find you on Twitter. In addition, search engines can also discover your Twitter. You can control your discoverability by email, phone, and on search engines. How to activate:
  https://help.twitter.com/en/safety-and-security/email-and-phone-discoverability-settings
  https://help.twitter.com/en/safety-and-security/remove-twitter-profile-from-google-search

- You can control your tweets and use Twitter safely by activating and deactivating (Tagging, Discoverability, Adds and Data Tracking, the Quality Filter, Hide Sensitive Content, Block and Mute Accounts, Mute Words, Shut Down your DMs and Reporting Accounts). How to activate and deactivate: https://help.twitter.com/en/safety-and-security/control-your-twitter-experience

10.1.3. INSTAGRAM

- Two-factor authentication helps protect your Instagram account and your password. It is a security feature which is necessary for your account security. How to activate: https://help.instagram.com/566810106808145
- Use a password manager. Create a complex password and change it randomly. Never use an old password and the same password for several accounts. Useful password managers:
  https:/www.dashlane.com
  https://www.stickypassword.com
  https://www.lastpass.com/features/password-generator
  https://www.passwordboss.com
- Control over who follows you on Instagram, who sees your Instagram photos, and who can comment on them. Additionally, you may control who has access to your Instagram account. How to activate and deactivate: https://help.instagram.com/116024195217477
- Control your privacy settings and information. how to do it: https://help.instagram.com/196883487377501
  https://help.instagram.com/377830165708421/?helpref=hc_fnav
- If your account is compromised. There are numerous steps you may be able to do using the website or the app to secure your account if you believe your account has been hacked or compromised. How to do this: https://help.instagram.com/149494825257596
- You can block users on Instagram. There are numerous ways to block an individual on Instagram. https://help.instagram.com/426700567389543/?helpref=hc_fnav
- You can report spams, inconvenient posts, comments, or individuals that are violating Instagram's community policy while you notice them by using Instagram's built-in reporting features. How to do this: https://help.instagram.com/165828726894770/?helpref=hc_fnav

10.1.4. TikTok

- Before using TikTok, you can read its four safety guides, Ads and Your Data, Well-being Guide, New User Guide, and Guardian's Guide. You can find the guides here: https://www.tiktok.com/safety/en/
- Two-step authentication, which TikTok enables, makes it necessary to provide additional verification each time you log in. It keeps your account and password safe. Here is how to

activate two-step authentication: https://www.tiktok.com/safety/youth-portal/keep-your-account-secure?lang=en

- To create a password, use a password manager. Create a complex password and change it usually (https://support.tiktok.com/en/log-in-troubleshoot/log-in/reset-password). Never use an old password and the same password for several accounts. Password managers, which can help you:

  https:/www.dashlane.com
  https://www.stickypassword.com
  https://www.lastpass.com/features/password-generator
  https://www.passwordboss.com

- You can have a private account, but only individuals you allow can follow you, watch your videos, LIVE videos, bio, likes, as well as your following and followers lists. Other users won't be able to Duet, Stitch, or download your videos if you have a private account. Here is how make your account private and or public: https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/making-your-account-public-or-private
- You can limit who can search you on TikTok and search engines. Go to the settings option in the top right corner of your profile if you wish to restrict who can access your TikTok account. https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/suggested-accounts
- For more Privacy, you need to turn off your location on TikTok. Here is How to turn off location services in TikTok: https://support.tiktok.com/en
- Avoid phishing scams. Attackers often use fraudulent messages, also known as phishing, to persuade victims to divulge sensitive information including passwords, credit card numbers, social security numbers, and other personal information. Email, SMS (text message), in-app communications, and messaging apps can all be used to send fraudulent messages. You can find how to avoid phishing here: https://support.tiktok.com/en/safety-hc/account-and-user-safety/avoid-fraudulent-message-attacks-on-tiktok

10.1.5. YouTube

- Use two-factor authentication or two-step verification to increase the safety and security of your Google accounts, including your YouTube account. By doing this, you can strengthen the security of your account in the event that your password is compromised. Once activated, you can access your account using either your phone or your password. Here is how to do it: https://support.google.com/accounts/answer/185839?hl=en&co=GENIE.Platform%3Ddesktop
- Turn on YouTube's Safety Mode by tapping the Safety Mode setting on YouTube. This function can assist in filtering out possibly objectionable mature content that you or other users of your devices may want to avoid seeing. Here is how to do it:

https://support.google.com/youtube/answer/174084?hl=en&co=GENIE.Platform%3Ddesktop

- Use a password manager and create a complex password. Randomly, change your password. Never use the same password across many websites. Password managers which can help you have a strong password:
  https:/www.dashlane.com
  https://www.stickypassword.com
  https://www.lastpass.com/features/password-generator
  https://www.passwordboss.com
- Log into your YouTube account safely if using a computer that is not yours. You can use a Virtual Private Network (VPN) for more private use of internet. First, verify the security of the browser. Do not select remember the password option. Once you're finished, log out of the account.
- A compromised YouTube account can be fixed. YouTube is the property of Google. If you assume your YouTube account on Google may have been hacked, taken over, or somehow compromised, to recover your Gmail or Google Account, you can follow some instructions to recover it. Here is how to recover it: https://support.google.com/youtube/answer/76187?hl=en
- YouTube is the property of Google. You can improve the safety of your YouTube account by strengthening the security and safety of your Gmail account linked to your YouTube. https://support.google.com/youtube/answer/76187?hl=en#zippy=%2Crequired—step-verification-for-creators-in-the-youtube-partner-program
- Safe your account from shady communications and information. Phishing is when a hacker poses as a reliable individual to steal personal information. Personal data may consist of:
  - fiscal information
  - Social Security Number/National ID
  - numbers on credit cards
  - Hackers may utilize emails, texts, or websites to pose as organizations, relatives, or coworkers.

  Notice your password, email address, or any other account information will never be requested by YouTube. If someone contacts you acting to be from YouTube, don't fall for it.
  https://support.google.com/youtube/answer/9701986?hl=en&ref_topic=7071231
- if you feel insecure and unsafe, hide and or delete your YouTube channel You have the option of completely deleting your channel or temporarily hiding some content on it. Note that your community posts, comments, and replies will be permanently deleted if you hide or deactivate a YouTube channel.
  https://support.google.com/youtube/answer/55759?hl=en&ref_topic=7071231
- Finally, as aforesaid, keeping your YouTube account secure reduces the risk of it or your channel being hacked, taken over, or compromised. Learn how to safeguard your account

if you believe it has been compromised. Below are the most important steps in securing your account:

- Create a complex password and remember it.
- Protect your password against hackers.
- Keep track of your passwords.
- Don't use an old password.
- Don't use the same password for numerous accounts.
- Never divulge your sign-in details.
- Conduct routine security checks.
- Update or add options for account recovery
- Set 2-Step Verification on.
- Remove suspicious users from your account and remove unnecessary websites and programs
- Update your software, and create account backups
- Stay away from suspicious requests
- Stay away from suspicious websites
- Report phishing or spam.

10.2. SIGNIFICANT POINTS OF SOCIAL MEDIA COMMUNICATION TOOLS

10.2.1. Gmail

- Avoid using your full name in your Gmail account. You should keep your first and last names private on Gmail. A false name or your pen name must be provided. https://support.google.com/accounts/answer/6304920?hl=en&co=GENIE.Platform%3DDesktop
- Use a password manager and create a complex password. Randomly, change your password. Never use the same password across many websites. password managers which can help you have a strong password:
  https:/www.dashlane.com
  https://www.stickypassword.com
  https://www.lastpass.com/features/password-generator
  https://www.passwordboss.com
- Managing your online privacy on all Google services is your priority. Some information on your Google Account can be made public or private. You may then decide who can access information like your birthday or phone number across all Google services. https://support.google.com/accounts/answer/6304920?hl=en&co=GENIE.Platform%3DDesktop

- Two-factor authentication is key factor in securing your Gmail and or google accounts. Use two-step verification/ two-factor authentication to secure your google accounts. Add another layer of protection to your account to keep hackers out. When you sign in, 2-Step verification aids in ensuring the privacy, security, and safety of your personal information. https://support.google.com/accounts/answer/185839?hl=en&co=GENIE.Platform%3DAndroid
- Log into your Gmail account safely if using a computer that is not yours. You can use a Virtual Private Network (VPN) for more private use of internet. First, verify the security of the browser. Brows in private. Do not select remember the password option. Once you're finished, log out of the account. For more information: https://support.google.com/accounts/answer/2917834?hl=en&co=GENIE.Platform%3DDesktop
- A compromised Gmail account can be fixed. If your Gmail may have been hacked, taken over, or somehow compromised, to recover your Gmail you can follow some instructions to recover it. Here is how to recover it: https://support.google.com/accounts/answer/6294825?hl=en
- Safe your Gmail account against phishing. Phishing is the use of phony emails, messages, advertising, or websites that mimic legitimate websites you often visit in an effort to steal personal information or gain access to online accounts. They usually:
    - Ask about your financial or personal details.
    - Ask you to download software or click on websites.
    - Pose as a reputable company, such as your bank, a social media platform you use, or your job site.
    - Pretend to be an individual you know, such as a relative, acquaintance, or coworkers.
    - Exactly like a message you would get from a source you trust.
- Use these tips to assist you in steering clear of misleading requests and messages.
    - Pay attention to Google's warnings.
    - Never provide personal information when requested.
    - Never input your password after clicking a message link.
    - Be wary of communications that seem urgent or too good to be true.
    - Before you click, stop and think.
    - To spot phishing emails, use Gmail.
    - Use Chrome's Safe Browsing feature.
    - Verify any suspicious saved passwords.
    - Protect your Google Account password by setting a 2-Step Verification.
    - Send a report to Google if you received a Phishing email.

  https://support.google.com/mail/answer/8253?hl=en
- Strengthen the security of your account. Google is committed to online safety. We strongly advise regularly carrying out the measures listed below in order to safeguard your Google Account.

- Perform a security check.
- A software update.
- Use secure, one-of-a-kind passwords.
- Remove any unnecessary browser extensions and apps.
- Defend against shady messaging and content.

https://support.google.com/accounts/answer/46526?hl=en&ref_topic=7189123

please note that Google and Yahoo do not offer the most secure email services. None of them encrypt your messages end-to-end.

10.2.2. Yahoo

- Avoid using your full name in your Yahoo account. You should keep your first and last names private on Yahoo. A false name or a sending name must be provided. In Yahoo Mail, alter your sending name by using the following steps:
  - Login to Yahoo Mail;
  - Click the Settings menu icon;
  - Tap Mailboxes;
  - Choose the account that needs editing;
  - To change or remove your sending name, click the "Your name" link; and
  - Press Save.

  https://help.yahoo.com/kb/SLN28072.html
- Your first line of defense against hackers and imposters is a strong password. Here are some helpful hints for making a strong password that will keep your data safe. To Create a strong password:
  - Use unique words;
  - Have 12 or more characters;
  - Don't be obvious by using personal information like your name, your Yahoo ID, your birthday, etc.;
  - Avoid sequences or repeated characters;
  - Use a different password for each account;
  - Use a passphrase;
  - Don't recycle old passwords;
  - Use antivirus software for your computer;
  - Keep your password fresh by Changing it regularly;
  - Look for yahoo.com to log in;
  - Be cautious - If you're being asked to change your password;
  - Type out the URL into your browser's address bar instead of clicking a link in an email; and

- Use Yahoo Account Key - If you're concerned about your password being stolen.

https://in.help.yahoo.com/kb/SLN3012.html

You can also use a password manager by using the following links.

https:/www.dashlane.com
https://www.stickypassword.com
https://www.lastpass.com/features/password-generator
https://www.passwordboss.com

- Yahoo values your right to privacy. You can view and manage several aspects of how your information is used with Yahoo products via the Privacy Dashboard. https://in.help.yahoo.com/kb/viewing-managing-account-data-sln28671.html
- Enable two-step verification to demand a code in addition to your password when a login attempt is performed from a new device or browser. To use 2-step Verification, you must disable Yahoo Account Key if you currently use it to log in. https://help.yahoo.com/kb/SLN5013.html
- Log into your Yahoo account safely if using a computer that is not yours. You can use a Virtual Private Network (VPN) for more private use of internet. First, verify the security of the browser. Do not select remember the password option. Once you're finished, log out of the account. For more information: https://ph.help.yahoo.com/kb/sln5283.html?redirect=true
- If you assume your account has been compromised, follow the below steps to secure it.
  - Immediately, change your password;
  - Remove app passwords you don't verify;
  - Check to see if your recovery options are up to date;
  - Retreat your mail settings if changed;
  - Ensure you have antivirus software installed and updated in your PC; and
  - Use Account Key or two-step verification to ensure your account has an extra layer of security.

  https://help.yahoo.com/kb/SLN2090.html

please note that Google and Yahoo do not offer the most secure email services. None of them encrypt your messages end-to-end.

10.2.3. Messenger

- Use end-to-end encryption in your messenger. In a conversation, end-to-end encryption adds additional security and protection so that only you and the other person can see, hear, or read the messages and calls you exchange. Messenger no longer supports Vanish Mode. In an end-to-end encrypted chat, users can still send disappearing messages. https://www.facebook.com/help/messenger-app/1084673321594605

- In Messenger, you can manage your privacy by deciding who can see your Active Status, selecting the audience for your Stories, using secret conversations, and more. Here is how to manage your Messenger privacy.
  https://www.facebook.com/help/messenger-app/408883583307426?helpref=faq_content
- You can control who reaches your chat list. You will get a message request if someone sends you a message on Facebook, but you are not linked with them. Remember that responding to a message request establishes a connection between you and the sender and makes any content they sent you visible. Find out how to limit who in Messenger can start a new chat with you.
  https://www.facebook.com/help/936247526442073?helpref=related&source_cms_id=907368596013605
  https://www.facebook.com/help/messenger-app/2258699540867663?helpref=faq_content
- If there are individuals you don't want to hear from, block, hide, or mute them. You can control messenger notifications for all conversations. Find out how to mute, ignore, or block individuals in Messenger.
  https://www.facebook.com/help/messenger-app/204908296312159?helpref=faq_content
  https://www.facebook.com/help/messenger-app/1245152242249842?helpref=faq_content
  https://www.facebook.com/help/messenger-app/330627630326605?helpref=faq_content
- Avoid replying and report the scam to Messenger if you notice something you believe to be a scam.
  https://www.facebook.com/help/messenger-app/833709093422928?helpref=faq_content
- On your smartphone, you can lock the app. You can enable Messenger's app lock feature for your Android or iOS device to provide your Messenger account extra security and privacy.
  https://www.facebook.com/help/messenger-app/2585155295072006?locale=en_US&helpref=faq_content
- For more security and safety of messenger please visit: https://www.facebook.com/help/messenger-app/1064701417063145/?helpref=hc_fnav

Note: You may access Messenger using your Facebook account as it is linked to Facebook. Both Messenger and Facebook are property of Meta. Please refer to Facebook's details for additional information about the security and safety of your Messenger.

10.2.4. WhatsApp

- Never divulge your WhatsApp verification code to anyone. The SMS verification code issued to your phone number is required to take control of your account if someone tries to do so. Without this code, anyone trying to authenticate your phone number will be unable to do so and use your number on WhatsApp. This implies that your WhatsApp account is still under your control. https://faq.whatsapp.com/619670298808780/?locale=en_US
- Enable two-step verification and enter your email address so you may receive reminders if you lose your PIN. https://faq.whatsapp.com/585667085685460/?locale=en_US
- You can set a device code. It's not necessary to keep your phone connected in order to use WhatsApp on up to four connected devices at once. On WhatsApp, one phone at a time can be connected. https://faq.whatsapp.com/381777293328336/?locale=en_US
- WhatsApp offers end-to-end encryption for all messages you send and receive in order to ensure that only you and the person you're talking to can read or listen to your personal messages. Here is how to activate: https://faq.whatsapp.com/629089898272226/?locale=en_US
- The steps listed below could help you regain access to your WhatsApp account if you were tricked into disclosing your WhatsApp code and lost access to that. https://faq.whatsapp.com/690494414810591/?locale=en_US
- You can hide chats on WhatsApp if you need. You can better organize your talks by hiding a specific individual or group chat from your chats list using the archive chat feature. https://faq.whatsapp.com/154568698849853/?helpref=search&query=hide%20chats&search_session_id=a71f37c78ad24eb384f8975249d20c9f&sr=8
- For more details on safety and security of your chats on WhatsApp please visit: https://faq.whatsapp.com

10.2.5. Viber

- Viber features end-to-end encryption by default. Your device sends messages to the recipient's device as an encrypted code that only that device can decrypt using an encryption key to reveal as plain text. Only on user devices and nowhere else do encryption keys exist. Therefore, no one can see your messages, not even Viber. https://www.viber.com/en/security/
- Viber has the Disappearing Messages feature turned on. Set a self-destruct timer for each message in your chat to ensure that it is automatically wiped from the Viber chat once it has been read by all parties involved. Actions involving screenshots will be reported in the conversation while it is ON. https://www.viber.com/en/security/
- Editing & deleting all messages is possible. It can be frustrating to send a message that contains a typo, but don't worry—just long tap the message to swiftly fix it. If you still want

to, even if it has already been seen, erase the message that was sent to everyone in the conversation. What you disclose is up to you.
https://www.viber.com/en/security/

- On Viber, you can use Hidden-Number Chats. Start a safer chat right away when you meet new individuals in a group or find them on Viber by name search without having to reveal or exchange your or their phone numbers.
https://www.viber.com/en/security/
- You can utilize Hide Chats on Viber more effectively. You don't want anyone to unintentionally overhear your chat and or want to check your phone intentionally. Chats can be hidden from your chat list and accessed at any time using a PIN. You are the one who can set a PIN.
https://www.viber.com/en/security/
- If you notice a spammer, you have the option to block and report anyone you think is a spammer or fraudster. Activate the auto spam check to enable Viber to check messages for malicious content received from contacts who are not in your contact list.
https://help.viber.com/en/article/protect-yourself-and-your-privacy-on-viber
- Deactivate your Viber account if you want all of your data that has been saved on another person's device removed. You will immediately find deleted all conversations you have had with anyone from both your device and theirs.
https://help.viber.com/en/article/deactivate-or-uninstall-viber-on-your-phone

10.2.6. Telegram

- You can hide your phone number on Telegram. You can send messages in groups and in private chats on Telegram without revealing your phone number. By default, only the contacts you've added to your address book as contacts can see your phone number. Nonetheless, you can hide it.
https://telegram.org/faq
- On Telegram, you can have a secret chat. The user whose profile you want to contact should be opened. Click "..." and then "Start Secret Chat." Keep in mind that Telegram's private chats are device-specific. On one of your devices, if you and a friend start a private conversation, just that device will have access to it. All of your private chats will be lost once you check out. You can make as many different private chats with the same contact as you like.
https://telegram.org/faq#q-how-are-secret-chats-different
- You can enjoy an end-to-end encryption on Telegram. The participating devices use the so-called Diffie-Hellman key exchange to exchange encryption keys when a secret chat is created. Following the creation of the secure end-to-end connection, we create a graphic that represents the encryption key for your chat. When you compare this image to your friend's, If the two photos are the same, you may be certain that the secret conversation is secure and that a man-in-the-middle assault cannot succeed.

https://telegram.org/faq#q-how-do-i-start-a-secret-chat

- Telegram has two-step verification, and you can turn it on. Although using an SMS code to log in is a messaging industry standard, if you want more protection or have reasons to be suspicious of your mobile carrier or government, you can secure your cloud chats with an additional password.
  https://telegram.org/faq#q-how-does-2-step-verification-work
- Everyone can find you on Telegram and view your profile and pictures. Everyone who is a member of the group can see your name on the member's list. You can receive messages from anyone.
  https://telegram.org/faq#q-do-you-have-a-privacy-policy

10.2.7. Skype

- Use a password manager and create a complex password. Randomly, change your password. Never use an old password. Password managers which can help you have a strong password:
  https:/www.dashlane.com
  https://www.stickypassword.com
  https://www.lastpass.com/features/password-generator
  https://www.passwordboss.com
- You can utilize end-to-end encryption on Skype. Voice, video, file transfers, and instant messages between Skype-to-Skype users are all encrypted. This protects you from conceivable listening in by malevolent individuals. The part of your call that passes through the PSTN (the conventional phone network) when you call mobile and landline phones from Skype is not encrypted.
  https://support.skype.com/en/faq/FA31/does-skype-use-encryption
- Skype is a property of Microsoft. Microsoft's two-step verification security feature works to keep your Skype account safe by making it harder for unauthorized users to access your Microsoft account. Here is how to activate it:
  https://answers.microsoft.com/en-us/skype/forum/all/skype-login-two-factor-authentication/303d1b3b-8827-49b4-bdaa-ea7f823d971c
- If your account is compromised and or hacked, please visit How to recover a hacked or compromised Microsoft account.
  https://support.microsoft.com/en-us/account-billing/how-to-recover-a-hacked-or-compromised-microsoft-account-24ca907d-bcdf-a44b-4656-47f0cd89c245
- People can search for you using your phone number to connect with you and start speaking if you use a phone number to sign up or log into Skype or if you have one listed in your profile. If you choose to make your phone number unsearchable, you can do this at any moment.

https://support.skype.com/en/faq/FA34934/can-people-find-me-with-my-phone-number-in-skype
You have control over who can access the details of your Skype profile and presence status. Some information is public, but if you don't want it to be displayed in your profile, you can leave it blank. Your email address is not displayed on Skype. No one can see it when looking at your profile. Your email address cannot be used to be found by anyone other than friends who already know it.
https://support.skype.com/en/faq/FA34745/who-can-see-my-skype-profile-and-presence-status
Log into your Skype account safely if using a computer that is not yours. You can use a Virtual Private Network (VPN) for more private use of internet. First, verify the security of the browser. Do not select remember the password option. Once you're finished, log out of the account.

10.2.8. signal

- Signal features end-to-end encryption by default. Signal is made to never collect or store any private data. Signal calls and communications are always end-to-end encrypted, private, and secure, so neither Signal nor any other third parties can access them.
https://support.signal.org/hc/en-us/articles/360007318911-How-do-I-know-my-communication-is-private-
- To maintain a clean communication history, use disappearing messages. Once the countdown expires, the message will be removed from your devices. This isn't for cases where your contact is your adversary; after all, someone who receives a disappearing message may always use another camera to take a photo of the screen just before the message disappears if they really want a record of it. Here is how to do it:
https://support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages
- Editing & deleting all messages is possible on Signal. If you still want to erase the message that was sent to everyone in the conversation, you can do it even if it is seen. Here is how to do it:
https://support.signal.org/hc/en-us/articles/360007320491-Delete-messages-alerts-or-chats
- Set up the Lock Screen on Signal. The Screen Lock feature of Signal makes use of the pin, passphrase, or biometric authentication on your phone (e.g., a fingerprint, TouchID, or FaceID). Here is how to activate it:
https://support.signal.org/hc/en-us/articles/360007059572-Screen-Lock
- Signal PIN is a code that supports features like identifiers that are not based on phone numbers. This means that if you ever lose or swap devices, your PIN can help you retrieve your profile, settings, contacts, and blocked users. An optional registration lock that uses

a PIN can stop someone else from registering your number on your behalf. For more information and PIN change, visit: https://support.signal.org/hc/en-us/articles/360007059792-Signal-PIN

- Signal operates the existing keyboard or Input Method Editor (IME) on your mobile device. You can activate Incognito Keyboard to stop your virtual keyboard software from monitoring your typing patterns and using that information to tailor its service if you are concerned about it. Here is how to activate that: https://support.signal.org/hc/en-us/articles/360055276112-Incognito-Keyboard
- You can blur faces on photos using Signal. All processing takes place locally, on your own device, to protect your privacy. To achieve that, switch on "Blur faces," and faces will be automatically detected and hidden.

11. GOVERNMENT LEGISLATION ON FREEDOM OF EXPRESSION AFFECTING DIGITAL RIGHTS

On September 19, 2021, the Taliban issued a list of 11 rules for news organizations and journalists. Nine of these regulations have an impact on how the media and activists operate. According to these rules, it is against the law to publish or post any of the following:

- Publishing topics in conflict with Islam.
- Insulting national figures in media activities.
- Insulting nationality and anyone's personal privacy.
- Distorting the news content by the media and reporters.
- Not respecting journalism principles in their writing.
- Not observing balance in publications.
- Not cautious about publishing topics whose authenticity is not known and has not been confirmed by others.
- Not cautious about publishing topics that have a negative impact on public opinion or spoil the spirit of the people.
- The media not maintaining their neutrality in publishing news and not publishing everything that is true.
- The GMIC tries to cooperate with the media and reporters and prepare media reports and report them in coordination with their respective department preparation.
- In the GMIC, for the convenience of the media and journalists, a form has been prepared to prepare a report with its cooperation[77].

[77] Unofficial translation

They created a regulatory framework based on ideas and procedures that are incompatible with journalism as a profession. The first three rules, which prohibit journalists from airing or publishing material that is "contrary to Islam," "insults national figures," or "violates privacy," are loosely based on Afghanistan's pre-existing national media law, which also included a requirement to abide by international standards, such as International Covenant on Civil and Political Rights, and article 19 of the Universal Declaration of Human Rights.

The absence of this obligation in the new rules leaves room for censorship and repression because it is unclear who decides—or on what grounds—that a comment or a story is disrespectful of Islam or a public figure.

Three of the regulations direct journalists to follow what is regarded as ethical standards. They must "follow journalistic values," "not attempt to alter news substance," and "ensure that their reporting is balanced." However, these guidelines might potentially be abused or interpreted arbitrarily due to the absence of references to accepted international norms.

Articles 7 and 8 within the regulatory framework make it easier to reinstate news restriction or control, which has been absent in Afghanistan for the past 20 years. According to their rules, "Matters that have not been verified by authorities at the time of publishing should be treated with care," and "Matters that could have a bad influence on the public's attitude or affect morale should be handled carefully when being broadcast or published."

The last two rules (10 and 11) indicate that the GMIC has "designed a specific framework making it easier for media organizations and journalists to prepare their reports in accordance with the rules" and that going forward, media must "prepare detailed reports in coordination with the GMIC," which raises the risk of a return to news control or prior censorship. We still don't know what these "detailed reports" are.

The ninth rule, which mandates that media outlets "adhere to the concept of impartiality in what they disseminate" and "only report the truth," could be interpreted in a variety of ways and exposes journalists to arbitrary retaliation.

12. REFERENCES

12.1. BOOKS

- Chuck Easttom, 2019, Computer Security Fundamentals, Third Edition
- Michael Bazzell, 2018, Personal Digital Security, New Version

- Carla Mooney, 2015, Online Privacy An Social Media
- Melody Karle, 2020, A Social Media Survival Guide
- S.M. Iacus G. Porro, 2021, Subjective Well-Being and Social Media
- Kevin Mitnick and Robert Vamosi, 2017, The Art of Invisibility
- Christopher J. Hadnagy, 2018, Social Engineering: The Science of Human Hacking

12.2. WEBSITES

- https://www.accessnow.org
- https://rsf.org/en/
- https://www.mei.edu/
- https://www.techtarget.com
- https://www.politico.com
- https://basecreative.co.uk
- https://www.ssl.com
- https://www.ssl.com
- https://freedomhouse.org/
- https://www.cyberghostvpn.com/
- https://www.kaspersky.com/
- https://www.tunnelbear.com/download
- https://www.vpngate.net
- https://protonvpn.com
- https://mullvad.net/en/download/
- https://bitmask.net
- https://cryptpad.fr/drive
- https://ufile.io
- https://send.tresorit.com
- https://send.tresorit.com
- https://veracrypt.fr/en/Home.html
- https://www.dropbox.com
- https://www.techtarget.com
- https://www.expressvpn.com
- https://www.vpn-mentors.com
- https://www.cloudflare.com
- https://www.microsoft.com
- https://www.antivirussoftwareguide.com
- https:/www.dashlane.com/
  https://www.stickypassword.com
- https://www.lastpass.com/features/password-generator
- https://www.passwordboss.com

- https://whatismyipaddress.com
- https://www.tripwire.com
- https://www.malwarebytes.com
- https://knowledge-base.secureflag.com
- https://owasp.org
- https://www.ibm.com
- https://securityboulevard.com
- https://www.techadvisor.com
- https://www.hypr.com
- https://www.businessinsider.com
- https://duckduckgo.com
- https://metager.org
- https://www.startpage.com
- https://account.proton.me/login
- https://www.fastmail.com
- https://www.zoho.com/mail
- https://account.riseup.net
- https://en.exp.activix.ca/users/sign_in
- https://www.facebook.com
- https://help.twitter.com
- https://help.instagram.com
- https://www.tiktok.com/safety
- https://support.google.com
- https://help.yahoo.com
- https://faq.whatsapp.com
- https://www.viber.com
- https://telegram.org/faq
- https://support.skype.com
- https://support.signal.org