CYBERSECURITY DURING CHRISTO-FASCISM

v1. 11/2024

Digital safety tips for Kinksters, Women, & Queer and Trans Folks!

RESOURCES TO LEARN MORE

Make a throw-away Reddit account, protect your password, and looking into these subreddits from your TOR browser:

- r/privacy
- r/cybersecurity_help
- r/self-hosted

Also use your TOR browser to check out https://ssd.eff.org

Pass this zine around & stay safe!

ENCRYPT YOUR FILES

Encrypting files or folders means requiring a password to open them, or else the data can't be read. This protects your data from people who gain access to your device. Free or low cost software you can use to encrypt includes **Microsoft OneDrive** and **VeraCrypt.**

Consider encrypting nudes, BDSM photos, healthcare documents, digital diaries, etc.
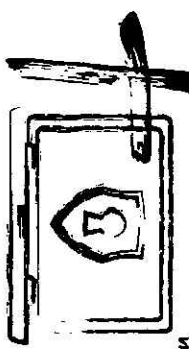
WARNING!

PASSWORDS

The Christo-facist state and its sympathizers can decrypt password-protected files, devices, and accounts. Here's how you make it harder for them.

- Choose a long, unique phrase for each password.
- Use a PINs + a biolock on devices when ever possible. FYI the police are allowed to forcibly use your face or fingerprint to unlock your devices, so use a PIN, too.
- Keep track of passwords in a paperwork notebook - maybe disguising it as a regular book in your home. Or use a digital password manager like **Bitwarden** which allows you give your keys to a trusted contact in case of an emergency who can then back up

---

TEXTING/CALLING/EMAILING

The most secure communication method is in person, then phone calls, then emails or texts. When you must email or text, switch to end-to-end encrypted applications.

End-to-end encryption is a way of securing messages so that only the sender and recipient of a message can read it, not for instance, the company who runs the service.

You want to choose applications like **Protonmail** for emails and **Signal** for texts and phone calls that are built to use end-to-end encryption.

OTHER TIPS

- Carefully review the security settings of the sites and devices you use and select the most private options you can. For ex: set your social media accounts to be private/unsearchable.
- Be cautious what info you share online anyway, even privately in DMs. All apps and websites can be exploited: a researcher famously found a severe vulnerability in Fetlife in 2023.
- **Be careful who you trust with your stories, your photos, and your experiences. When in doubt, vet people before sharing personal information.**

CENSORSHIP & BOOKS PART 2

Libraries are not as secure as they once were about protecting patron's borrowing history from the State, particularly with borrowing e-books. But you can still read any physical book in a library without checking it out if you are very worried about that.
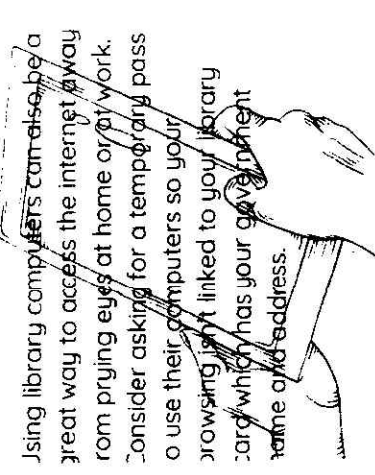
Using library computers can also be a great way to access the internet away from prying eyes at home or at work. Consider asking for a temporary pass to use their computers so your browsing isn't linked to your library card/ which has your government name and address.

I'M NOT TECH SAVVY!

Don't worry: this zine is for you! Read this zine to learn basic cybersecurity terms and practical tips for securing the communications and devices of people who are targeted by the Christo-fascist Nation State and its actors, especially kinksters, women, queer and trans people.

PLEASE NOTE!

PART 1

The Christo-fascist State is well practiced in banning or censoring parts of books. Did you know that ebooks are also not safe? That's because you don't actually own them. When you "buy" an ebook, you're actually paying to "license" the content on your device. This means the government can force a publisher to change or remove your ebook at any time.

To avoid this, you need to strip the Digital Rights Management (**DRM**) software out of your ebook files. **Calibre** is a free software for your computer that strip DRM from your ebooks and also help you manage the files and load them onto your devices.

---

1. Make a list on paper of what parts of your life are threatened by the Christo-fascist State. (For ex: do you need abortions? Do you need to research health care guides for kinksters? Or organize to support trans rights?)

2. Consider how you use digital tools (like texting, laptops, or ebooks) to access and engage with these parts of your life. Think of these digital tools as vulnerabilities into private parts of your life that you need to secure.

3. Try applying the safety tips in this zine for the tools you use! And ask experts on the subreddits listed in the back if you need need.

Police can and have forcibly used peoples' face or fingerprints to unlock devices. So use a password or PIN in addition to a bio-lock like those.

Check your device's security setting ensure you:

- Have auto-lock turned on
- Wipe data after a certain number of incorrect password attempts
- Have all updates downloaded and installed. Updates contain patches that fix various security

---

HIPPA does *not* apply to fertility and period tracking apps! So it's best to track your cycles by hand either on paper, or in an encrypted notes app like **Turtl**.

This is especially important for data that can reveal abortions or miscarriages. If you have medical emails, photos, or documents relating to these, consider encrypting them!

While the Christ-fascist State is poised to become stronger, it has already targets kinksters, women, and queer & trans people. For ex:

- **38 states have "foetal assault laws" and can (and do) charge people for miscarrying.** Look up Brittany Poolaw's case.
- **19 states still allow conversation therapy,** including kidnapping trans and queer minors to the camps.
- **BDSM falls into odd legal gray areas** where it's allowed on paper, but various state laws can still punish people for impact play, owning handcuffs, swinging while married, or having BDSM in one's past while fighting for child custody.

Every time you Google something, you leave a trail of what you were searching for. Keep your online browsing and website visit history private by using the free **Onion Router (TOR)** which protects your privacy by sending your data through encrypted layers.

Some websites (like banks) won't let you access them using TOR because a Christo-fascist state assumes anyone seeking privacy is a criminal. Whenever you must use a "regular" browser, use **DuckDuckGo**, plus a Virtual Private Network (VPN) to mask your IP address. There are many VPNs tailored to what you need. **TOR offers a free VPN, too.**

Doxxing means sharing personal information online that identifies who someone is, or where they live, work, etc. **When in doubt, don't share information about yourself online.**

If you must share photos, check that they don't reveal your tattoos, ID info on a pet collar tag, landmarks near your home, or other info that could doxx you. Strip the metadata attached your photos that shares where and when and how the photo was taken by using free EXIF-remover software like **EXIF Cleaner.**

Don't forget to review old photos and social media posts for personal

---

1. These tips can't keep your data 100% safe from a Christo-fascist State or its actors, but they can help you become safe-r. The next page has resources to help you dive deeper into these topics.

2. When it comes to privacy, cash and paper are still king. When in doubt, don't post it or say it online

3. The more people who encrypt their files, browse using TOR, and talk about cybersecurity in general, the harder the State and its actors have to work to hurt us. So share this zine with your friends! More paper or digital copies are availab at **decolonizationcoven.com**

Protect your data to protect yourself.