CRISIS READY MEDIA
SAFER JOURNALISTS. STRONGER STORIES.

DIGITAL SECURITY INFOSHEET

Digital hygiene basics

Your devices, accounts and communications hold your sources, your reporting and your location. Secure them before the assignment, not during it.

1 Start with your risks

Your plan should fit your threats

No single setup fits every journalist. Before an assignment, ask:

- [ ] What is on my devices, and which accounts are they logged in to?
- [ ] Who might want that information, and how likely are they to get it?
- [ ] What could they do with it?
- [ ] Which details, such as identities, must be protected before publication?

Your answers decide which defenses matter most.

2 Lock down your accounts

Start with your email

- [ ] Check haveibeenpwned.com for breaches. Change any breached password and never reuse it
- [ ] Use a password manager to create a long, unique password for every account
- [ ] Turn on two-factor authentication (2FA) everywhere it is offered. 2fa.directory lists instructions
- [ ] Print backup codes and store them where you can physically reach them
- [ ] Use passkeys where a service supports them

GOOD	BETTER	BEST
Text-message codes. Can be intercepted by SIM swapping.	Authenticator app. Works without cell service.	Security key. Resists phishing.

3 Secure your devices

Phone and computer

- [ ] Turn on automatic updates for the operating system and apps
- [ ] Turn on full-disk encryption: FileVault on a Mac, BitLocker on Windows
- [ ] Set a long passcode. iPhones are encrypted once a passcode is set. Modern Android phones are encrypted by default
- [ ] Review app permissions. Delete apps that want access they do not need
- [ ] Back up your devices before the assignment
- [ ] Encrypt external drives and USB sticks that hold reporting material

4 Protect your communications

End-to-end encryption by default

- [ ] Use an end-to-end encrypted app such as Signal for messages, voice and video
- [ ] Set a Signal PIN, and a username so you do not have to give out your phone number
- [ ] Turn on disappearing messages for sensitive conversations
- [ ] Hide message content from lock-screen notifications
- [ ] Verify safety numbers with key contacts, in person or over a second channel
- [ ] On WhatsApp, turn on the stronger security settings. They are not on by default

KNOW THE LIMITS

Encryption does not protect an unlocked phone in someone else's hands, or a device with malware on it.

5 Spot phishing

Links, logins and attachments

- [ ] Do not trust the sender name alone. Watch for lookalike addresses that are off by a letter or two
- [ ] Hover over a link, or long-press on a phone, to see where it really goes. Do not open shortened links
- [ ] If an email asks you to log in, type the site's address yourself
- [ ] Do not open unexpected attachments. Ask the sender to paste short text into the message instead
- [ ] Be suspicious of any message that pressures you to act immediately
- [ ] Turn off automatic image loading in your email. Images can reveal when you open a message
- [ ] Share these tips with your team. One compromised account puts everyone's sources at risk

Crisis Ready Media
Safer journalists. Stronger stories.
A 501(c)(3) nonprofit. EIN 93-4927139.

54 Danbury Road, Suite 412, Ridgefield, CT 06877
1-855-NEWS-911 | crisisreadymedia.org
Support this work: donate.crisisreadymedia.org

6 Before a high-risk assignment

Protests, civil unrest and anywhere devices may be seized

- [ ] Consider a secondary phone that is not logged in to your personal accounts
- [ ] Turn off fingerprint and face unlock, and use a long passcode. Weigh this against cameras that could capture you typing it
- [ ] Call and text over Signal, not standard calls or SMS
- [ ] Share your location and contact information with colleagues before you go
- [ ] Carry an external battery that can recharge your phone two to three times
- [ ] Keep memory cards and drives on your person. Most cameras cannot encrypt what they record, so back up as soon as you can
- [ ] Blur faces before publishing when identities need protecting

> **ANDROID USERS**
> Encryption takes full effect only after the phone is completely powered down, not in sleep mode.

7 Control location and metadata

Your phone and your files say where you have been

- [ ] Turn off location services around sensitive events, or switch apps from precise to approximate location
- [ ] Turn Wi-Fi and Bluetooth off in Settings. The control center toggle does not stop the signals
- [ ] Remove metadata from photos and documents before you share them
- [ ] Do not tag posts with your location, and check photo backgrounds for clues
- [ ] Use a trustworthy VPN on networks you do not trust
- [ ] Avoid logging in to your accounts on a source's network. Your IP address can link you to them

Airplane mode does not block location services. Only a full power-off stops cell tower tracking.

8 Shrink your footprint

Prepare for online harassment before it starts

Defenses are far easier to build in advance than in the middle of an attack.

- [ ] Search for yourself. Map what is public: home address, phone, family, old accounts
- [ ] Send opt-out requests to data broker sites that list your personal details
- [ ] Tighten privacy and security settings on your social media accounts
- [ ] Write a response plan: who you tell, how you document abuse and who covers for you

9 Protect your sources

Their risk is not the same as yours

- [ ] Give sources a safe way to reach you first. Publish a Signal username, not a phone number
- [ ] Remember that encrypted chats still produce metadata: who contacted whom, and when
- [ ] Check files a source sends for hidden metadata before you share or publish them
- [ ] Ask how a transcription or cloud service stores your audio and files before you upload sensitive material

DIGITAL SECURITY EMERGENCY

Access Now's Digital Security Helpline is free and available 24/7 for journalists: accessnow.org/help

ARRESTED OR DEVICES SEIZED

Contact a lawyer immediately. Ask for your attorney, and ask that questioning stop until you have spoken with one.

This infosheet is general guidance and does not replace training or a risk assessment for your assignment. Tools and settings change, so confirm current instructions before you rely on them. November 2026.

Crisis Ready Media
Safer journalists. Stronger stories.
A 501(c)(3) nonprofit. EIN 93-4927139.

54 Danbury Road, Suite 412, Ridgefield, CT 06877
1-855-NEWS-911 | crisisreadymedia.org
Support this work: donate.crisisreadymedia.org