Digital Safety Checklist
Device Security

The following checklist will help guide journalists on how best to protect their devices and the content on them.

- [ ] Set your devices, browsers, and apps to update automatically.
- [ ] Encrypt your computer. Mac users can enable FireVault, and Windows users can turn on Bitlocker. For Linux operating systems, turn on LUKS.
- [ ] Encrypt your phone. To turn on encryption for an Android phone go to *Settings > Security > Encrypt phone*. iPhones have been encrypted by default since 2014.
- [ ] Encrypt your iCloud account by turning on Advanced Data Protection.
- [ ] Create a process to regularly audit the information stored on your devices and backup and remove any data that you would not want others to access.
- [ ] Move sensitive data and backups onto an external hard drive and encrypt that drive.
- [ ] Lock your devices with a password or PIN code. Avoid securing devices with biometrics if you are crossing borders or if you are concerned about having your devices searched or seized.
- [ ] Review the app settings on your devices and limit what data they can collect.
- [ ] Remove any non-essential apps from your devices.
- [ ] Power off your devices when they are not in use, including at night.
- [ ] If you are concerned about being targeted by spyware, turn on Lockdown Mode for all Apple devices linked to the same iCloud account.
- [ ] If you have an Android phone, power it down and restart it at least once a day to remove malware, including spyware.

Editors and journalists should consult CPJ's Digital Safety Kit for more information.

emergencies@cpj.org

Issue date: February 24, 2026

CPJ