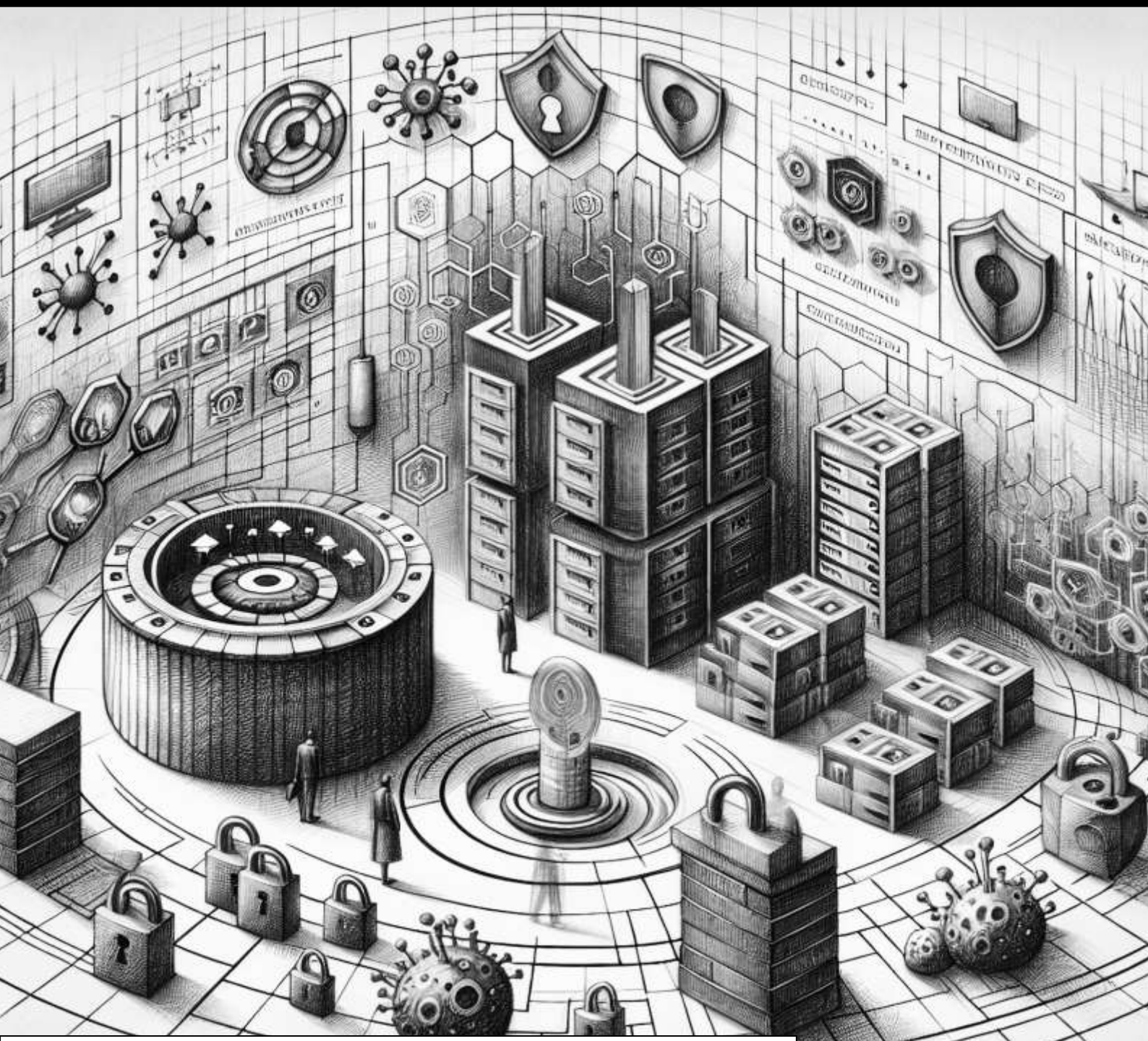

# Digital Security Handbook for Journalists

# Digital Security

## Handbook for Journalists

Alexandra Tóthová



The publication was based on resources created during the Journalist Security Fellowship in Central and Southeastern Europe led by Internews

Illustration picture: Stock AI-generated image ID #2475400847

# Content

# The importance of digital security

*Sara, a journalist working for local and international news organisations, reports on a wide range of sensitive political issues, such as corruption, abuse of human rights, abuse of political power, and governments making life harder for certain minorities in her country. The newsroom she is working for is considered a trustworthy source of information. After the parliamentary elections, the government started to limit press freedoms and raided newsrooms, and the homes of selected prominent journalists.*

While Sara's character is fictional and any similarities with reality are pure coincidence, she will illustrate during these articles the importance of digital security for journalists. By its very nature, journalism is stressful. It's a vocation that, by definition, involves risky circumstances and individuals, in addition to deadline pressure and dwindling job security. However, journalism plays a critical role in democratic societies.

Free, independent journalism is important for safeguarding democracy. They are providing information on local, national and international events that impact lives in various communities, thus helping to understand complex issues– including corruption or abuse of power, keeping the leadership accountable. However, who is guarding the journalists?

In countries where the media is politicized, journalists are suppressed to maintain control. In the current global political climate, it is crucial to focus on cybersecurity as cyber threats are pervasive.

Cybersecurity, in short, is the defence against hostile attacks by spammers, hackers, and cybercriminals against internet-connected devices and services, but also the prying eyes of those leveraging the position of power against critics.

These articles seek to inspire not only journalists but also civil society to adopt good digital hygiene for their safety and protection against hacking, surveillance, or online harassment.

People don't like to be forced to follow security rules, particularly when those rules do not fit neatly into their existing workflows. The following series of articles aims to explain, why certain security rules are important to follow, and ease their everyday application. Don't let the perfect be the enemy of the good, even the basic application of digital security measures is better than no application at all.

*Sara is working with a team of journalists on various reports on corruption. However, not all journalists in her team have the same level of digital skills and safety knowledge and practices. She is aware that some of her team members tend to have sloppy practises.*

*While working on an investigation, Sara receives a phone call from her source, telling her "The government knows what's coming, there was a leak". Sara knows the leak was coming from inside her organisation. After checking the access control, she learns that the designer team had access to the organisation's whole shared Google Drive, including her file with sensitive information. The designer team accidentally shared the file with a freelancer, who also works for the government.*

Rookie mistake, right? Talking about the poor digital safety that can significantly hamper a journalist's career, and threaten the position of colleagues and sources, is important, as it leads to ensuring not only our own protection but the people around us. When onboarding members of the team to adopt digital safety measures it is important to make them all be comfortable with their usage. In the digital domain, we are only as safe as the weakest link. Do a small investigation around your colleagues, check if they adopted the security protocols and if they follow them, who has access to files and the information.

This series of articles aims to encourage the usage of good digital hygiene and cybersecurity practices for the sake of guarding against identity theft, ransomware attacks, phishing scams, data breaches, and monetary losses. Many organisations operate without an official organisational security policy adopted, showcasing how little attention is paid to digital security. Instead, they rely on unofficial rules and "trust" of their colleagues.

It is clear to see why it is insufficient in the modern world that is predominantly digital, moreover, it is difficult to guarantee that employees are adhering to the same security guidelines. The most basic security events can catch new members off guard. Sparking the discussion on digital security is thus important. The concept of digital security might sound complicated, but adopting basic digital hygiene is not. These articles will try to present the topic as easily as possible. Digital safety is an ongoing process, not an end-goal.

The articles were created based on resources prepared during the Journalist Security Fellowship conducted by Internews.

Useful resources:

- Resources - Information Saves Lives | Internews
- Totem project (totem-project.org)
- Electronic Frontier Foundation | Defending your rights in the digital world (eff.org)
- Access Now - Access Now

# Passwords, password managers, two-factor authentication

*Sara used the same password for her Netflix account as her working email. Her Netflix account was leaked, posing a security threat to her team.*

In our digital lives, we have a plethora of diverse online accounts, including those for social media, email, government services, healthcare, shopping, and messaging apps like Signal and WhatsApp.

Since these accounts frequently hold enormous quantities of potentially sensitive information, some attackers may be very interested in gaining access to or taking control of them. Additionally, they may want to exploit our accounts to impersonate us.

Because of this, it's imperative that we keep our accounts safe, and the best ways to do this are by utilising two-factor authentication, creating strong passwords, and avoiding phishing.

A website called haveibeenpwned effectively illustrates the risks associated with password reuse. You can type in your email address on the main search page, and it will show you all the credential leaks which it was involved in.

Using the same password is a dangerous security practice, as if someone figures it out on one site, they can get to other sites as well– from email to social media, to internet banking, to medical records. The solution to avoid this is to use a unique password everywhere.

## Password managers

Password managers are amazing tools, that create and store unique passwords for you. It is recommended to use them as often as possible. In-browser ones work great, you can also sync the passwords between different devices. It aims to protect all of your passwords with a single master password. The master password needs to be very strong. You can also add two-factor authentication as an additional layer of protection.

Password managers aren't always easy to set up or implement and they may not be for everyone. Password managers do their best to mitigate security problems connected to data breach. It, however, creates a single point of failure and is often target for adversaries.

Some password managers that are recommended include 1Password (free for journalists), eePassXC, and BitWarden. You will have to spend some time to familiarise yourself with them and with their advanced features, such as like autofill in web browser windows, which can protect against some phishing.

KeePassXC, for example, allows you to store all your passwords on your device (and not the cloud), while 1Password warns you if one of your passwords was leaked or part of a security breach. Each password manager has a different setting.

If you are targeted by a powerful adversary, for example from the government, it is important to choose carefully the right password manager and play around with the settings to maximize security.

If your computer or phone gets compromised by spyware, the spyware can watch you type in the master password to your password manager and steal all your passwords. Therefore, it is important to keep your devices malware-free. If you have suspicion that your device is infected, reach out to Access Now.

If you don't want to spend time on a password manager, there are non-tech solutions too. Having a unique password for each site you use and having it written down on a piece of paper at a secure location is better for security than reusing the single password on every site.

## Creating a strong password

You should memorize the strong passwords you use for your device, encryption, and email address.

A good password combines upper and lowercase letters, numbers and special characters. Passphrases, consisting of multiple random words, are best. However, people usually are not very good at making random, unpredictable passwords.  If you have a problem with memorizing

your password, think about how you can complicate something easy to remember. Programs breaking the passwords operate on dictionary words, the more unpredictable you make it, the more secure it will become. The more characters, the harder to break.

Example:

- password
- passwordcrossword
- Passwordcrossword007
- Passwordcrossword#007
- P@ssw0rd*cr0ssword#007!

## Security Questions

"What was the name of your favourite pet?". These types of questions are often used by sites in case you forgot your password. While it is an easy way to get to your account, the problem with that it can be too easy. Think about entering an information, that is not that easy to guess– in example, the name of the pet and their birthday.

## Two-factor authentication (2FA)

The essence of it is a two-step verification for accessing your account– a strong password and a second way of verification. The second way of verification can be done in multiple ways, such as an SMS or email code, verification by an additional application, or a stand-alone hardware in a form of security key.

A security key is always a better option, since SMS or email verifications can be redirected or bypassed. You can receive free or low-cost physical security keys, through Yubico's Secure It Forward program.

# Phishing and protection against it

A typical technique for attackers to gain access to your account is through phishing, which is when someone sends you a phoney message asking you to click on a malicious link and enter your login credentials or download malware. The main signs might include strange phasing, a sense of urgency, suspicious URL, suspicious email address of the sender, etc.

*Sara received a phishing email, clicked on it, entered her username, password and 2FA code she got from her authentication app. She realized it was a phishing page only after entering her credentials.*

Phishing attacks can deceive even experienced security experts due to their frightening effectiveness and persuasiveness. The link that leads to the phishing attempt can look very similar to regularly used websites, like a popular social media account. However, the credentials will not lead to the regular login, but to the storage of the attacker.

Learn to recognise phishing emails (formatting errors, sent from weird addresses, links to unusual pages, gives off a sense of urgency) but also use physical security keys and password manager auto-fill as extra protection.

Physical security keys are resistant to many types of phishing. A sophisticated adversary could set up a fake webpage where users type in passwords. Physical security keys are specially crafted to stop these attacks. After a phishing attack, change your password.

# Secure messaging, secure file sharing and why is it important

## Why is secure messaging important?

*Sara, a journalist, have been contacted by someone via Facebook's Messenger claiming to have sensitive information from the Ministry of Defence, that he wants to share with her. Sara wants to move the conversation to a more secure channel, that is end-to-end encrypted, to protect the source.*

End-to-end (E2E) encryption means that the message can't be read while in transit, not even the company which operated the messenger. The message will not be stored unencrypted on the servers of the company either. In case of E2E encryption, law enforcements will ot be able to access the message from the messaging channel. If there is a hack attach on the account that was used to send the message, they will not be able to access the content of the message, unless there were unencrypted backups. However, messages can be read other ways, if a phone is seized and unlocked.

Using disappearing messages as often as possible, especially for sensitive chats add an additional layer of protection. If you need an archive of messages, talk about alternative ways to save them (screenshots that are sent to your newsroom then deleted, handwriting in a notebook, etc.).

## Which messaging channel is the best?

Different messengers work for different threat models—there is no perfect tool.

**Signal** is the secure messenger as usually recommended. It offers open source E2E encryption, collects no metadata, and has been analysed and endorsed by leading security experts.

**WhatsApp** is also a good alternative. While it gives Meta access to all your metadata, it's E2E encrypted and more common so you are less likely to stand out when using it.

Both these apps require a telephone number, that is usually registered with a personal ID. If journalists do not want to reveal their phone numbers, we recommend they use **Wire.** However, since it is less common, it might stand out and be difficult to convince sources to use it). **Telegram** is more common than Wire, but you must explicitly enable E2E encrypted chats and dig through the settings to hide your phone number.

In any case, you must go through your messenger's settings. This might involve enabling disappearing messages, disabling unencrypted cloud backups, and hiding your profile from users not in your contacts list.

Most messengers offer some sort of two-factor authentication, where anyone who wants to activate their account on a new device needs to enter a special password. A password must always be unique. Never repeat passwords or use similar ones.

We strongly recommend enabling two-factor authentication whenever possible. Physical security keys are best, followed by authenticator apps. Two-factor authentication through SMS is the least secure, but much better than nothing.

## File sharing

*While working on an investigation, Sara receives a phone call from her source, telling her "the Government knows what's coming, there was a leak". Sara knows the leak was coming from inside her organisation. After checking the access control, she learns that the designer team had access to the organisation's whole shared Google Drive, including her file with sensitive information. The designer team accidentally shared the file with a freelancer, who also works for the government.*

This type of mistakes is easy to make. You need to audit the shared documents frequently and only have information on an as-needed basis. Decide, how the team should communicate, store files and access these files and to what degree. Ensure, everyone is following the same protocols related to file sharing.

If possible, very sensitive information, such the identities of susceptible sources, should only be disclosed to those who truly need to know. When distributing documents, think about utilising pseudonyms and other techniques for anonymisation. Also, you can use a strong password (shared by a different channel) for Microsoft Office files (Word, Excel) when sending documents.

Discourage people from taking files and documents outside the work environment (e.g. forwarding emails to personal accounts, taking materials home on an USB) as you have little control over what is installed on those computers, if they are protected by a strong password and have up-to-date software.

End-to-end encryption when it comes to file sharing is important. You could safely share files with other people in the following ways:

• Direct file transmission over Signal (up to 100 MB of data supported)

• Making use of the OnionShare programme, which safely transfers files over the Tor network (no set maximum file size).

• Making use of the Tresorit Send service (up to 5GB of files)

SecureDrop is great if you want to receive tips and documents anonymously but can be hard to use since it requires Tor Browser.

An app called Dangerzone turns potentially suspicious documents into safe and readable PDFs. Reputable programmers actively develop it, which means it gets better and better with each version.

You can also set up a public Signal number for sources to share the files, making both available and easy.

## Opening files

*Sara is investigating a corruption case, that is involving two countries. She travels often in her personal life and for work purposes. She receives a document from her source from the government. She opens it, reads it, but as not containing any important information, discards it. What she might not be aware of is that the document had a tracker connected (e.g. canary token), which notifies the sender about the IP address of the reader, through which the physical address can be determined. Now her source knows she is working on the reveal of the full international corruption case.*

Opening a suspicious file is part of the job of every journalist, therefore it is important to pay attention to opening the file SAFELY. The simplest method of sanitization is to just upload the file on a safe cloud, such as Office 365 (online from Microsoft) or Google Drive using the usual web browser. Keep in mind that you'll need an account with one of the providers for this. When you access a file in Google Drive or the web edition of Office 365, the entire file is opened and converted into a format that can be seen by your web browser by Google's or Microsoft's servers. Therefore, any potentially harmful elements in the file would not affect your machine, but rather Google's and Microsoft's servers, which are equipped to identify and remove malware.

A cleverly crafted malicious file, such as an Office Document, could infect a device, being it a PC or phone. For this reason, it’s best to open suspicious files on your phone or within Google Drive or Office 365. Avoid desktop apps (Adobe, Word, Excel, etc.) as a potential malware can infect your device.

## Safe collaboration with colleagues

One of the simplest methods for sharing files and working together on documents is still through online services like Google Drive or Office 365, both of which are considered to be safe by the security community. However, all members of your organisation must adhere to stringent security configurations (strong passwords, ideally 2FA). All journalists who have access to extremely sensitive material should look at Google's Advanced Protection Programme.

Sharing files via the internet, such as Google Drive, might make it simple to forget who you shared a document with and when. To prevent "permission creep," be sure to regularly audit your files or remove them. Have a procedure for removing somebody’s access to all files, logins, and social media posting privileges the moment they leave the project, team, or organization.

# Secure Browsing

We are connected to the internet through network. When someone at your network—a telecom employee or an office manager, for instance—accesses unencrypted data you send over the network, network tracking takes place. They could still be able to see the websites you are visiting

or the services you are connected to, even in cases when the direct connection with a webpage is encrypted.

Device tracking occurs when someone uses cookies, for example, to follow your browser or device. Your identity is retained by the website you visit even if you connect to a different network. There are occasions when this is helpful. For instance, since your webmail provider recognises you, you don't need to sign into your email again when using a new Wi-Fi network. The issue is that you can also be recognised or identified by potential enemies and advertising. While most journalists are not at risk from this kind of surveillance, it is good to bear in mind the protection against it.

When it comes to online tracking, there might be consequences. A telecom or government agency can see the website you're visiting (like wikipedia.org) and possibly how much time you spend there when you use a website but not the specific page you're reading. Could it sink an investigation if a telecom or government knows what pages you visit? Depending on who we're protecting against, there are a few things we can take to lessen internet tracking.

*Sara is travelling. When arriving to the airport, she is stopped and searched by the border police. They force her to unlock her phone. She sees the police is checking her contacts, messengers, photos. She's prepared for this, everything sensitive is sent to her newsroom to Google Drive and deleted from her device. However, she did not clear her browsing history, where she searched for the localisation of the institution she was going for an interview.*

Browsing history as such could also be used for harvesting sensitive information, when a device is confiscated. Learn how to clear it and use it regularly. Use it not only for your browser history, but also on apps on mobile devices, such as Google Maps.

The internet connection itself can be monitored. When using Google services such as Gmail, Google Drive, this is not an issue, because only the connection is seen, not exactly what is going on during the connection (uploading files, sending email, etc.). In this case, a VPN is not necessary. However, there are situations where you want to mask your internet connection.

## IP address, VPN, Tor browser

Your IP address can be seen by websites you visit, which may let them to determine your office identity or even your geographical location. You can mask your IP address by using a VPN.

VPNs are often very useful. They create an encrypted link that separates you from the website you are viewing. This implies that while your VPN provider can see what you browse, neither your telecom nor the government can view it directly. Select a reliable supplier because they will have access to your metadata. An untrustworthy VPN could be more of a threat than a helper.

VPN recommendations:

- TunnelBear is a Canadian VPN service.
- Mullvad is an open-source commercial VPN service based in Sweden.
- ProtonVPN is a Swiss VPN service.

The Tor Browser is a great anonymizing tool. It routes your web traffic through a series of other computers, which makes it incredibly hard for any adversary to track your browsing. At the same

time, many websites can block Tor connections, either explicitly (by refusing to connect) or implicitly (for example by asking you to constantly select pictures of traffic signs). If you use the Tor Browser most or all the time, you might need to modify some of your browsing habits. Use Tor Browser when you require an even higher level of anonymity than VPNs provide, for example when researching very sensitive topics. VPN landscapes regularly change, so recommendations quickly go out-of-date. The Tor Browser makes it extremely difficult for any opponent to track your surfing activity by rerouting your web traffic through several other computers. Sometimes you might work at a location where certain content is censored, restricted or unavailable. Tor and VPNs also make it possible to get around censorship.

# Protect your device

*On a Monday morning, around 50 police officers arrive to the newsroom Sara is working at. They have a warrant, which is shown to the editor, then they demand all the journalists to leave immediately.*

It's natural, the colleagues will want to be in touch, so they create a group chat (via Signal or WhatsApp). In this case, it might be a good idea to communicate through personal phones instead of work numbers, as those might me linked with devices that stayed in the office.

At first, you should consult any steps with a lawyer, as any steps towards protection might be considered as tampering with evidence. If destroying evidence, it could be a legal issue. If possible, log out remotely from all devices that are in the office and change passwords.

In situations like this, it is important to think about the personal and organizational safety, but also the safety of your sources. Most of the situations, where digital security is compromised are not this intense. Losing a device, sloppiness around access to shared documents, phishing attacks, lack of antivirus are more common ways, how sensitive information can end up in the wrong hands.

## Mobile phone security

*A source sends files to Sara via Signal, she views them on her mobile. She is happy to have the information and goes out with her friends to celebrate her friend's birthday on a Friday night. While at the party, she loses her phone and realizes her simple password (1111) might be easily guessed. She starts to panic. What can she do?*

Generally speaking, mobile phones are safer than laptops and desktop PCs. They are nearly always encrypted by default, have specialised security hardware, and can frequently only launch apps from approved sources (which slows the spread of malware).

However, you also need to protect your phone with a password. With a passcode (or fingerprint), someone trying to steal or find your locked phone won't be able to access its contents. While biometric passwords are convenient, such as a fingerprint or face recognition, they might not be the safest (someone can force you to put your finger on the phone to unlock it). Numeric passcodes are considered safer, but there needs to be a variety of not-that-easy-to-guess numbers.

Moreover, you need to keep your software on your phone up to date. Adversaries look for software flaws or gaps to access your phone without authorization. When one of these vulnerabilities is found, the programme is updated to close the gap, making it impossible to attack going forward.

On both Android and iOS, you may search for and install updates, or turn on automatic updates. When your gadget no longer supports software updates, it's time to change to one that does.

Even with the greatest security settings, you can still be required to unlock your phone—for instance, during a border crossing. Therefore, it's a good idea to use disappearing messages for critical chats, delete chat apps altogether when entering a dangerous situation, and to routinely remove sensitive data from your phone that you may no longer need.

What can Sara do in her situation? She can remotely wipe her phone if this functionality is switched on. She can sign in to her email and social media accounts to change her passwords immediately, and if possible, sign out of all logged devices. As a precaution in the future, she can also lock all her applications, such as messengers, with an additional password.

Your phone may be taken from you by security or law enforcement, for example, during a search. Don't think your phone is secure once it has been given back to you. It's also possible that malware was installed on your phone by a security service if it was seized. The best course of action would be to replace the seized phone with a new one.

Another method would be to perform a complete factory reset as soon as possible. A complete factory reset will remove all of the data on your phone, including contacts, messages, images, and all other data. Thus, be prepared to use a backup to restore. Change all of your passwords after the reset is complete, just in case.

## Localisation through phone

In order for a mobile phone network to link a particular phone to the appropriate tower and send and receive signals from it, the phone must first be located. You should presume that your mobile provider is always aware of your phone’s location when it is powered on. In places (like crowded cities) where there are more mobile towers, you can locate your phone more precisely. Moreover, there are plenty of apps that can track your location. Audit these apps regularly and grant access to your location only while using them (e.g. Google Maps).

## Meeting a sensitive source

Sensitive sources, in general, require more focus on their protection. You might think about pseudonyms when saving their contact, as a form of anonymisation.

Another aspect is localisation. Due to the localisation, you might consider to be mindful about your phone. Do not just turn off your phones before a meeting or when you get to the meeting site if you have a sensitive source scheduled and you are concerned that a government agency or telecom could be utilising location data to determine that you are both in the same place.

It's far wiser to attempt to mimic typical activities instead, such as leaving your phones on at home or at work before a meeting (or shutting them off hours in advance, if you're the kind of person whose phone batteries die all the time). Anybody following you or they may quickly discover if both people's gadgets abruptly stop connecting to the network.

## PC security

The least you can do is lock your computer with a strong password, and not leave your PC running without it when not present working on it. Restart your computer regularly to update the software. Lock your sensitive documents stored in the document with a password (applicable for Excel and Word documents too).

### Encryption

Using tools such as VeraCrypt or similar is useful when encrypting data on hard drives, USB or external drives.

### Paper

Applying safeguards around paper notebooks is also important and also be mindful about physical copies of documents. Hide your notes, don't keep them at the same location, ideally lock them up, and while making notes, use pseudonyms, acronyms, and short hands that only you understand. Consider regularly destroying what you don't need. Scan and destroy paper documents, use encrypted digital backup. Also be aware of any legal ramifications of storing sensitive information at your home, instead of an office.

## Online harassment

Sara is working on a piece regarding ethnic minority and how government policies are leading to increased marginalisation of this group. Over a few weeks, Sara notices a spike in her social media comments, where she shares personal posts and her work. She starts to receive hateful and derogatory comments, she notices trolls are targeting her.

She flags the issue to her male colleagues, who tell her not to worry about it, it will go away. However, she is stressed and feels like her team members are not listening or try to understand her situation. It is important to notice, these toll campaigns target men and women differently, the latter is usually hit harder as there is a gender-related hate too.

When an accident happens, upon arriving at the scene, first responders evaluate any physical injuries the victim may have. Although online harassment sometimes seems to be limited to the "virtual" world, we need also be aware of this tangible and physical side.

Thankfully, talking about mental health is becoming less and less tabularized. Our brains react similarly to both physically and virtually posed threats; for instance, they trigger a cortisol-fueled "Fight, Flight or Freeze" reaction (FFF) when faced with a threat. The body recognises that it is time to go into "survival mode" when the stress cycle is triggered. It takes a lot of energy to do this. The FFF takes precedence over everything else, including thought, in the brain. The autopilot is activated.

Even if we survive, the FFF response wears us out from the body's perspective– we react in the same way to a lion standing in front of us than an online threat. The end of the threat is not a sufficient information for the body to end the reaction to the threat. Handling the stressor does not equate to handling the stress. This is why "completing the stress cycle" is a crucial task. Not only must we comprehend what the cycle is, but we also need to apply it to our regular mental health practices. Reaching the conclusion of our stress cycle entails communicating to our body that we are safe.

What can Sara do in her situation? She can check if trolls are using the same language, keywords, or even hashtags, indicating a coordinated campaign. See also the most common posting time, as again, it can indicate and automated coordinated campaign. She can also use the built-in block and report functions on social media or contact the social media companies directly and report a large-scale harassment. In many cases, trolls thrive off attention and publicity. As such, do not engage them if you can; they will see that you reacted and try to annoy you further. If possible, mute rather than block trolls—you will no longer see many of their replies, but they will

not know they are muted. You can outsource the blocking and managing the trolls to Trollwall. Similarly, the Block Party App can help reduce harassment on Twitter by muting or reducing the visibility of harassing content and identifying those who spread it.

When you need to criticize a troll, it's best to take a screenshot of their post and comment on that, rather than quoting or replying to the original post. That way, you can show the troll's statement to others without notifying them or getting recommendation algorithms to promote the post.

Online harassment, troll campaigns, smear campaigns, hate speech can add to the overload of the levels of stress, thus the nervous system and the brain. Managing stress is therefore key, by closing the stress cycle regularly. When we comprehend the motivations behind sports, relationships with others, playing with dogs, or making art, these activities take on greater significance.

## Activities for managing stress:

- sport, movement of the body
- breathing techniques, meditation
- positive social connections (friends, family, but positive small talks with strangers too)
- affection with close connections: partner, friends, family, pets
- let it out. Crying is OK. Laughing is OK.
- fostering creativity and art, find serenity there
- spirituality, nature, connect with something larger

We should pay attention to verbal crimes (hate speech), cyberbullying, doxxing, online harassment, and any other type of online persecution. The negative impacts of such persecution on one's bodily and mental well-being are no longer regarded as socially acceptable. They can cause harm that is equal to or greater than physical violence, affect more than just the immediate target, and have far-reaching effects.

The effects of online harassment can be difficult for most people to understand or even relate to, so be cautious where you seek guidance. It's possible that your family members experience this also. When well-intentioned family members or friends inquire, "couldn't you just delete your social media accounts?" they may unintentionally exacerbate the matter. Although such inquiries may originate from a sincere wish to assist, they may ultimately minimise your emotional suffering and overlook the intricacy of the circumstances for an individual employed in the media.

Creating an effective support network are crucial. Journalists and their organizations should spend time investing in networks of friends, mental health professionals, and experts who can help them when things get tough.

## There are things you can do to protect yourself:

- Have a *no photos in the newsroom* policy
- Switch on the request to review before being tagged on photos on social media
- Delete old photos, especially those which might compromise your reputation (university party photos, etc.). Think about the number of pictures with your face and how AI can be trained to create a compromising deepfake utilizing your photos too.

- Think what information is shared before you publish your personal photos. Don’t publish photos from your neighbourhood (danger of publishing your home address) or places you travel often to (e.g. local swimming pool, again, there is a danger of spillover from online to physical harassment)
- Don’t post photos of your family members or friends you meet often publicly
- Ask a friend or search the web for your name, analyse your social media from the perspective of a stranger, and summarize any information you can find. This exercise can feel incredibly vulnerable and expose sensitive details.
- Continue posting work-related content but limit personal content. If you drop from the internet completely, the trolls will win.