Digital Safety Kit for Journalists

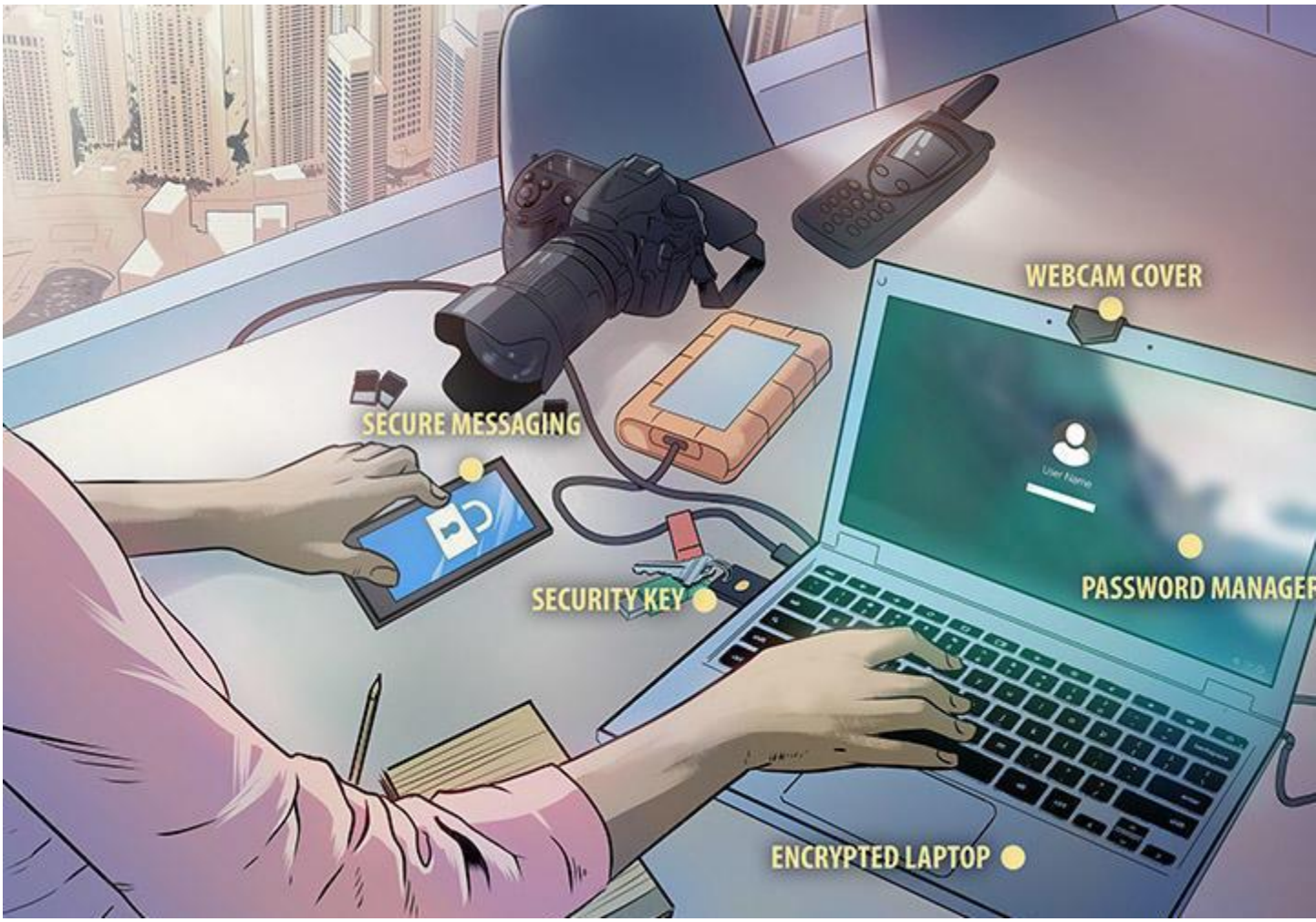
By Admin

5 Days Ago

144

0

13 Minutes Read



Artwork: Jack Forbes

CPJ Launches Digital Safety Kit

The Committee to Protect Journalists has launched a new, updated Digital Safety Kit for journalists looking to better protect themselves, their sources, and their information. The kit, produced by CPJ's

Emergencies Response Team, combines six bite-sized safety notes on different topics in an accessible format that is easy to digest.

Journalists should protect themselves and their sources by keeping up-to-date on the latest digital security news and threats such as hacking, phishing, and surveillance. Journalists should think about the information they are responsible for and what could happen if it falls into the wrong hands, and take measures to defend their accounts, devices, communications, and online activity.

Protect your accounts:

To protect your accounts, Journalists should use a variety of online accounts and these hold both personal and work-related information on themselves, their colleagues, families, and sources. Securing these accounts and regularly backing up and removing information will help protect against hackers. These steps are particularly important for journalists who may be targeted by an adversary with sophisticated tech capacity.

- Think about what information is stored in each account, and what the consequences would be for you, your family, and your sources if your account is breached.
- Review your privacy settings and understand what information is public, especially on social media.
- Create backup copies of any information that is sensitive or that you would not want to be made public, including private messages, then delete them from your account or device. Store the copies securely on an external drive or in the cloud.
- Delete any accounts that you no longer use. Remember to create copies of any information you want to save.
- Create long, unique passwords for every account. Do not reuse passwords. Use a password manager to help you manage your passwords.
- Turn on two-factor authentication (2FA), and use a security key like a Yubikey if possible.
- Regularly review the ‘account activity’ section of each of your accounts. This will reveal if devices you don’t recognize are logged in.

Phishing

Journalists often have a public profile and share their contact details to solicit tips. Adversaries looking to access journalists’ data and devices can target them–or a colleague or family member–with phishing attacks in the form of tailored email, SMS, social media, or chat messages designed to trick the recipient into sharing sensitive information or installing malware by clicking on a link or downloading a file. There are many types of malware and spyware which range in sophistication, but the most advanced can grant remote attackers access to the device and all of its content.

To defend against phishing attacks:

- Research the tech capabilities of your adversaries to understand the threat and the likelihood you or someone you know could be a target.

- Be wary of messages that urge you to do something quickly or appear to be offering you something that appears to good to be true, especially if they involve clicking on a link or downloading an attachment.
- Check the details of the sender's account and the message content carefully to see if it is legitimate. Small variations in the spelling, grammar, layout, or tone may indicate the account has been spoofed or hacked.
- Verify the message with the sender using an alternative method, like a phone call, if anything about it is suspicious or unexpected.
- Think carefully before clicking on links even if the message appears to be from someone you know. Hover your cursor over links to see if the URL looks legitimate.
- Preview any attachments you receive by email; if you do not download the document, any malware will be contained. If in doubt, call the sender and ask them to copy the content into the email.
- Upload suspicious links and documents to Virus Total, a service that will scan them for possible malware, though only those that are known.
- Enable automatic updates and keep all software on your devices up-to-date. This will fix known vulnerabilities that malware relies on upon to compromise your security.
- Stay particularly alert to phishing attempts during elections and periods of unrest or if colleagues or local civil society groups report being targeted.

Device security

Journalists use a wide range of devices to produce and store content and to contact sources. Many journalists, especially freelancers, use the same devices at home as well as at work potentially exposing a vast amount of information if they are lost, stolen, or taken. Encrypt computer hard drives, phones, tablets, and external storage devices, especially if you travel, to ensure that others will not be able to access this information without a password.

To secure your devices:

- Lock devices with a password, code, or PIN. Longer personal identification numbers or passwords are more difficult for others to unlock.
- Update your operating system when prompted to help protect devices against the latest malware.
- Audit the information stored on your devices and consider how it could put you or others at risk.
- Back up your devices regularly in case they are destroyed, lost, or stolen. Store the backup copies securely, away from your regular workstation.
- Delete sensitive information regularly, including chat messages. To prevent an adversary from restoring deleted files, use secure deletion software to wipe the device, if available; otherwise, reset it and use it for unrelated activities in order to rewrite the device memory. (Back up anything you want to keep first or you will lose all your data.)
- Don't leave devices unattended in public, including when charging, as they could be stolen or tampered with.

- Don’t plug devices into public USB ports or use USB flash drives that are handed out free at events. These could come loaded with malware which could infect your computer.

- Be aware that your device may back up your data to the cloud account linked to the phone. Information stored in the cloud may not be encrypted. You can turn off automatic backups in the settings.

- Set up your devices to allow you to wipe any data remotely if they are stolen. This feature must be set up in advance, and the device will only wipe if it is connected to the internet.

- Always get devices repaired with a reputable dealer.

To encrypt your device:

- Newer smartphones come with an encryption function, just make sure it is switched on in the settings.
- Use Bitlocker to turn on full-disk encryption for Windows, Firevault for Mac, or the free Veracrypt software for hard drives and external storage.
- Creating a long, unique password is key to using encryption; on a smartphone, check the custom settings to add a longer, more complex password.
  - Be aware that an adversary with knowledge of your password or power to compel you to decrypt your device will be able to look at the information.
  - Always research the law to ensure encryption is legal in the country you are living in or traveling to.

Encrypted communications

Journalists can communicate with sources more securely using encrypted messaging apps or software that encrypts email so only the intended recipient can read it. Some tools are easier to use than others. Encryption protects the content of messages, but the companies involved can still see the metadata, including when you sent the message, who received it, and other revealing details. Companies have different policies on how they store this data and how they respond when authorities ask for it.

Recommended messaging apps offer end-to-end encryption, meaning that the information is encrypted when it is being sent from the sender to the recipient. Both parties must have an account with the same app. Anyone with access to a device sending or receiving the message or to the password of the account linked to the app can still intercept the message content. Examples of messaging apps with end-to-end encryption include Signal, WhatsApp, and Telegram.

Encrypted email is a more secure way of exchanging information with a source or contact. Both parties must download and install specific software in order to send and receive encrypted email.

To use encrypted messaging apps:

- Research who owns the app, what user data they keep, and whether that data has been subpoenaed by a government. Check to see what their policy is for responding to requests to share user data.

- Use a PIN or password with the app where possible to prevent someone from opening it if they steal your phone.

- Understand where information sent to your messaging apps is stored on your phone.
  - Anything you download, like photos, will be saved on your device and may be copied to other devices and apps, especially when you back up your data.
  - Some services, like WhatsApp, back up your message content to the cloud account linked to the telephone number.
  - Contacts stored in your phone sync with messaging apps and cloud accounts, so numbers you try to delete in one place may be preserved somewhere else.

- Back up and delete messages regularly to store as little as possible on a single device or account. Create a process for reviewing content, including documents and multimedia messages, and store downloads or screenshots on an encrypted external storage device.
  - Signal's disappearing message function allows you to automatically delete messages after a certain time.

To use encrypted email:

- Get help from a trusted contact who is tech-savvy. Encrypted email is not always easy to set up if you are new to it.

- Choose reputable email encryption software that has been peer-reviewed. Always update your software to protect against security vulnerabilities.

- Take time in advance to create a long, unique password for your encrypted email software. If you forget this password you will lose access to encrypted emails.

- Send encrypted emails regularly so that you don't forget how to use the software.

- Details about the email, including the title and the email addresses sending and receiving the message, are not encrypted.

Examples of email encryption software include GPG Suite for Mac, GPG4win for Windows and Linux, Thunderbird with the Enigmail extension, and Mailvelope.

Secure internet use

Journalists rely on the internet, but may not want to share their online activity with

every internet service provider, internet cafe, or hotel with free WiFi. Criminals, as well as sophisticated adversaries, can steal information or monitor journalists using insecure websites or public WiFi connections.

To use the internet securely:

- Look for https and a padlock icon at the start of every website such as URL (https://sanef.org.za**),** indicating that traffic between you and the site is encrypted. Check sites you visit are secure using the Electronic Frontier Foundation's HTTPS Everywhere browser extension.

- Check that the website address is authentic, not a spoof. The URL should be spelled correctly and include https.

- Install an ad-blocker to protect against malware, which is often hidden in pop-up advertising. Ad-blockers allow you to exempt certain sites from being blocked.

- Install Privacy Badger to block websites and advertisers from tracking what sites you visit online.
- Disable Bluetooth and other file-sharing apps and services when not in use.
- Use a VPN to protect Internet traffic, especially when using public WiFi, which is not secure and leaves you vulnerable to hacking or surveillance.
- Avoid using public computers, especially at internet cafes or press rooms. Log out of all sessions and clear your browsing history after use if it cannot be avoided.
- Consider installing the free Tor Browser Bundle to use the Internet anonymously or Tails, a free operating system that routes all your internet traffic through Tor. Tor is especially recommended for journalists who investigate sensitive topics like high-level government corruption in countries with sophisticated tech capacity.

Artwork: Jack Forbes

Crossing borders

Many journalists cross borders carrying work and personal information that they may not want others to access on electronic devices. If border guards take a device out of your sight they have an opportunity to search it, access any accounts, copy information, or install spyware. Journalists crossing U.S. borders should consult CPJ's safety note, "Nothing to Declare."

Before you travel:

- Find out what information is on your devices and how it could put you and your contacts at risk. Assume your devices could be subject to the same level of scrutiny as notebooks and printed material in your luggage.
- Back up all your devices to an external hard drive or to the cloud. Remove any information that you would not want border officials to access from your devices.
- Buy clean devices to use only for travel if possible, especially if you are working on highly sensitive stories. If you are traveling with a personal or work device, securely back up your content then perform a wipe or reset.
- Turn on full-disk encryption for all devices to ensure that your information cannot be accessed without a password. Research restrictions on encryption of the country you are visiting to ensure you are not breaking any laws. Be aware that security forces may legally be allowed to ask for your password. Seek advice from your employer or lawyer before travel if there is a possibility you will be stopped at the border.
- Log out of all accounts on your devices and uninstall apps until you have crossed the border and reached a secure Internet connection.
- Clear your browsing history on all your devices. (Your internet service provider will still have a record of which websites you have visited.)
- Lock all devices with a PIN or password instead of biometric data like your face or fingerprint.
- Enable remote wiping of your devices and leave clear instructions with someone you trust to wipe your devices remotely if you are detained.

At the border:

- Power off your devices to activate disk encryption.
- Keep an eye on your devices as they pass through security.
- Do not turn on your phone until you are away from the airport. Any calls and SMS messages will be routed through a local service provider who may collect the content or share it with authorities. Use a VPN when connecting to the airport WiFi.

If any device is confiscated at the border or anything is inserted into it, assume it is compromised and that any information on it has been copied.