DIGITAL SECURITY

Best Practices for Journalists

PASSWORD PROTECTION

- Passwords should be at least eight (8) characters long.
- Don't use dictionary words and ideally, choose a passphrase instead (a short sentence)
- Add upper and lower case letters, numbers and symbols to make your password more secure.
- Change passwords fairly regularly. Every three months is advisable.
- Use a password manager (for example: Keepass, 1Password or LastPass), which allows you to generate unique passwords and store them securely with a single access phrase serving as a master password for accessing all other passwords. Make sure you store the master password in a secure location.

CELL PHONE SECURITY

- Always password protect your cell phone. A combination of digits, letters and symbols is the safest option. Activate passwords not only to access your cell phone, but also to enter into applications (email, social networks, etc.)
- For further security, protect your SIM card with a SIM pin code, usually accessible in the Phone settings.
- Never share highly sensitive information over chat. By "highly sensitive" we are referring to your bank information or your passwords, but this also includes anything else you don't want others to read without your authorization.
- To communicate securely with others use applications that integrate end-to-end encryption, such as Signal or Wire. This means that your messages are encoded and no intermediary can read them.

DIGITAL SECURITY

Best Practices for Journalists

PROTECTION OF SOURCES

- If you communicate with sources who are not familiar with Internet security, follow these steps to communicate via email:
  1. Create a Protonmail email account for yourself at https://protonmail.com.
  2. Ask your source to create one too recommending to choose secure passwords. If the source decides to use Protonmail from a public computer, recommend to use the browser in Private/ Incognito mode and save attachments, if any, on a personal USB stick instead than on the local hard disk.

- If you communicate with sources who are more familiar with Internet security, ask them activate PGP (Pretty Good Privacy), which allows you to set up a public password and electronically sign documents to authenticate them. Share your PGP password with your sources.
- Activate a secure password in order to access your cell phone and computer/laptop contact lists.

DATA PROTECTION

- Avoid downloading pirated or questionable software so that your data is not put at risk.