re: POWER

Welcome to Digital Safety: Workplace Safety Planning for Home, Field or Office; How to Secure Networks & Devices

Thanks for Joining!

- Folx are on mute to keep background noise to minimum
- A recording of today's workshop will be made available
- Throughout the workshop, please attend to your bio needs: Stretch, go to the bathroom, eat a snack, etc.
- We will interact by posting in the Zoom Chat box.

Let's Start! *Question 1: What candy is or was cast aside in your Halloween haul? Or what sweet is overrated?*

In this workshop, we will...

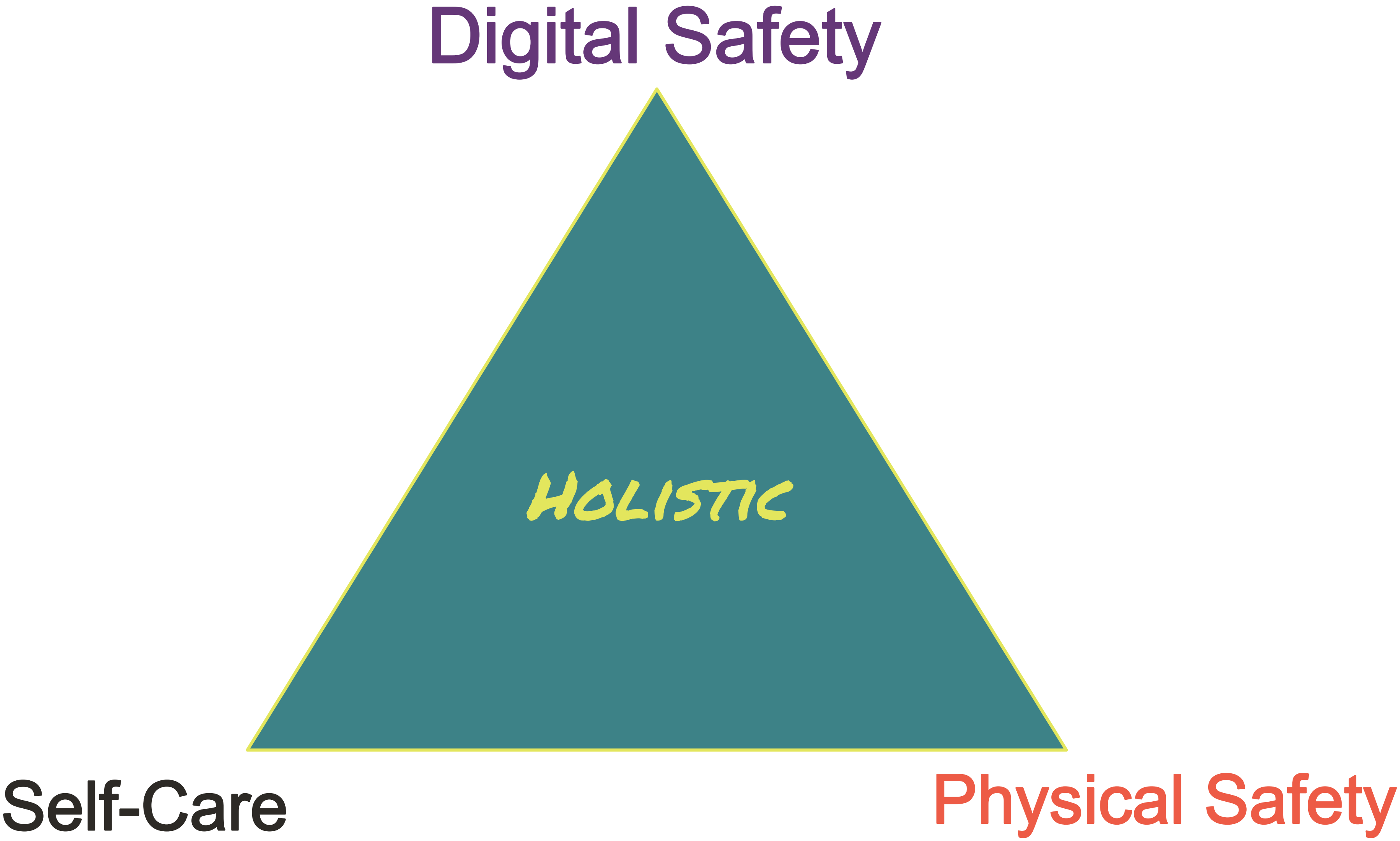
- Learn what a network is and how to connect more safely to the Internet
- Understand the strengths and weaknesses of a virtual private network or VPN
- Pick up some tips for securing our smartphones and other devices
- Learn about data backup practices
- Learn how to keep ourselves and our connected devices safer online and in direct action activities

Trainer Intro: Seth Pinckney (he/him)

Why should I care?

- I have nothing to hide, so why do I need to protect privacy?
- I'm worried about my digital security to the point of being overwhelmed. I don't know where to start.
- I'm ready to take action, but not until I have a perfect handle on how all of these technical concepts fit together.
- There's no such thing as perfect security, so why even bother? If someone wants to hack me, they'll figure out a way to do it.

Source: https://sec.eff.org/articles/why-your-audience-should-care



Digital Safety

HOLISTIC

Self-Care

Physical Safety

Workshop 3 Recap

Why Use Encryption?

```
@                                   /Telco
```

This is an example SMS Insecurity GIF

In the GIF, the user is using the command line to search for texts between users. The telephone numbers are visible by the eavesdropper, and the text messages themselves are unencrypted.

One user asks: "Can you send me the password?"

The other user responds: "It's 123caterpillar."

The Ecosystem

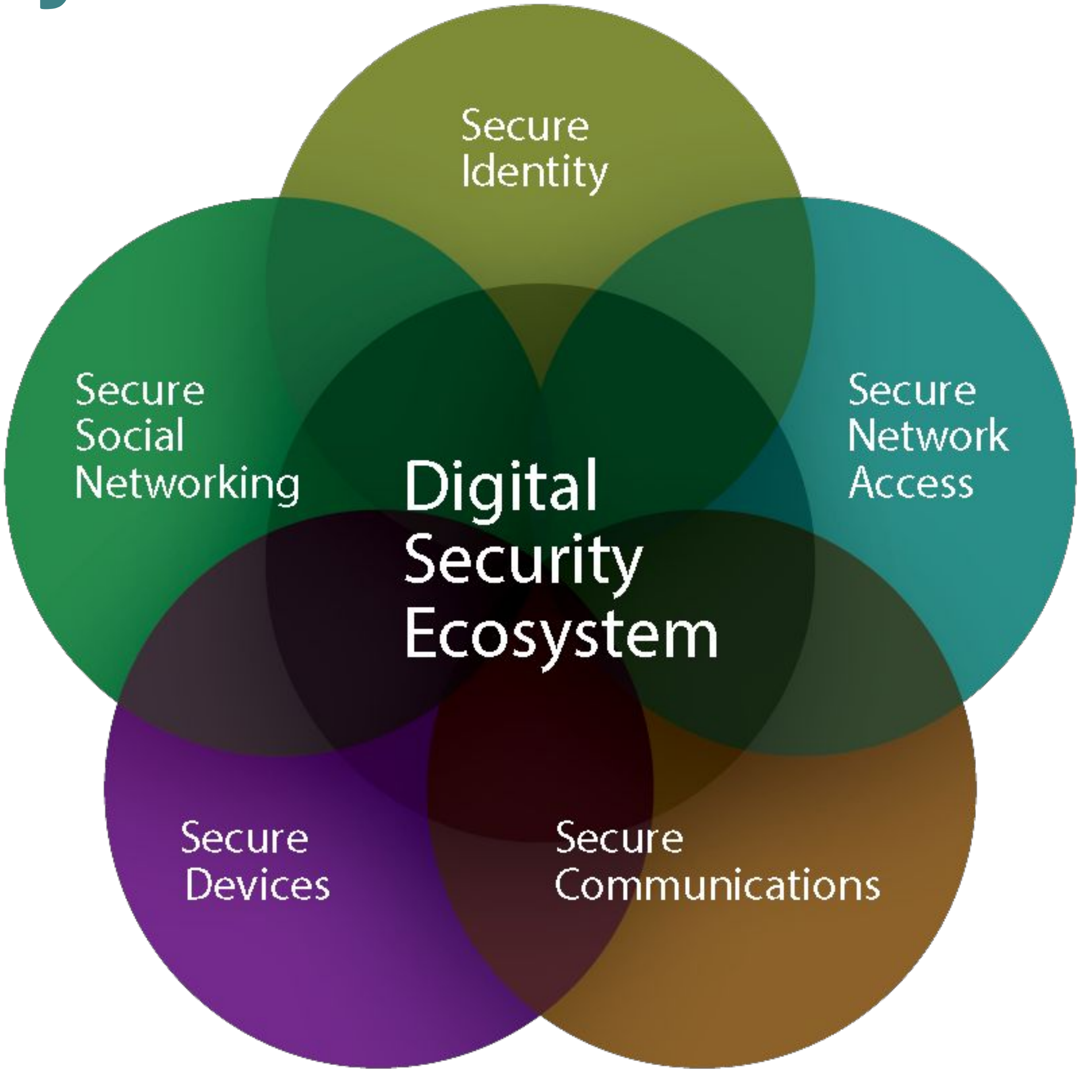


Image source: http://digitalsecurityforall.org/en/curriculum/what_is_digital_security

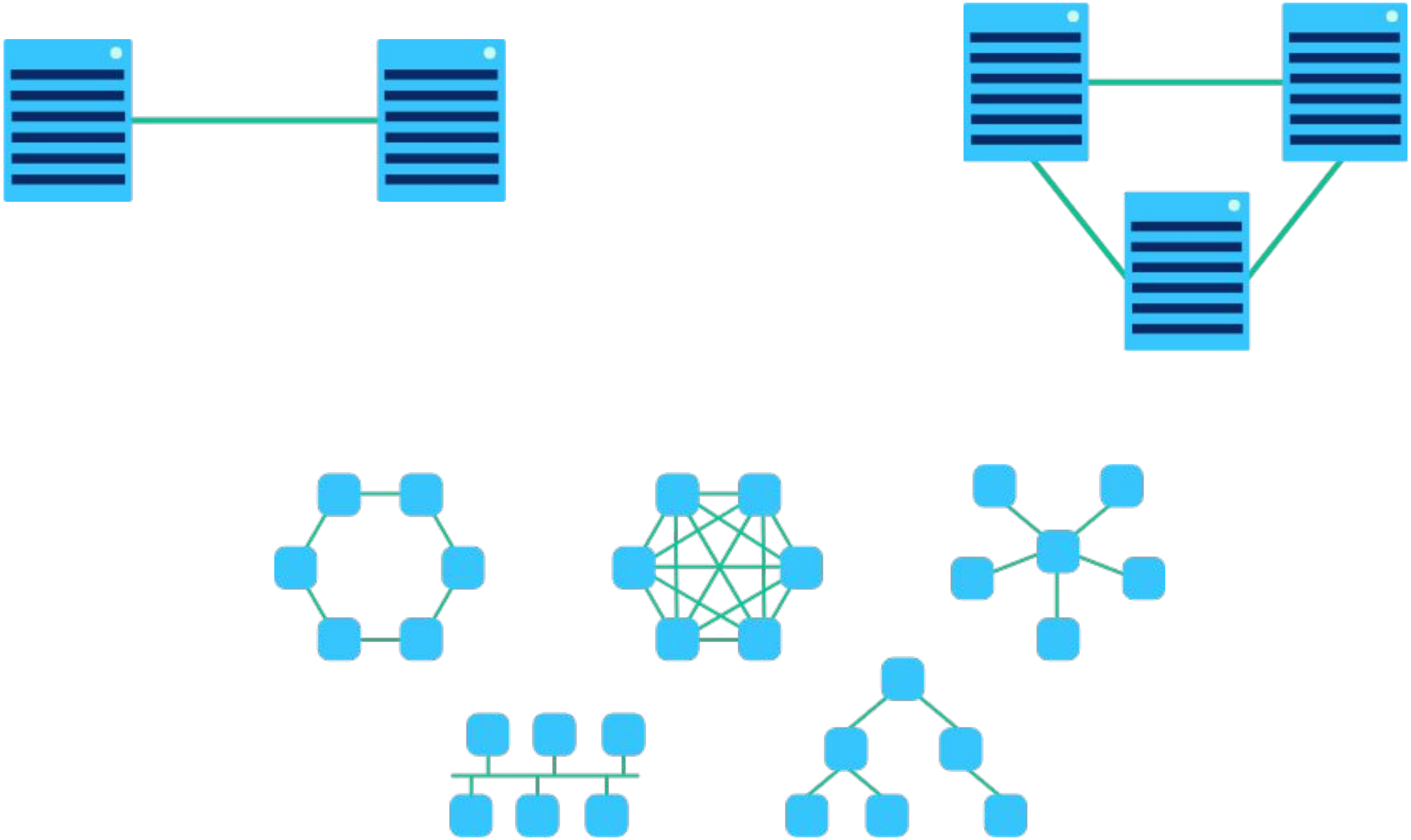
What is a Network?

The Internet is the world's largest computer network.

A computer network is any group of interconnected computing devices capable of sending or receiving data. A computing device isn't just a computer—it's any device that can run a program, such as a tablet, phone, or smart sensor.

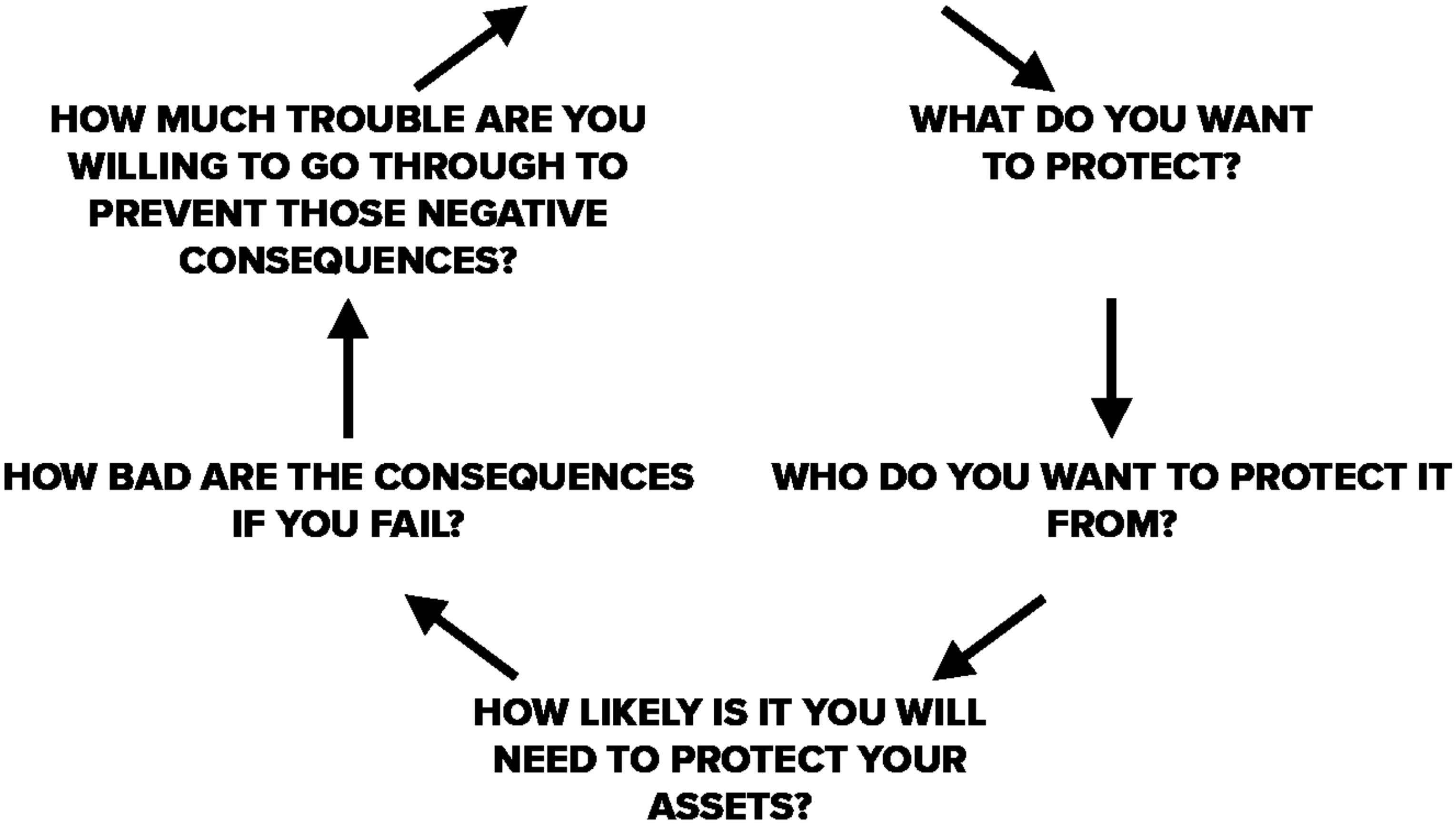
https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:connecting-networks/a/computer-networks-overview

What is a Network?



https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:connecting-networks/a/computer-networks-overview

YOUR RISK ASSESSMENT



WHAT DO YOU WANT TO PROTECT?

WHO DO YOU WANT TO PROTECT IT FROM?

HOW LIKELY IS IT YOU WILL NEED TO PROTECT YOUR ASSETS?

HOW BAD ARE THE CONSEQUENCES IF YOU FAIL?

HOW MUCH TROUBLE ARE YOU WILLING TO GO THROUGH TO PREVENT THOSE NEGATIVE CONSEQUENCES?

Threats & Risk

- On your device, if it is infected with malware or if someone observes your communication directly
- At your WiFi router, if it is infected with malware or controlled by someone with malicious intent
- While passing through a physical cable on the Internet backbone, if it is "tapped" (typically by a state actor)
- On any of the servers that store or route your communication
- At some other participant's WiFi router, if it is infected with malware or if they have malicious intent
- On some other participant's device, if it is infected with malware or if someone observes their communication directly

Source: https://securityinabox.org/en/guide/secure-communication/

Secure Your Network Access

Securing your network access is crucial to being able to access the Internet safely as your Internet Service Provider (ISP) is often where much surveillance happens.

- Use a Virtual Private Network (VPN)
- Use TOR
- Use Tails

Source: https://securityinabox.org/en/guide/secure-communication/

*Question

Has someone ever asked you to watch over something of theirs? For example, has someone ever asked you to watch their bag?

- *How did they know you were trustworthy?*
- *What did you do with the valuable information or item they gave you?*

What is a VPN?

VPN (or virtual private network) services create a secure, encrypted connection between your computer and a VPN server at another location. That type of secure connection is a worthwhile investment for anyone who wants to wrap their data in an extra layer of privacy and security, especially when connecting to public Wi-Fi networks.

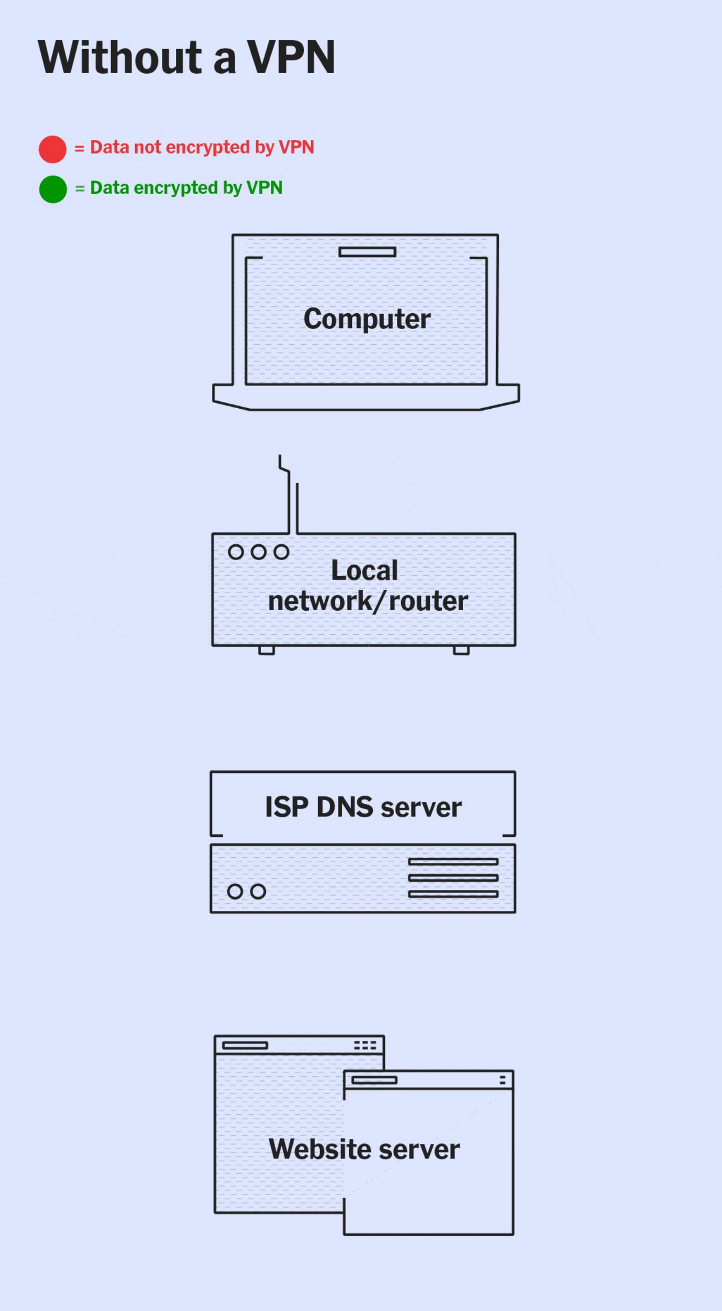
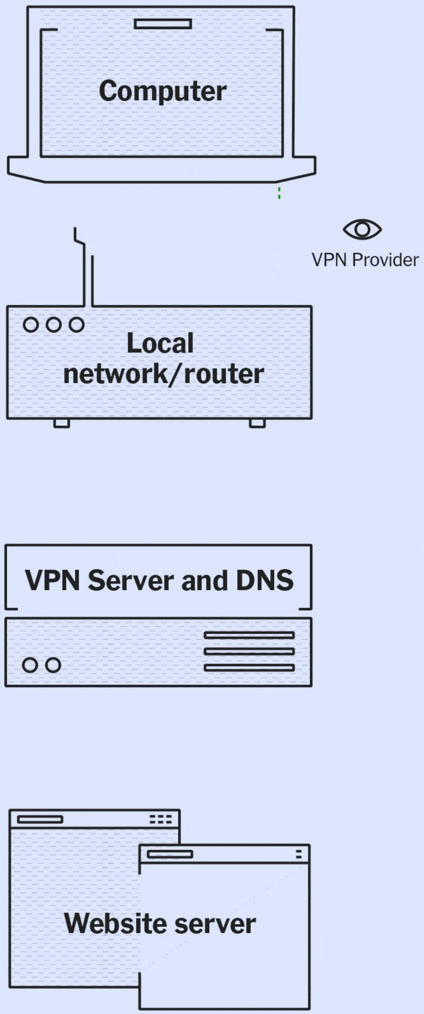


Illustration: Sarah MacReading, source: https://www.nytimes.com/wirecutter/reviews/best-vpn-service/

With a VPN

🔴 = Data not encrypted by VPN

🟢 = Data encrypted by VPN



re: POWER

Illustration: Sarah MacReading, source: https://www.nytimes.com/wirecutter/reviews/best-vpn-service/

Why use a VPN?

- VPNs are good for securing public Wi-Fi
- VPNs reduce some types of online tracking
- VPNs limit potential ISP monitoring (but an untrustworthy VPN could monitor you instead)

https://www.nytimes.com/wirecutter/reviews/what-is-a-vpn/#how-a-vpn-works

VPN Limitations

- VPNs are unreliable for accessing international video services like Netflix
- VPNs are no guarantee against government tracking
- Your ISP could block or throttle a VPN connection
- Business Model & Data Collection Practices

https://www.nytimes.com/wirecutter/reviews/what-is-a-vpn/#how-a-vpn-works

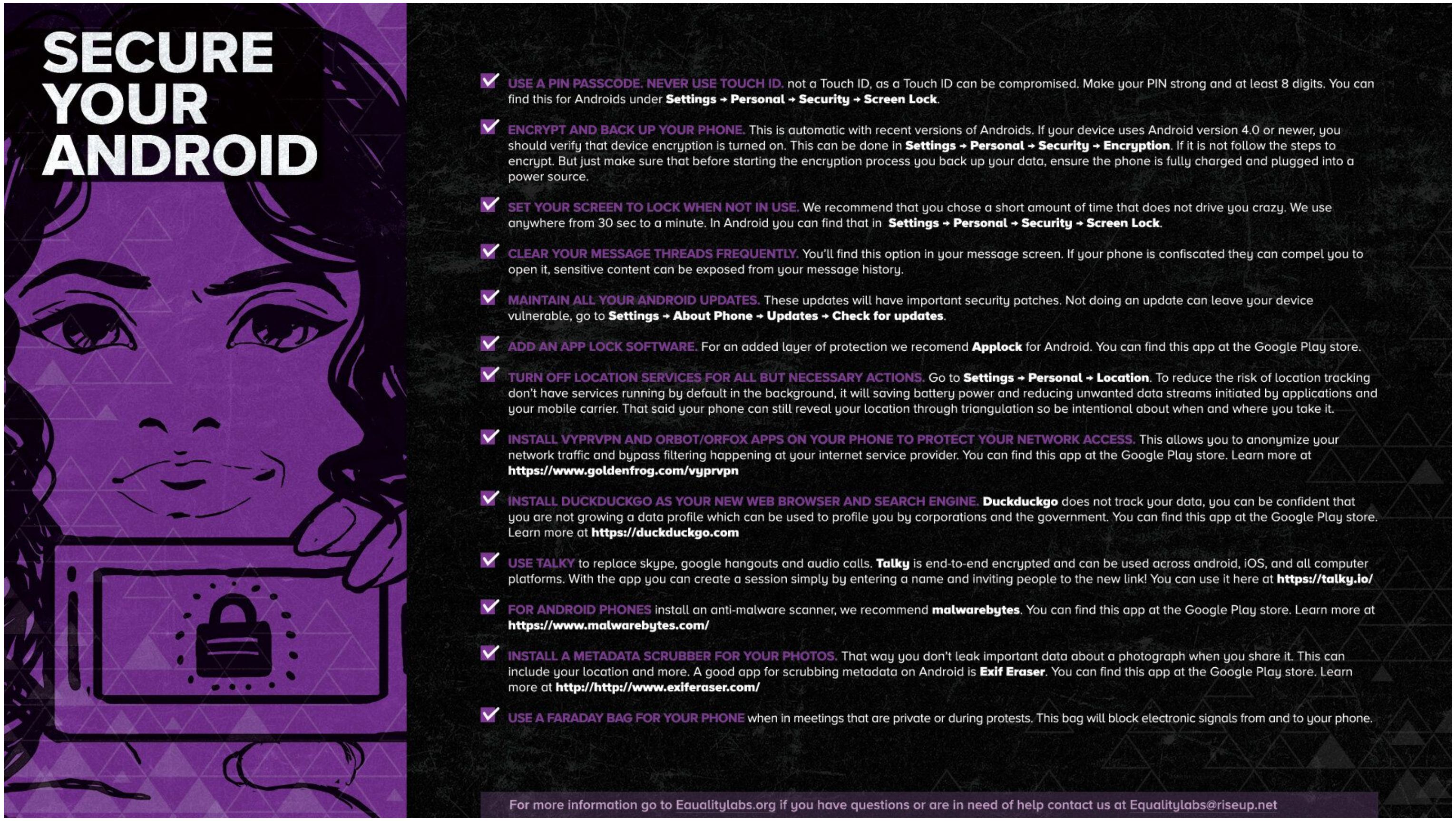
Securing Your Phone

- Protect your data: Phone Encryption on iOS and Android
- Protect your texts
- Protect your calls
- Protect your smartphone browsing

Illustration Source: Kurt Woerpel for The Intercept

Android & iPhone Tips

(https://www.equalitylabs.org/resources-1#quick-guides)



SECURE YOUR ANDROID

- ☑ **USE A PIN PASSCODE. NEVER USE TOUCH ID.** not a Touch ID, as a Touch ID can be compromised. Make your PIN strong and at least 8 digits. You can find this for Androids under **Settings → Personal → Security → Screen Lock**.
- ☑ **ENCRYPT AND BACK UP YOUR PHONE.** This is automatic with recent versions of Androids. If your device uses Android version 4.0 or newer, you should verify that device encryption is turned on. This can be done in **Settings → Personal → Security → Encryption**. If it is not follow the steps to encrypt. But just make sure that before starting the encryption process you back up your data, ensure the phone is fully charged and plugged into a power source.
- ☑ **SET YOUR SCREEN TO LOCK WHEN NOT IN USE.** We recommend that you chose a short amount of time that does not drive you crazy. We use anywhere from 30 sec to a minute. In Android you can find that in **Settings → Personal → Security → Screen Lock**.
- ☑ **CLEAR YOUR MESSAGE THREADS FREQUENTLY.** You'll find this option in your message screen. If your phone is confiscated they can compel you to open it, sensitive content can be exposed from your message history.
- ☑ **MAINTAIN ALL YOUR ANDROID UPDATES.** These updates will have important security patches. Not doing an update can leave your device vulnerable, go to **Settings → About Phone → Updates → Check for updates**.
- ☑ **ADD AN APP LOCK SOFTWARE.** For an added layer of protection we recomend **Applock** for Android. You can find this app at the Google Play store.
- ☑ **TURN OFF LOCATION SERVICES FOR ALL BUT NECESSARY ACTIONS.** Go to **Settings → Personal → Location**. To reduce the risk of location tracking don't have services running by default in the background, it will saving battery power and reducing unwanted data streams initiated by applications and your mobile carrier. That said your phone can still reveal your location through triangulation so be intentional about when and where you take it.
- ☑ **INSTALL VYPRVPN AND ORBOT/ORFOX APPS ON YOUR PHONE TO PROTECT YOUR NETWORK ACCESS.** This allows you to anonymize your network traffic and bypass filtering happening at your internet service provider. You can find this app at the Google Play store. Learn more at **https://www.goldenfrog.com/vyprvpn**
- ☑ **INSTALL DUCKDUCKGO AS YOUR NEW WEB BROWSER AND SEARCH ENGINE.** **Duckduckgo** does not track your data, you can be confident that you are not growing a data profile which can be used to profile you by corporations and the government. You can find this app at the Google Play store. Learn more at **https://duckduckgo.com**
- ☑ **USE TALKY** to replace skype, google hangouts and audio calls. **Talky** is end-to-end encrypted and can be used across android, iOS, and all computer platforms. With the app you can create a session simply by entering a name and inviting people to the new link! You can use it here at **https://talky.io/**
- ☑ **FOR ANDROID PHONES** install an anti-malware scanner, we recommend **malwarebytes**. You can find this app at the Google Play store. Learn more at **https://www.malwarebytes.com/**
- ☑ **INSTALL A METADATA SCRUBBER FOR YOUR PHOTOS.** That way you don't leak important data about a photograph when you share it. This can include your location and more. A good app for scrubbing metadata on Android is **Exif Eraser**. You can find this app at the Google Play store. Learn more at **http://http://www.exiferaser.com/**
- ☑ **USE A FARADAY BAG FOR YOUR PHONE** when in meetings that are private or during protests. This bag will block electronic signals from and to your phone.

For more information go to Eaualitylabs.org if you have questions or are in need of help contact us at Equalitylabs@riseup.net

Source: https://securityinabox.org/en/guide/secure-communication/

Secure Your Computer

- **Create a Strong Password.** It should be original, complex, use no personal information, and update it every three months.
- **Create User Admin Accounts**
  - on a Mac *Apple Menu -> System Preferences -> Users and Accounts.*
  - on a PC for Windows 10 at *Start -> Settings -> Accounts -> Family and other people -> Add someone else to this PC.*
- **Encrypt Your Computer**
  - On a Mac this is done through the security panel in system preferences, turning on FireVault. You can find this at *System Preferences -> Security & Privacy -> FireVault*
  - On Windows machines you can check if Device Encryption is enabled by opening the Settings app, navigating to *System -> About*, and looking for the "Device Encryption" setting at the bottom of the *About* panel.
- **Use A Strong Anti-Malware Software Routinely**
  - Try for once a week. One tool is MalwareBytes
- **Be Careful with Attachments**
- **Update Your Operating System Frequently**
  - On a Mac you can find this at *Apple Menu -> App Store*
  - On a PC in Windows 10 automate your updates by going to Control Panel and check if your automatic updating is turned on.

Data Backup

“Make sure to ALWAYS backup your files locally in addition to syncing them to the cloud. If your cloud service suddenly died for whatever reason, you’d be awfully vulnerable (and your laptop would probably get stolen that same week or something because the world is cruel). Back up your most important files to an external hard-drive, which you should -definitely- encrypt as well.”

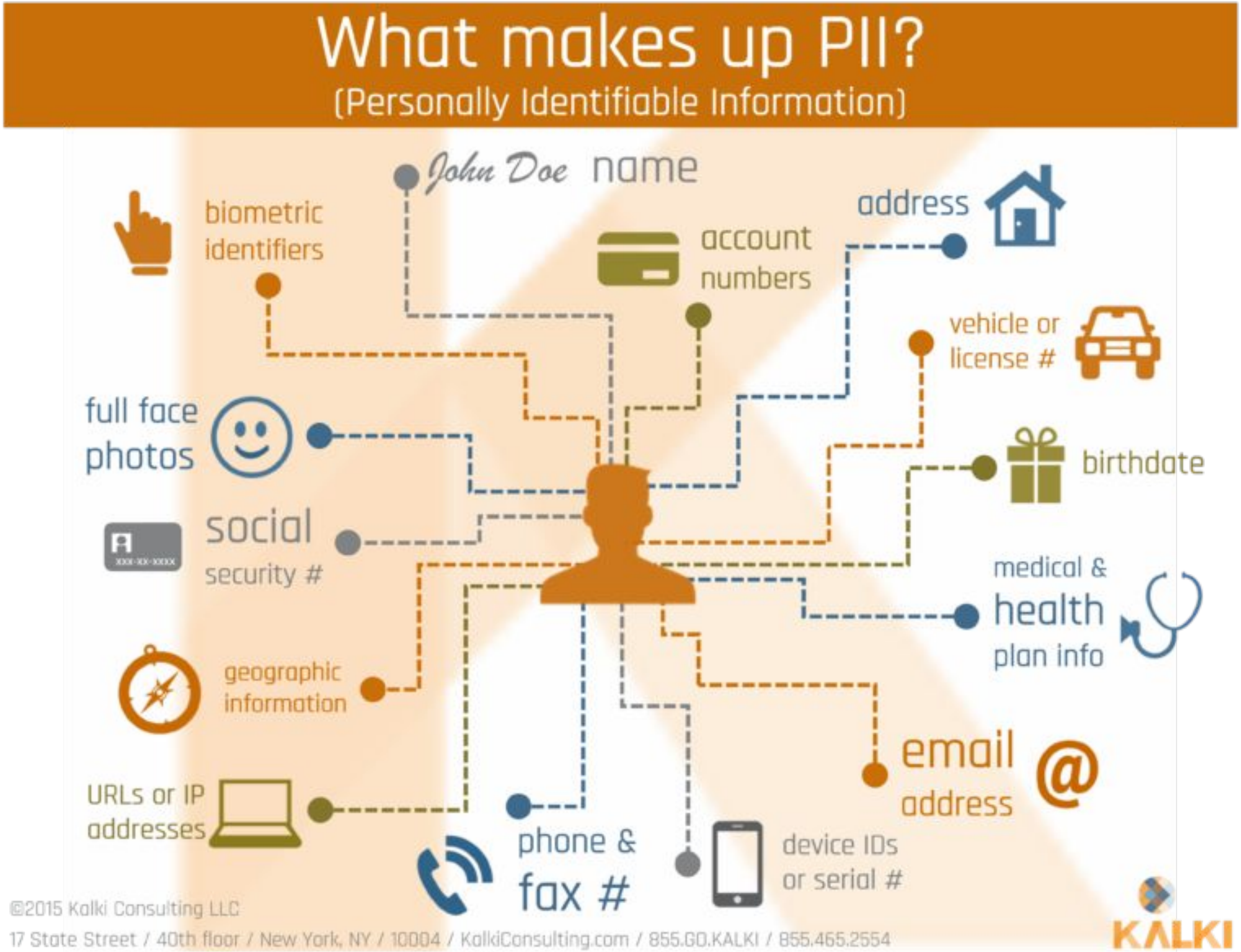
- **https://hackblossom.org**

A note on...

Video Conferencing

What makes up PII?

(Personally Identifiable Information)



John Doe name

biometric identifiers

account numbers

address

vehicle or license #

full face photos

birthdate

social security #

medical & health plan info

geographic information

URLs or IP addresses

phone & fax #

device IDs or serial #

email address

17 State Street / 40th floor / New York, NY / 10004 / KalkiConsulting.com / 855.GO.KALKI / 855.465.2554

Stingrays or Cell-Site Simulators

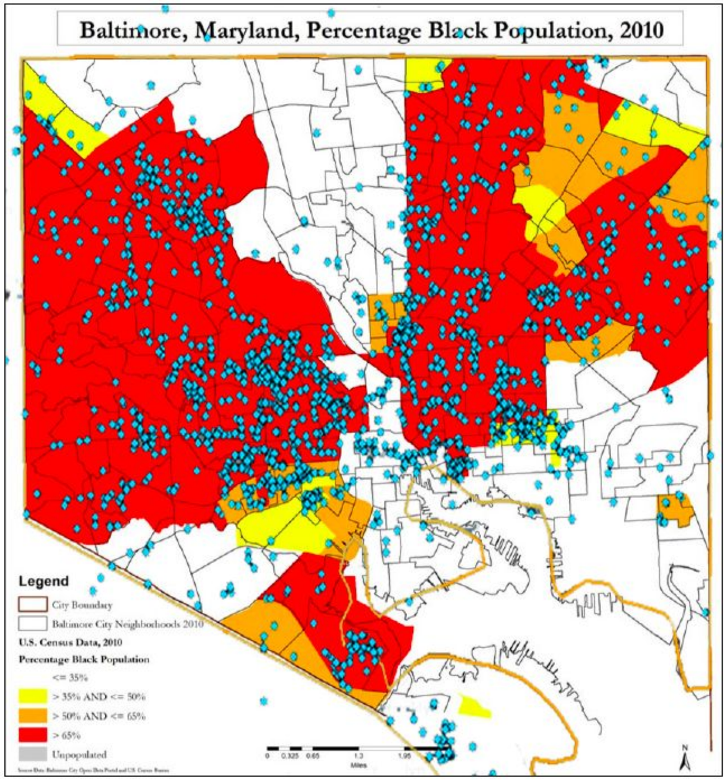
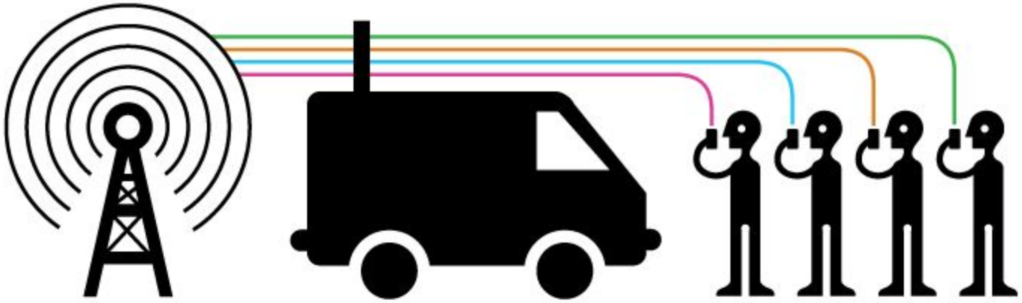

Baltimore, Maryland, Percentage Black Population, 2010
Legend
City Boundary
Baltimore City Neighborhoods 2010
U.S. Census Data, 2010
Percentage Black Population
<= 35%
> 35% AND <= 50%
> 50% AND <= 65%
> 65%
Unpopulated
0
0.325
0.65
1.3
1.95
Miles
N
Source Data: Baltimore City Open Data Portal and U.S. Census Bureau

Figure 2 –Deployment Sites Overlaid on Map of Baltimore's Black Residents

CELL-SITE SIMULATOR SURVEILLANCE

Cell-site simulators trick your phone into thinking they are base stations.



Depending on the type of cell-site simulator in use, they can collect the following information:

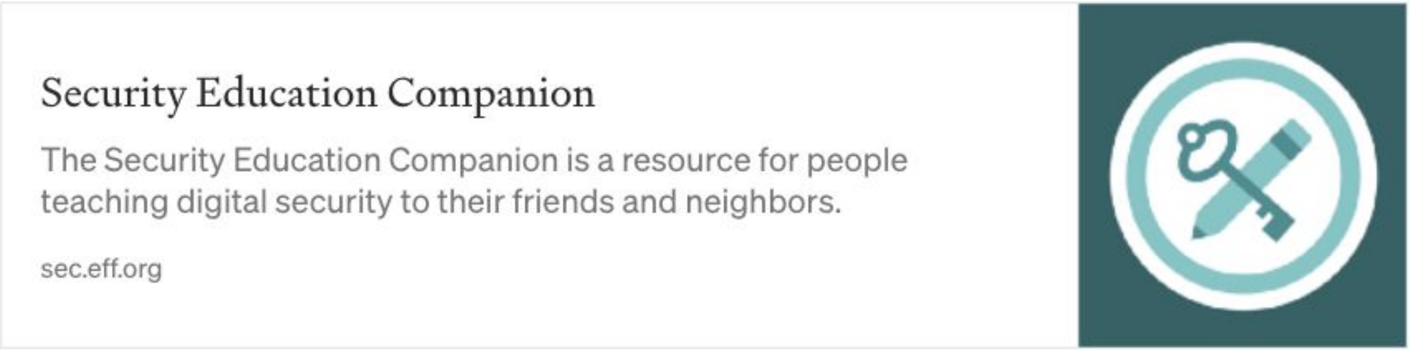
1. identifying information about the device like International Mobile Subscriber Identity (IMSI) number
2. metadata about calls like who you are dialing and duration of call
3. intercept the content of SMS and voice calls
4. intercept data usage, such as websites visited.

https://www.eff.org/sls/tech/cell-site-simulators

You should also make sure that your phone is encrypted.

What other things can we do organizationally?

Become a Trainer! You can do quarterly Digital Safety and Security trainings.



Security Education Companion

The Security Education Companion is a resource for people teaching digital security to their friends and neighbors.

sec.eff.org

A few tools

Tor Browser: Web browser to experience more private browsing without tracking, surveillance, or censorship.

Tails live OS: Tails is a live operating system that you can start on almost any computer from a USB stick or a DVD.

Authy by Twilio: Two Factor Authentication for many apps

YubiKey: Two-factor and passwordless authentication.

Burner: reroute calls coming to your Burner temporary phone number and send them to your cell phone so your personal number stays private.

OpenVPN: Virtual Private Network

Resources

Digital Security Helpline

Access Now's Digital Security Helpline works with individuals and organizations around the world to keep them safe online. If you're at risk, we can help you improve your digital security practices to keep out of harm's way. If you're already under attack, we provide rapid-response emergency assistance.

The Digital First Aid Kit

The Digital First Aid Kit is a free resource to help rapid responders, digital security trainers, and tech-savvy activists to better protect themselves and the communities they support against the most common types of digital emergencies.

Create an action plan:

https://securityplanner.consumerreports.org/action-plan

re: POWER

Reclaiming Our Power for Radical Change