NWC | NATIONAL WHISTLEBLOWER CENTER

CYBERSECURITY: WHISTLEBLOWER BEST PRACTICES

General information-sharing tips

- Do not use a device that is owned by the government or your employer. It is best to use a device that is not linked to you personally.
- Do not use your home or work internet network.
- Create alias communication accounts (use fake names for email, social media, messenger, etc).
- Do not engage in other activities which could identify you when sharing information, such as checking email, social media, online shopping, etc.
- If you do not feel comfortable reporting on your own, work with an NGO or attorney to make the report.
- Use Protonmail and its associated VPN to communicate via email.

Using a mobile device

- If possible, use a mobile phone that has been purchased only for whistleblowing purposes. It should not have any personal contacts, photos, or other information on it. As an alternative, use a publicly-available phone that is unconnected to your identity.
- Before using a mobile device, turn off all tracking and Bluetooth functions and close any active applications.
- Use internet browsers such as Tor, Orwall, Orbot, or Orweb, to make the report on your mobile device.
- For text messaging purposes, use encrypted applications such as TextSecure, Silent Circle, or Threema.

Using an internet cafe or other public wifi

- Check to make sure that the cafe, library, or other location does not require a valid identification before letting you use a computer or internet.
- Download the Tails operating system or the Tor browser bundle to a USB drive, and use these tools when at an internet cafe, even if using a personal computer.
- Make sure no one can walk by and see your computer screen without your noticing them.
- Log out of all accounts and remove all devices and software after using a computer at an internet cafe.

Need advice?

Contact the National Whistleblower Center:
contact@whistleblowers.org