

print your own from
zines.headingnorther.com!

@headingnorther
@heading_norther

Questions? Compliments? Corrections?

headingnorther@protonmail.com



September 14th 2020

from southeastman and
headingnorther

Digital Security FOR PORTLANDERS

VOL III

Learn to manage
your overwhelming
internet dread!

Contains homework
(there may be
a test)



CITATIONS

1. "What Should I Know About Encryption?" Surveillance self-Defense, Electronic Frontier Foundation, March 7, 2019.
2. "Communicating with Others." Surveillance Self-Defense, Electronic Frontier Foundation, June 9, 2020.
3. "Keeping your Data Safe." Surveillance Self-Defense, Electronic Frontier Foundation, November 12, 2019.
4. "Attending a Protest." Surveillance Self-Defense, Electronic Frontier Foundation, April 1, 2019
5. Scott, Tom. *This Video Is Sponsored By █ VPN*, 2019
6. "Choosing the VPN That's Right For You." Surveillance Self-Defense, Electronic Frontier Foundation, April 2, 2019.
7. "Why Metadata Matters." Surveillance Self-Defense.
8. "Why Metadata Matters." Surveillance Self-Defense.
9. "Attending a Protest." Surveillance Self-Defense.
10. Quintin, Cooper. "A Quick and Dirty Guide to Cell Phone Surveillance at Protests." Electronic Frontier Foundation, June 25, 2020
11. "Doxcare." CrimethInc, August 26, 2020
12. "A Guide to Doxing Yourself on the Internet." The New York Times
13. Bazell, Michael. *Extreme Privacy: What It Takes To Disappear: Intel Techniques*. 2.5 ed., 2020
14. "Your Security Plan." Surveillance Self-Defense, EFF, April 1, 2019
15. "Activist or Protester?" Surveillance Self-Defense, EFF, April 1, 2019
16. "Credit Freeze FAQs" FTC Consumer Information, September 24, 2019

FURTHER READING

- The EFF's website is an amazing resource with a lot of information we didn't have room to get into. Check out their Surveillance Self-Defense Guide (ssd.eff.org), maybe read an article about securely deleting your data.
- If you'd like to know more about doxxing & its aftermath, read the CrimethInc "Doxcare" article.
- If you like podcasts, check out Reply All episodes 130: The Snapchat Thief and 97: What Kind of Idiot Gets Fished?

ACTIVITY SECTION

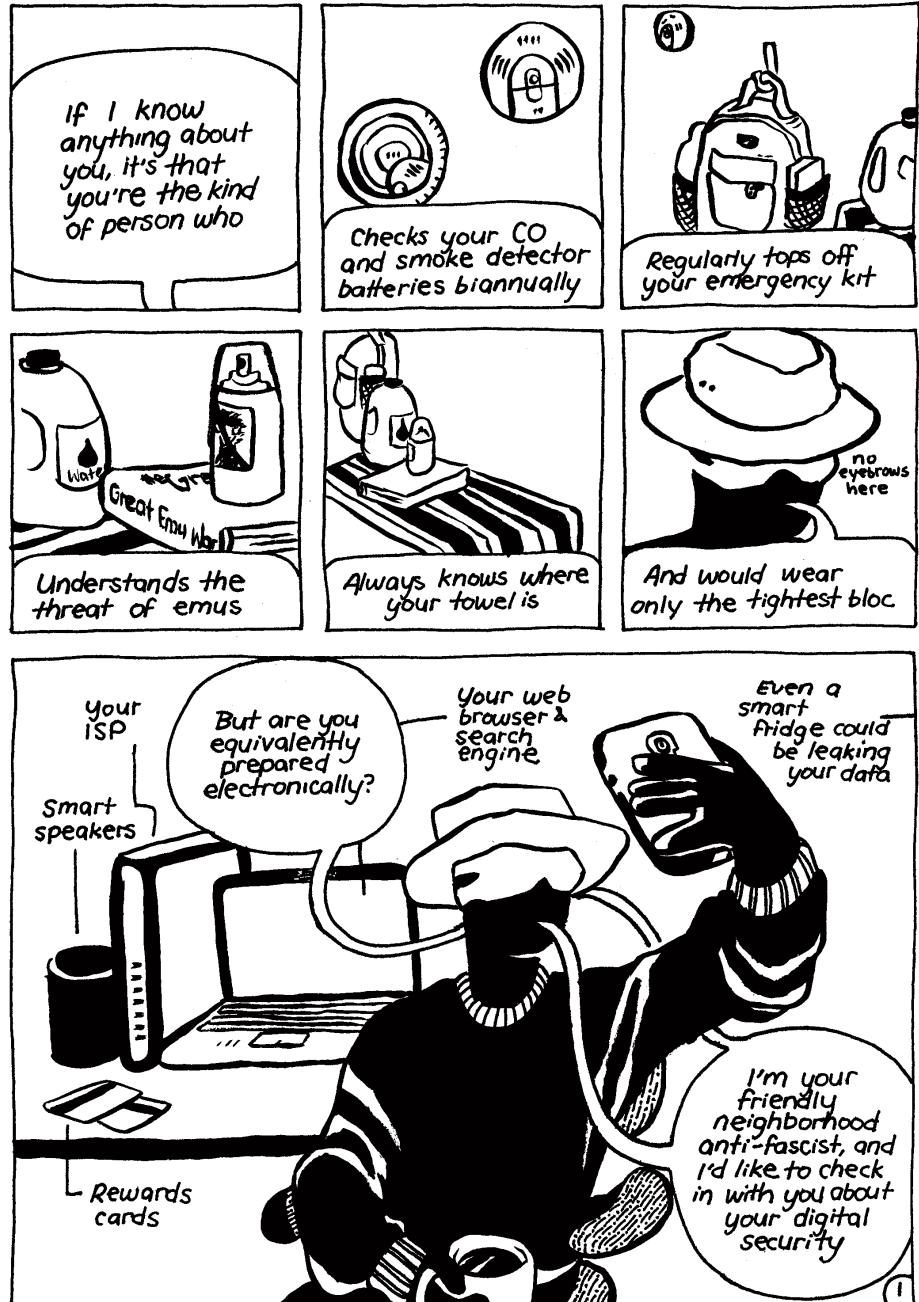


You should do this today!

Digital Security Action Items

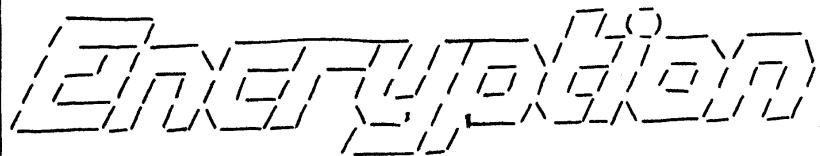
- Get a password manager & change all your passwords to secure, randomly generated ones. (Consider Dashlane, 1Password, or LastPass)
- Check your emails at haveibeenpwned.com to see what data breaches you've been involved in and prioritize changing those passwords
- Sign up for services with a different email from the one you use for essential accounts (bank, etc)
- Turn on 2-factor authentication everywhere (and use an authenticator app or Yubikey rather than your phone number)
- Lock your credit (only unlock for credit checks) (For instructions, look at the FTC site in citations)¹⁰
- _____

Thanks for reading
and see you next time!



000 fnaf@home

(When Alice and Bob wish to talk to each other very badly, they turn to)



/ \ / ncryption matters when you're sending data
/ \ / that has the potential to be inspected by
/ \ / uninvited third parties. It works by making
this data look like gobbledegook to those without the
decryption key. Encryption is everywhere-- from your
bank account to your interaction with nearly every
website you visit. (Terms like 'military grade
encryption' don't mean much-- modern encryption
standards are 'military grade')

/ \ / Communication: for messaging and email you want
/ \ / END TO END ENCRYPTION where your messages are
/ \ / encrypted both on their way from your phone to
whoever you're talking to, and also encrypted from the
app you're messaging on, so the app's servers can't
see them. That way even if your messaging service is
subpoenaed or hacked there's nothing to see.²

-- INSERT --

THREAT ASSESSMENT

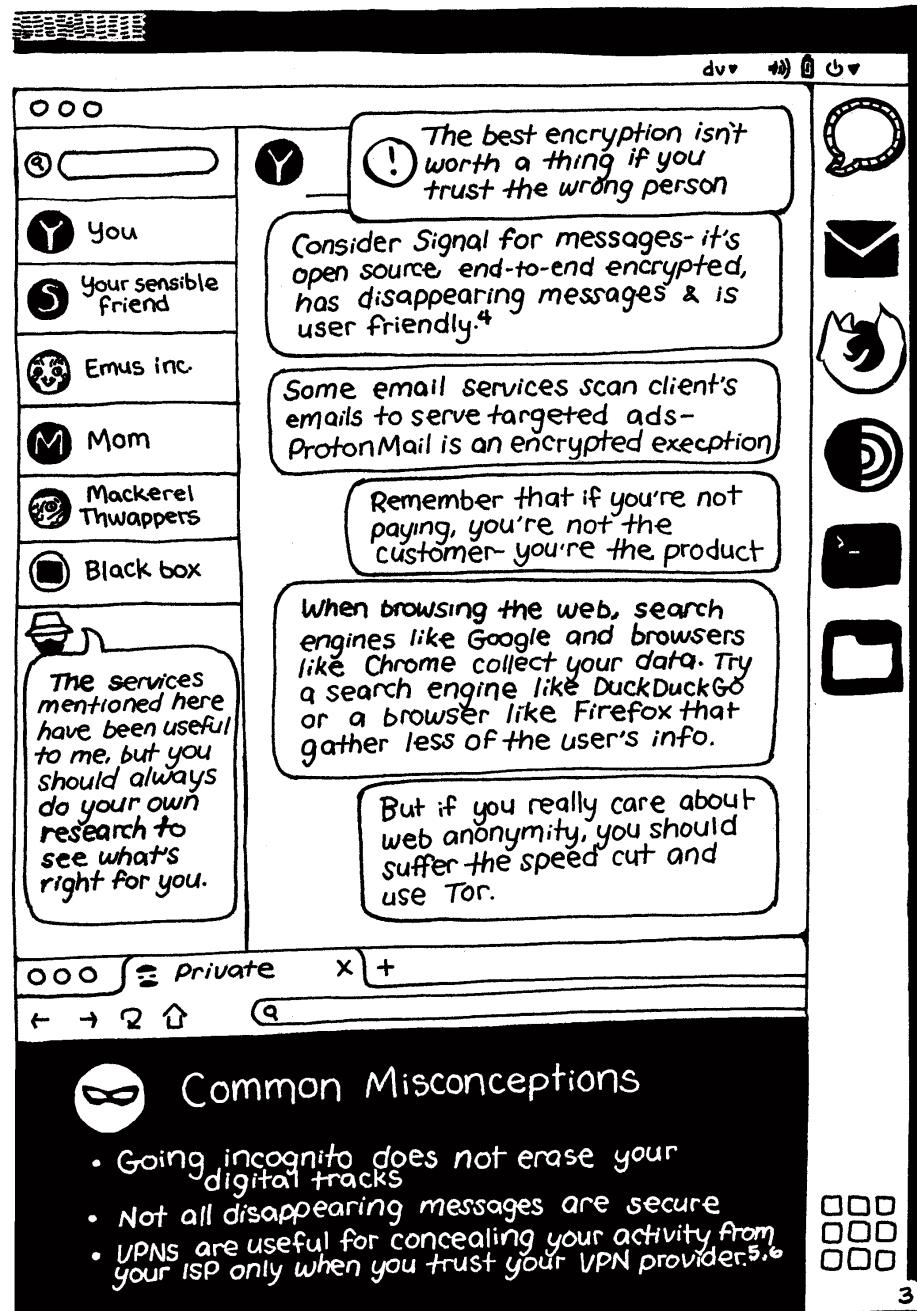
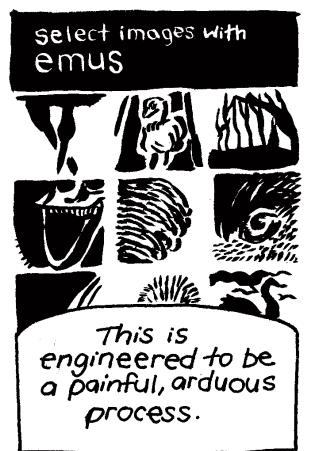
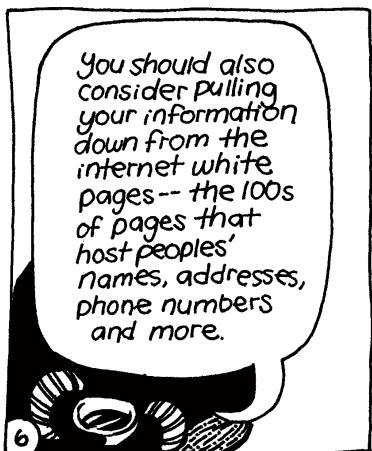
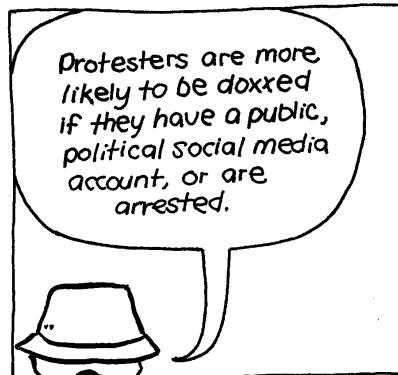
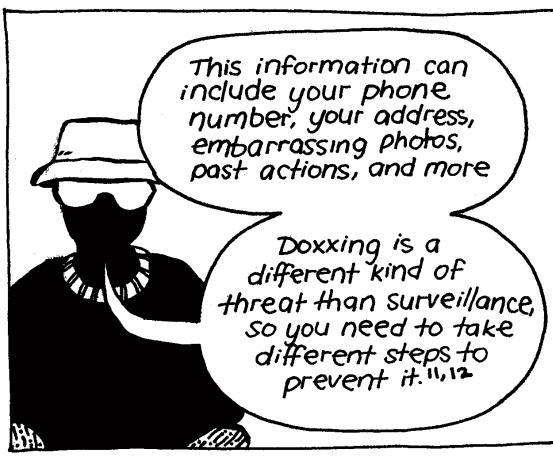
The Electronic Frontier Foundation (EFF) suggests asking:¹⁴

- What do I want to protect?
(messages, location, passwords)
 - Who do I want to protect it from?
(people, the government)
 - How bad are the consequences if I fail?
(humiliation, arrest, assault)
 - How likely is it that I'll need to protect it?
(do you have a public presence? been victim of a breach?)
 - How much hassle am I willing to go through?
(having a secret phone number is a lot of work, for example)

For more information, check out the EFF's digital security guide for activists in the citations.¹⁵

I've never done anything illegal-- why should I care about internet security?

- You could still be targeted by malicious actors
 - If you're secure, then the people around you—your friends, neighbors, contacts—will be more secure, too
 - Security shouldn't be a precaution—view it as a right



Have you heard about METADATA?

DOMINO'S calls	home 2am
Q youshould havebeen preparing foremuis.gov websites	home 2:30am
Your Sensible Friend	home 2:34am
[redacted]	2:39am
[redacted]	2:43am
text logs	
2x throw net \$39.98 VISA	2:50am
credit card transactions	

Your personal data - the contents of your texts and calls, your photos and emails are protected and require a warrant to search. It's hard, if not impossible, to see this data w/out physical access to your device.

Your metadata is not so well protected. Metadata is everything except for the content of your data - it's the data about your data. This includes timestamps, subject lines, geolocation, who you call, the websites you visit.⁷ Much of this information is stored by your ISP and could be accessed without your knowledge.

Legal precedent concerning metadata remains uncertain. Different police departments and courts have different standards.



Photos include the time they're taken & the location they're taken at, which is visible to anyone with the image. One easy way to remove this metadata is to send the image to yourself through Signal.⁸

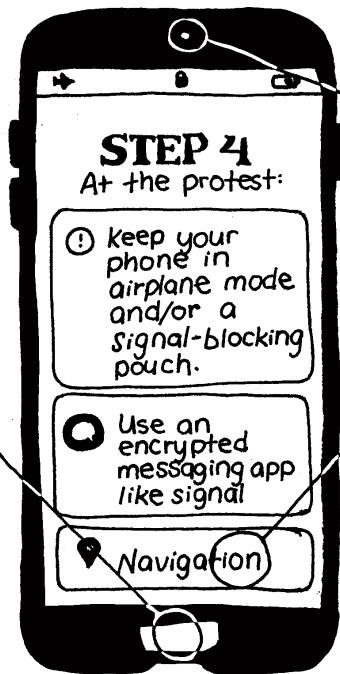


You know Google Docs saves your edit history, but did you know Word does too? Next time, consider a PDF.

SO YOU BROUGHT YOUR PHONE TO A PROTEST⁹

STEP 1. Reconsider: Try a brief digital detox, or acquire a phone without your personal information that you only turn on at protests

STEP 2. So you'll bring a phone: Assume it will be confiscated. Remove any sensitive data from it (messages, images, etc)



STEP 3. Turn off biometrics: Unlock your phone with a long, random pin - not your face (cops can't legally search your phone w/out a warrant)

STEP 5. Think carefully before you film: Are you documenting or protesting? If you film, do it while your phone is locked.

STEP 6. Heading home: If you'll need a map, download it beforehand and navigate with your phone still in airplane mode (GPS is receive-only)

YOU MAY ENCOUNTER¹⁰

- Cheap devices that mimic WiFi networks and intercept all activity on them - always be suspicious of open networks and never connect at protests.
- Stingrays mimic cell phone towers and collect any outgoing data from your phone - texts, calls, location, searches... They're usually operated in vehicles.
- Dirtboxes, a similar device with a wider range, mounted on an aircraft. To protect against this, use airplane mode