thriv·ol·o·gy

Protecting Yourself From Hacking

A Starter Guide for Sex Educators

Practical strategies to help you protect your accounts, data, and devices from hacking

Hacking is when someone gets access to a digital system without permission. When you think of hacking, what might come to mind are large-scale attacks on organizations' sensitive data—like when hackers accessed a lab services database used by a health center and stole patient data in 2024.[1] However, it's important for sex educators to understand that hacking can also target individuals' devices or accounts. For example, Dr. Cindy Tsai, a physician with a large social media presence, said about her experience being hacked:

"My Instagram account was hacked, and I lost access to everything. I have heard stories about people getting hacked and never paused to think that it could happen to me. Until it did. Ugh."[2]

Teaching sex ed is powerful work, and you deserve to feel safe doing it—not just physically and emotionally, but also digitally. While there's still a lot to learn about sex educators' experiences of hacking, taking steps to stay safe online can support your overall well-being.[3]

As you read through the tips below, you may find that you're already taking steps to protect yourself from hacking! Starting to use even one new strategy in this tip sheet can help protect your privacy and security, keeping you in the work safely and sustainably.

Healthy Teen Network

Johns Hopkins
Center for Adolescent Health

Protecting access to your accounts is your best defense.

As a sex educator, taking steps to keep your accounts safe is crucial for guarding your sensitive data and possibly even information about the young people you work with.

Turn on multi-factor authentication.

Multi-factor authentication adds a layer of protection for your accounts by requiring you to prove it's really you in two or more ways to log in. For example, you might need to enter your password as well as a one-time code sent to your phone or email. This extra step blocks up to 99% of automated hacking attacks.[4]

Multi-factor authentication is often referred to as "MFA." Two-factor authentication ("2FA") is simply multi-factor authentication with exactly two verification steps.

There isn't a way to turn on multi-factor authentication across all your accounts at once. Start by enabling it in the individual accounts that are most important—like email, cloud storage, and that shiny, new password manager you just set up.

> *"I admit I did not have [multi-factor authentication] activated on social media, and this was the first thing I did after losing access. I used to roll my eyes when I had to do this for work and never thought it would be relevant in my personal life. But if you think about it, isn't your personal life even more important to protect?"*
>
> *-Cindy Tsai, MD[2]*

Use a password manager—consistently.

Since weak passwords are the most common way hackers get into accounts, a powerful defense is to use complex, unique passwords. But how can you do that when you might have dozens or hundreds of accounts across your work and personal life? Common approaches like reusing the same password across accounts, choosing simple and easy-to-crack passwords, or storing all your passwords in an unencrypted file (or written down on a sticky note) all make it easier for hackers to get in.[5]

A **password manager** solves this problem by storing all your passwords in one secure place, making it easy to consistently use complex and unique passwords.[6]

Option 1: Built-in password managers

These are built into your web browser (the app you use to search the web) or included with your device's software. Web browsers with built-in password managers include Firefox, Opera, Brave, Safari, Microsoft Edge, and Google Chrome. Apple devices (iPhones and Macs) come with the Passwords app, and Google devices (Android phones and Chromebooks) have a Password Manager app.

Pros

- Integrated into apps and platforms that you already use and are comfortable with.
- Quick to set up because they do not require new software or additional accounts.

Cons

- Less secure. Anyone who gains access to your device can see your passwords.
- Less functionality than a standalone password manager.
- May not work across all platforms.

Option 2: Standalone password managers

These are third-party apps that you must install and create an account for. Proton Pass, Bitwarden, 1Password, and KeePass are popular free options at the time of publication.

Pros

- Your most secure option. You must log in to access your passwords. This keeps them protected even if someone gains access to your device.
- Offer a wide range of features, including weak password alerts and reminders to update passwords.
- Work across many platforms. Many have browser extensions available that autofill password forms.

Cons

- Many require paid subscriptions to access their full functionality.
- Less convenient since you need to download an app and optional browser extensions to set them up, and you must log in to access them.
- Autofill may not work with some apps.

Which password manager is best? The one you'll actually use!

What's most important in a password manager (and all our other suggestions) is to find what works for you. Your needs and priorities are likely based on factors including how visible your work is, how risk-averse you are, and what resources you have available.

Try a standalone password manager if you prioritize security or work across multiple platforms and browsers. Choose a built-inoption if you prioritize convenience and mostly stick to one platform and browser.[7,8,9]

TIP:

For a password that's easy to remember but shockingly hard to crack, consider making up a passphrase! Passphrases are combinations of four or more random words such as "Be-Flower-Describe-Using" or "Improve.Aware.Boat. Horse."[10]

After securing your accounts, try out additional defenses.

Turn on automatic software updates for your devices.

Most cyberattacks target software vulnerabilities that your device's maker has already found and fixed. Turning on automatic updates in your device's settings ensures you get the latest security fixes.[11]

Switch to a privacy-focused web browser and search engine.

As a sex educator, you likely make searches that are more risqué than the average professional. Luckily, it's quick to switch to a free, private search engine and web browser that protect you from tracking and surveillance.

Search engines are software that let you type in a query and get results. As opposed to Google Chrome, privacy-focused search engines like DuckDuckGo and Brave do this without keeping logs of your search queries, browsing history, or clicks.[12]

These search engines work on many popular browser apps. However, you lose some of the privacy benefits if the browser itself isn't also privacy-focused. DuckDuckGo and Brave each have their own privacy-focused browser. Firefox is another safe browser that you can use with either search engine.[13]

Use encrypted messaging platforms.

When you text someone, that message is sent in plaintext that is readable to anyone who intercepts it. Luckily, encrypted messaging offers the solution.

Encryption is a way of encoding messages so that only you and the people you are messaging can read what's sent—not the app, phone company, or potential hackers. Some messaging apps encrypt only your message itself, while others can also encrypt metadata. Metadata is additional information about your message such who sent the message, who received it, and when.

Below are three popular free platforms for encrypted messaging.[14]

- **Signal:** Works across platforms and encrypts your metadata
- **WhatsApp:** Most widely used, doesn't encrypt metadata
- **iMessage:** Very secure choice if everyone involved is using an iPhone

To switch to an encrypted messaging platform, you'll need to download the app you choose, set up an account, and get your contacts to do the same. If you message someone on an app, they'll need to use the same one to receive it and respond.

Get a physical webcam cover.

Using a webcam cover is a cheap and easy way to protect yourself against hackers (or even some exploitative "free" apps) who record you when you think your camera is off. You can purchase a magnetic or sticker version for just a few dollars online, or even use a sticky note.

TIP:

Preventing hackers from listening in isn't as simple as protecting your camera. You can adjust your device's sound settings to mute your mic whenever you aren't using it, but if you're having particularly sensitive conversations offline, consider moving your devices to a different room.

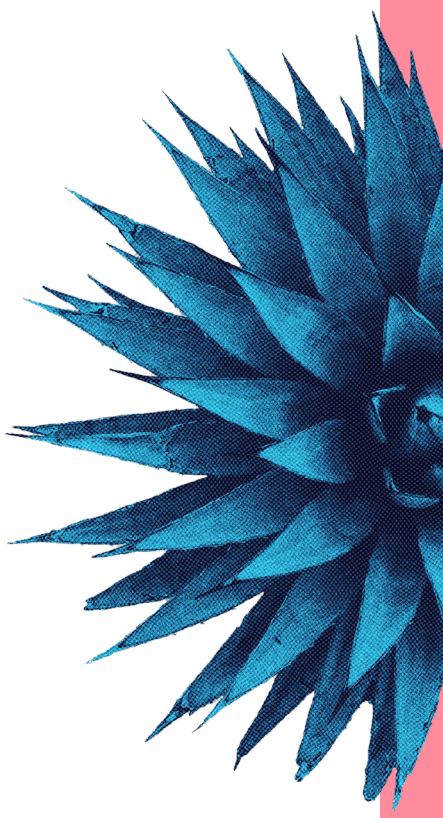
Avoid sharing sensitive information over public Wi-Fi networks.

Public Wi-Fi networks often aren't encrypted, which means that your web usage data is being sent in plaintext, making it easier for hackers and cybercriminals to see what you're doing online.

Encrypted websites have URLs that start with “HTTPS” (the “S” is for “secure”) instead of "HTTP."[15] You can tell whether a webpage is encrypted by looking at the URL or checking for a lock icon in the address bar.

If possible, try to avoid using public Wi-Fi by working offline or connecting to your phone’s wireless hotspot. If you need to use public Wi-Fi, avoid entering sensitive data (like account login-in information) and using unencrypted websites.[16]

Start by taking just one step from this guide. And remember: when you take steps to keep yourself safe, you're also safeguarding your ability to keep doing the important work of showing up for young people!



Additional resources

- Manging Your Personal Information Online: A Starter Guide for Sex Educators**:** This workbook by Thrivology gives you practical strategies to take control of the information that’s available about you online.
- Digital Safety Kit: A guide by the Committee to Protect Journalists that expands on the topics in this tip sheet. Also includes information on preventing targeted phishing attacks.
- What To Do After Getting Hacked: A guide from All Things Secured on five key steps to take right away if you’ve been hacked.
- Digital security for activists: A concise guide that includes information on threat modeling, which can help you assess risks and priorities.
- Cybersecurity and Privacy for Activists: An in-depth guide to help you build your security toolkit. Includes detailed information on threat modeling, using secure communications, and protecting your identity and anonymity online.

References

1. Alder, S. (2025, May 27). Planned Parenthood patients file lawsuits over laboratory services cooperative data breach. *The HIPAA Journal*. https://www.hipaajournal.com/laboratory-services-cooperative-class-action-lawsuits/
2. Tsai, C., MD. (2022, June 5). What I learned after being hacked on social media. *KevinMD.com*. https://kevinmd.com/2022/06/what-i-learned-after-being-hacked-on-social-media.html
3. SchoolSafety.gov. (June 2023). *Online safety resources for the K-12 community.* https://www.schoolsafety.gov/sites/default/files/2023-06/SchoolSafety.gov%20Online%20Safety%20Resource%20Infographic_June%202023.pdf
4. National Cybersecurity Alliance. (2025, January 17). *What is multifactor authentication (MFA) and why should you use it?* https://www.staysafeonline.org/articles/multi-factor-authentication
5. Cybersecurity & Infrastructure Security Agency. (2023, August 4). *Secure our world passwords tip sheet.* https://www.cisa.gov/sites/default/files/2024-09/Secure-Our-World-Passwords-Tip-Sheet.pdf
6. Tkacik, D. (2022, January 27). Why should we use password managers? We asked a security researcher. *CyLab Security and Privacy Institute*. https://www.cylab.cmu.edu/news/2022/01/27-password-managers.html
7. Freist, R. (2023, November 16). How to use your browser as a password manager. *PCWorld*. https://www.pcworld.com/article/2127903/browser-as-password-safe-better-than-classic-password-managers.html
8. Key, K. (2025, January 15). The best free password managers for 2025. *PCMAG*. https://www.pcmag.com/picks/the-best-free-password-managers
9. UMA Technology. (2025, January 11). *Your browser's password manager may not be as safe as you think.* https://umatechnology.org/your-browsers-password-manager-may-not-be-as-safe-as-you-think/
10. Australian Signals Directorate. (2023). *Set secure passphrases.* https://www.cyber.gov.au/learn-basics/explore-basics/passphrases
11. Cybercrime Support Network. (2022, October 3). Automatic updates: The benefits and how to turn them on. *FightCybercrime.org*. https://fightcybercrime.org/blog/automatic-updates-the-benefits-and-how-to-turn-them-on/
12. Oliver, G. (2025, July 28). The 20 best private search engines to use in 2025. *PrivacySavvy*. https://privacysavvy.com/security/safe-browsing/private-search-engines/

13. Muchmore, M. (2025, May 24). Lose the trackers: The best private browsers for 2025. *PCMag*. https://www.pcmag.com/picks/stop-trackers-dead-the-best-private-browsers#

14. Aten, J. (2025, March 27). Signal, WhatsApp, and iMessage: Which messaging app is most secure? *Inc*. https://www.inc.com/jason-aten/signal-whatsapp-and-imessage-which-messaging-app-is-most-secure/91167562

15. Hashim, A. (2025, September 8). HTTP vs. HTTPS: What are the differences to know? *PrivacySavvy*. https://privacysavvy.com/security/safe-browsing/http-vs-https/

16. Federal Trade Commission. (2022, February 9). How you know your information is safe when you're using a public wi-fi network. *Consumer Advice*. https://consumer.ftc.gov/node/78344

Suggested citation

Brahm, C. B. & Rodriguez-Anello, J. B. (2025). *Protecting yourself from hacking: A starter guide for sex educators*. [tip sheet]. Healthy Teen Network. https://www.HealthyTeenNetwork.org/Thrivology/Resources/protecting-yourself-hacking

Acknowledgments

Thank you to everyone who helped this resource come to fruition. Research Alliance members Amber Barcel, Isaiah Lawrence, Jaclyn Friedman, and Lauren Lapointe shared important insights to make this a useful and usable resource through interviews and multiple rounds of reviews—thank you all! Thank you to our colleague Megan Thomas for your stellar visual design work, and to Nicholas Sufrinko and Gina Desiderio for your thoughtful branding and dissemination guidance. We extend our thanks as well to Milagros Garrido and Mackenzie Piper for their help in conceptualizing and planning for this resource. Finally, we are deeply grateful to our colleague Randa Dean for her guidance, support, leadership, and all the rounds of reviews that were needed to bring this resource to its final form.

Thrivology is supported by the Office of Population Affairs (OPA) of the U.S. Department of Health and Human Services (HHS) as part of a financial assistance award (1 PHEPA000006-01) totaling $1,168,985 with 100 percent funded by OPA/OASH/HHS. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement by, OPA/OASH/HHS, or the U.S. Government. For more information, please visit opa.hhs.gov.