JOURNALIST TOOLKIT

Reporting on Addiction

HOW-TO: DIGITAL SECURITY

A beginner's guide to protecting yourself and your sources online

Protecting ourselves and our sources is more important than ever.

In today's digital climate, journalists must be hyper-vigilant. We **must prioritize the protection of our data and identifying information** to safeguard our sources, preserve the integrity of our investigations and prevent potential reprisals. Securing communications and information allows journalists to protect the confidentiality of sensitive sources and materials and to thereby uphold journalistic ethics and principles of trust. Having secure communication channels allows us to **offer a safe environment for individuals to come forward with crucial information without fear** of retaliation, ultimately serving the public interest by exposing wrongdoing and holding those in power accountable.

Recommended Tools

- Proton - encrypted email
- Signal - encrypted messaging
- SecureDrop - securely transfer files
- DeleteMe - remove personal info online

This resource was created in consultation with digital security experts, including journalists who report on democracy, extremism and politics, and have frequently interacted with whistleblowers.

View more resources at reportingonaddiction.org.

CONDENSED CHECKLIST

for the Fundamental Digital Protection of Yourself and Your Sources

□ Use a password manager, secure passwords/passkeys and two-factor authentication to protect each account.

□ Monitor the personal information you put online, through social media posts, email content and other places that could be breached.

□ Be cautious who you share personal information with.

□ Know who you're talking to by confirming your sources identity - online and in person.

□ Use a VPN.

□ Review, maintain and scrape the files located on your cloud-based storage.

□ Keep professional and personal digital ecosystems separate.

□ Be cautious when using transcription services and aware of who can access your transcriptions.

□ Review the privacy and security settings on services and platforms you use.

Continue reading for additional context and recommendations ▶

EXPANDED CHECKLIST

□ Use a secure password manager and set up two-factor authentication to protect your accounts.

- Password managers will keep track of your passwords and passkeys, security questions/answers and any other critical account information.
- Use a different password for each account. Make your password at least 16 characters. Your password manager can suggest secure passwords.
- AVOID:
  - Passwords obtained from previous breaches.
  - Dictionary words.
  - Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd').
  - Context-specific words, such as the name of the service or username.
- For two-factor authentication use an authenticator app or hardware key. It is not recommended to use SMS for two-factor authentication.
- Do not share your passwords.
- When creating security questions – LIE. Your answer can be anything, and the password manager will remember it for you. Do not choose an answer that can be easily found online (such as your mother's maiden name or your high school).
- If your information has been breached or compromised, update you password or passkey ASAP. Your password manager or email server may monitor breaches for you. You can also check **haveibeenpwned.com/** for breaches.

□ Monitor your social media and email footprints.

- There's a lot of pressure on journalists, particularly freelancers, to have a prominent social media presence and be easily accessible through digital accounts. While sharing information can help build trust within your community, it also could put you in harm's way. Do not share photos/information that could identify personal details about yourself or loved ones, or your physical location, like your home or a coffee shop you frequent. The more social media accounts you have, the more accounts you need to manage.
  - This is also true for your sources. Discuss this with sensitive sources – have them do a social media audit prior to a story publishing to ensure personally identifying information isn't publicly available.

□ Be cautious who you share personal information with.

- Be mindful that when sharing your phone number or email, it can be used to find even more personal details about you, such as your address and your voting record.
  - Use the same considerations for the personal information you include in email footers!

□ Know who you’re talking to.

- Bad-faith actors online can use deep fake artificial intelligence technology, but there are also lo-fi ways to scam people or spoof their identities that are becoming increasingly common. Take whatever measures you can to identify in advance who you’re interacting with – through background research or potential mutual acquaintances. We also advise that, whenever reasonably possible, you meet with sources in person – this is the best way to ensure they’re who they say they are. You can also have an agreed-upon passphrase you share with each other when meeting in person as an added layer of security.

□ Use a VPN.

- Purchasing a reliable virtual private network (VPN) that will work on your mobile device and your computer provides an encrypted connection to the internet. This prevents your internet service provider from seeing your online activity by masking your IP address (unique device identifier).
  - **Learn more about selecting a VPN here, from the Freedom of the Press Foundation.**

□ Maintain your cloud-based storage.

- When you have a source upload something to cloud storage, you don’t want it to stay there indefinitely – both for their safety and yours. Regularly review and delete documents you no longer need. Be sure you don’t have anything in your cloud storage that you don’t want seen.

□ Protect your web browsers.

- Separate your professional digital ecosystem from your personal digital ecosystem. Consider using one browser for your work and another for your personal life. Separate emails. Separate phone numbers. This will avoid, for example, information being auto-filled that you don’t want to be exposed. And be aware that not all browsers offer the same level of privacy and security.
  - **Learn more about selecting a web browser here, from the Freedom of the Press Foundation.**

□ Be cautious when using transcription services.

- If you use a cloud-based transcription service in your newsroom, be aware that others in the newsroom might have access to it. Once a transcription is complete, we recommend downloading it and saving on an external hard drive, then deleting from the service.
  - **Learn more about selecting a transcription service here, from the Freedom of the Press Foundation.**

INTERACTING WITH WHISTLEBLOWERS AND OTHER AT-RISK SOURCES

/Know exactly how much exposure you already have before you move forward.

Have they called you? Are they using personal devices to communicate with you? Have they taken anything off a government or work device, transferred it to another device, then sent it to you? (In most cases, making a physical copy is best.) If you're dealing with somebody who's going to remain anonymous throughout the reporting process, you want to meet in person if possible, and be thoughtful about where you meet.

/There's a limit to how much you can tell your source about keeping themselves anonymous.

There's a line between, "I'm a journalist; you can send me documents," (legal) and "I'm trying to get you to steal government secrets" (illegal). That's a line you cannot cross. Educate yourself on what you and your sources are legally allowed to do. It varies from state to state.

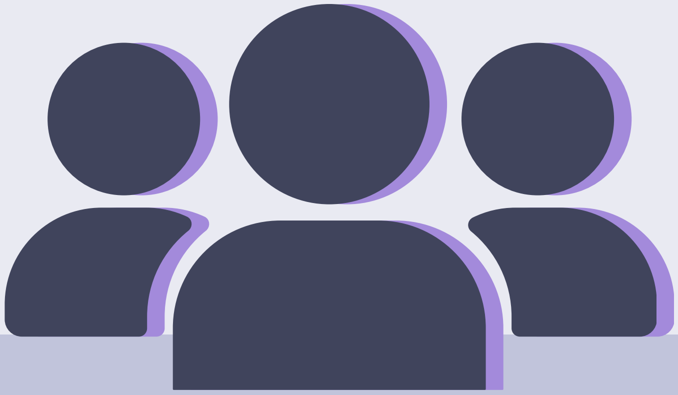
Learn more about confidential sources here, from Free Speech Center at MTSU.

/Learn everything you can about your sources in advance.

If they're a government employee, you're dealing with whistleblower protections that are legally protected. Be informed what they're allowed to tell you and what protections are in place for them to do so.

/If you've already communicated with this person digitally, assess what's out there and be aware that if there's a paper trail, all that could potentially be subpoenaed.

Again, always use VPNs on both ends and use an encrypted messaging service to protect yourself and your source.



TOOLS TO HELP PROTECT YOUR PRIVACY

/Proton uses encryption to secure sending and receiving email (to others with encrypted email) and in transmitting and storing documents. Proton doesn’t sell ads or share your information with advertisers.

- Offers mail, storage, calendar, VPN and password management services.
- Can send password-protected emails to non-Proton accounts.
- Can send password-protected documents.
- Note that when you send an email from a Proton account to a non-Proton account, it will not be end-to-end encrypted by default. You can see the encryption status of any message you send or receive by checking the lock icon in the “To” field. Non-proton users with PGP encryption can also be messaged with securely: **proton.me/support/how-to-use-pgp**
- *Offers free and paid versions on Android, iOS and desktop.*

/SecureDrop is a newsroom tool, used most frequently as a secure tips line. It’s used to securely “drop” files to the recipient. While it is a free service, it does require the purchase of hardware.

- Note that this service can be difficult to set up.

/Signal is a free (donation-based) app on Android, iOS and desktop. Signal uses end-to-end encryption that prevents the app and third parties from accessing your messages or calls. You can send secure individual or group messages, make voice and video calls, and share files. You can lock the app to prevent unwanted access. Signal allows for private usernames, so you don’t have to share your cell phone number. Additionally, you can set messages to disappear after a certain amount of time, as well as export and archive chats.

/DeleteMe is a paid service that removes your personal information from search engines and data broker websites for an entire year, after purchase. This service might be a good idea to use before publishing sensitive work.

- Note that pulling your information offline takes at least 7 business days (leave ample time for the program to run before publishing) and once your subscription expires, they will no longer scrape your information offline.

Organizations with Additional Resources

- Bellingcat
- Center for Investigative Reporting
- Coalition Against Online Violence
- Freedom of the Press Foundation
- International Women’s Media Foundation
- Investigative Reporters and Editors
- Pen America
- Privacy Guides
- Trollbusters

There are many more services your newsroom may use as part of its workflow and not all of them will be secure. When using services, make sure to familiarize yourself with its privacy and security features, create a secure password, and use two-factor authentication (if available).

About Reporting on Addiction

We are a 501c3-supported organization dedicated to increasing the accuracy and empathy of reporting on addiction. To accomplish this, Reporting on Addiction provides innovative training, technical assistance, and resources for journalists, journalism educators, experts through training, and experts through experience.

We work to:

- *Improve the themes/story narratives chosen by journalists.*
- *Improve the language used by journalists.*
- *Improve the images/videos created by journalists.*