

DATA THAT ISN'T COLLECTED CAN'T BE STOLEN, SOLD, OR USED TO CAUSE HARM.

Physical access to digital spaces also matters. Screen volunteers, limit access to workspaces, and require sign-ins for visitors.

Establish shared security practices for staff and volunteers, covering communication, accounts, devices, web use, and app choices. Make training ongoing, not one-off.

Limit data collection to what's necessary, and always explain how it's used. Consent isn't optional.

Who can access it?

Where is it stored?

Do we actually need this?

Digital safety is collective care. The way your organization handles data can protect people — or put them at risk.

TAKE A COLLECTIVE APPROACH TO DIGITAL CARE

YOUR DATA YOUR DECISIONS

The safest digital spaces are the ones we build together. Encrypt, limit exposure, and protect each other.

For more digital safety tips:



Delete the clutter. If you don't need an app, delete it. Limit unnecessary permissions — your voice memo app doesn't need your location.

APPS

Turn off or delete browsing history, reject unnecessary cookies, and limit third-party tracking and targeted ads.

WEB BROWSERS/SEARCH ENGINES

Review app permissions to limit access to your contacts, photos, call logs, messages, camera, microphone, and location.

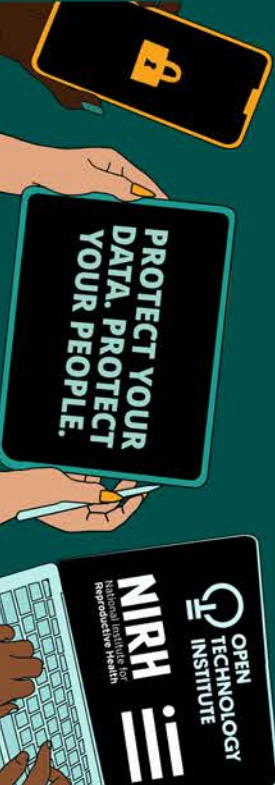
DEVICES

Remember to regularly update at all levels!

Default settings are designed for data collection, so make sure to customize them with your privacy in mind.

DITCH THE DEFAULT TAKE CONTROL OF SETTINGS

TOP DIGITAL SAFETY & PRIVACY TIPS FOR ADVOCACY ORGS



FOR ORGS:

- Limit who has access to accounts and audit regularly
- Get consent before sharing photos or stories
- Think before sharing staff information on websites
- Talk openly with staff and volunteers about online safety

Check your profile settings:

- Platforms collect and share personal data
- Data brokers sell your data
- Online details can fuel harassment or doxxing

You can't be invisible online, but you can choose to share less. Because:

- A screen name is better than a real name
- Hide personal info
- Set accounts to private (when possible)
- Don't reveal your location in your profile pic
- Limit old posts and tagged photos
- Speak with friends and family about what they share

PROTECT YOUR POSTS AND YOUR PEACE!

ENCRYPTION IS KEY

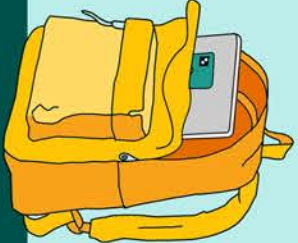
Encryption helps you communicate securely. It scrambles your data so only the right people can access it.

For sensitive conversations, choose end-to-end encrypted apps with added privacy, like Signal or Proton Mail, to keep your chats private.

You can even turn on disappearing messages to add another layer of protection against older data being exposed.

Don't forget your devices!

Turn on full-disk encryption so if they're lost, stolen, or seized your data stays locked up.



REMEMBER: IF IT'S NOT ENCRYPTED, IT'S EXPOSED!

PHISHING = DIGITAL TRICKERY. DON'T BITE.

- Don't open unknown attachments from unknown senders!
- Don't respond to spam or suspicious messages!
- Report and flag anything suspicious

Avoid public wifi or hotspot networks, but if you need to use them, use a VPN to keep your web activity private.

Limit online tracking with privacy-focused tools. Recommendations and tools can change, so stay updated on browsers, search engines, and VPNs.

DON'T GET PHISHED! Scammers count on urgency. Pause before you act.

SURF SMART

STRONG PASSWORDS AND 2FA SINGLE-FACTOR LOGINS

- Use loooong complicated passwords
- Update passwords regularly
- Never reuse passwords across accounts

No one can manage all their passwords by hand.

Let a password manager do the work — you just need to remember one strong password.

- Other password helpers: Diceware, Code/word generators, Hardware tokens
- Turn on two- or multi-factor authentication (2FA) wherever possible.