re: POWER

Welcome to Digital Safety: Safer Communication & Internet Browsing

re: POWER

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 was the make and model of your first cell phone?*

In this workshop, we will...

- **Learn how to better secure communication**
- **Understand what is encryption and how it works**
- **Cover what are some safer browsing practices**

Trainer Intro: Seth Pinckney (he/him)

Workshop 2 Recap

Image source: https://www.rlmartstudio.com/product/my-vote-notecard/

The Ecosystem

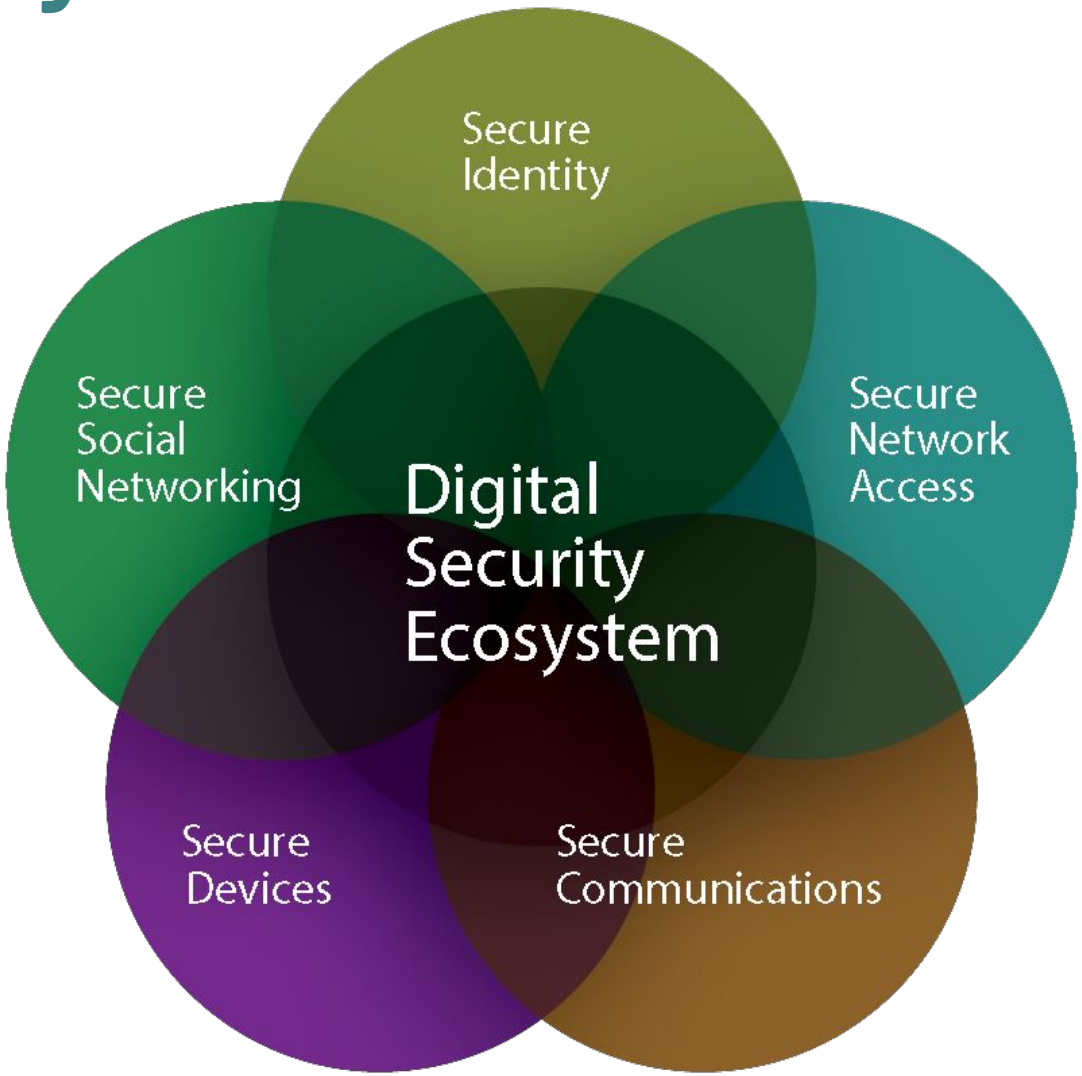
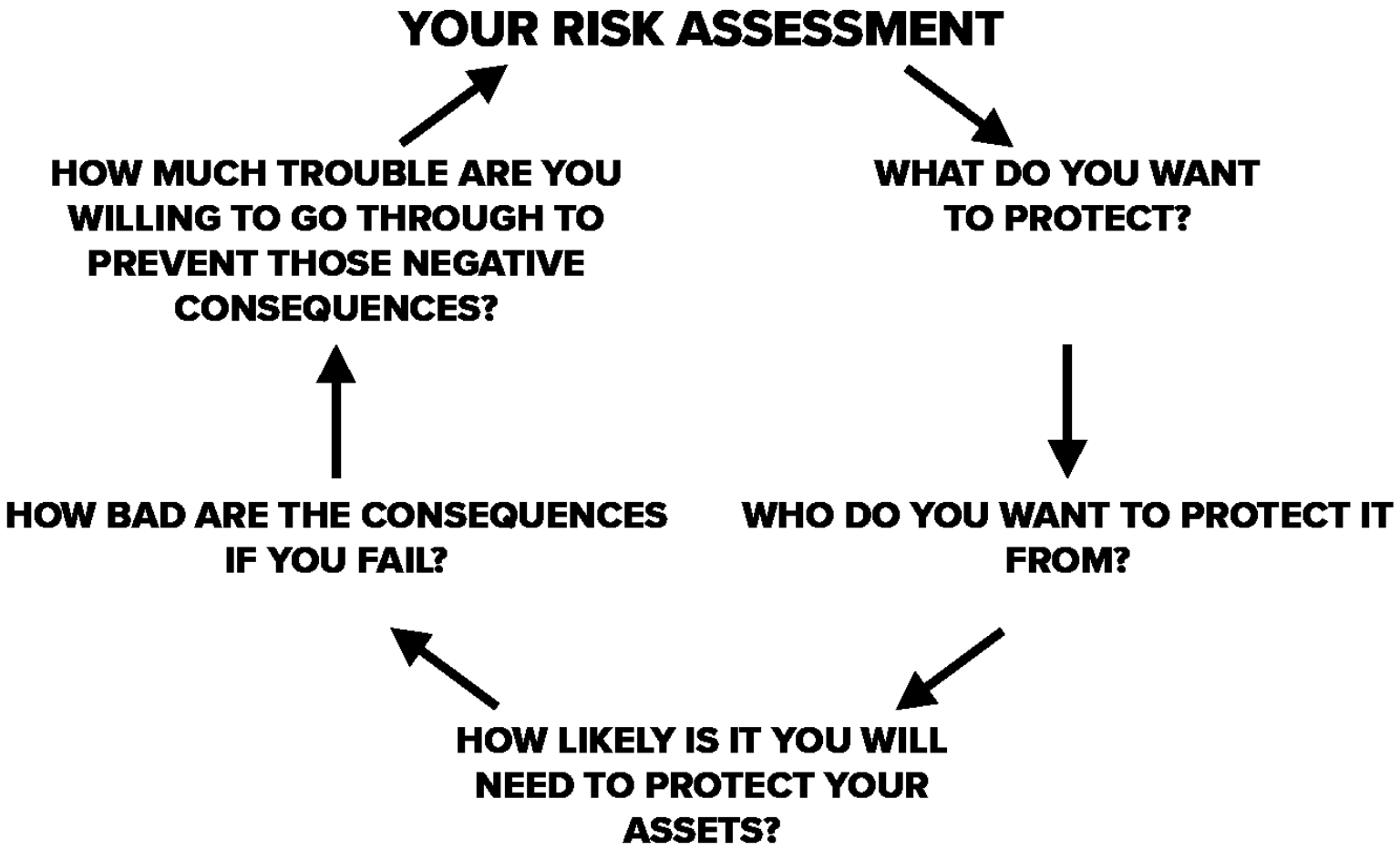


Image source: http://digitalsecurityforall.org/en/curriculum/what_is_digital_security


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?

Navigating Malicious Threats

If your Internet activity is not encrypted, it is NOT private and you should assume that someone or something could see it.

+

Left unchecked, your cookies will feed personal data to private companies.

+

Public wifi is insecure.

The amount of protection you adopt is totally up to you: usually the trade-off is the more protection you want, the slower and more inconvenient browsing on the web can be!

Source: https://hackblossom.org/cybersecurity/


PARENTS BE LIKE
"YOU GOT SOME MAIL OVER HERE"
makeameme.org

Safer Communication

*"In order to protect our **digital communication**, we will need to address a variety of threats. Doing so requires some technical knowledge, like **understanding what happens to messages between our devices and that of a recipient**, but it also requires good habits like keeping our devices secure from malware, using strong passwords, avoiding phishing attempts and **maintaining a communication plan that suits our needs**."*

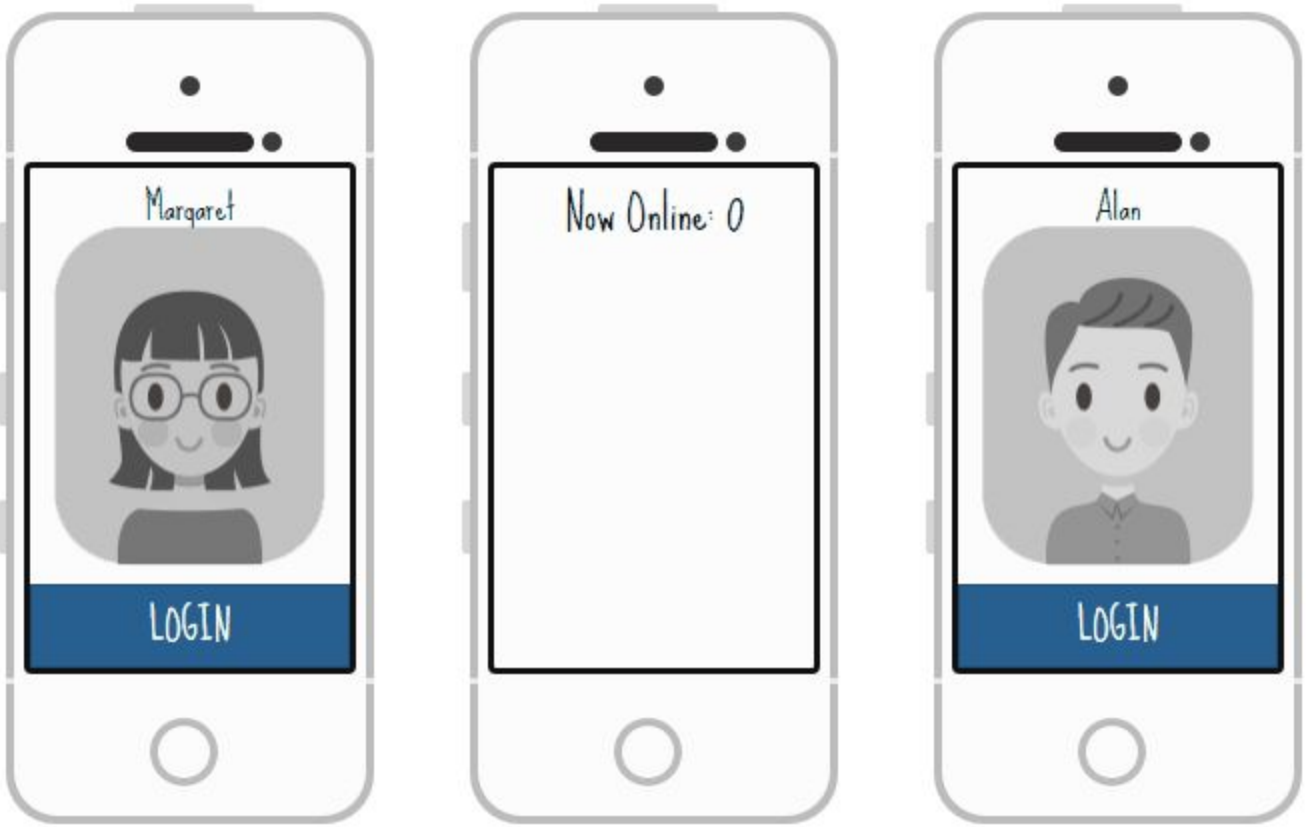
Source: https://securityinabox.org/en/guide/secure-communication/

Communication Methods

Whether we are using the Internet, a mobile phone network or some other technology, you probably have a number of different communication methods to choose from. Each of these technologies and methods comes with its own set of advantages and disadvantages in terms of convenience, popularity, cost, performance and security, among other considerations.

- Voice calls on mobile phones and landlines
- Email
- SMS text messaging over mobile phone networks
- Internet-based "messenger" apps, which typically handle text, photos, voice calls, and video calls
- Online discussion boards and social media platforms

Safer Communication



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

Web based Communication

- Web based communication involves two or more people; if they are using the same service, their paths are connected in the middle by the "website" That website could be Gmail, for example.

- Social networking platforms, messaging apps, discussion forums and other communication services work in more or less the same way.

- Mobile phone calls and SMS text messages work in a similar way, assuming at least one participant is on a different network, in a different country or subject to surveillance of some kind.

- Regardless of whether you are connecting through WiFi or through mobile data, calendars, fitness trackers, news readers, social networking apps and messengers (such as Signal or iMessage) all send and receive information using the Internet.

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

Threats & Risk

Your communication could be targeted by people who want to cause harm
They might be seeking valuable information, harassing people who fit a certain profile or trying to prevent you from doing your work, among other possible motives.

Your digital communication could be monitored or intercepted:

- 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
- By your ISP or mobile provider, either for their own purposes or on behalf of a third party
- At a national gateway, sometimes even if all participants and services are located in the same country
- While passing through a physical cable on the Internet backbone, if it is "tapped" (typically by a state actor)
- By the ISP or website of the service you are using
- By the ISP or mobile provider of the people with whom you are communicating
- 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/

Safer Communication

"You can help protect yourself from these risks by: ***paying attention to your surroundings, keeping your devices up-to-date, avoiding malware, watching out for phishing attacks, relying on trustworthy services, creating strong passwords, configuring your accounts to use two factor authentication, using encryption*** *and helping those with whom you communicate do the same."*

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

HTTP & HTTPS

- There are two ways for a website to get to your browser: HTTP and HTTPS. The difference is that “S,” which stands for “secure.”

- When you see “https” and a little green lock next to the web page address in the top of your browser, that means you are using a secure connection. You have probably seen this when shopping online or entering credit card information.

- Now, however, the web is in the middle of a large shift to using HTTPS for all webpages. This is because HTTP lacks any meaningful security, and HTTPS comes secure by default.

- If someone is spying on the network and trying to see what websites users are visiting, an HTTP connection offers no protection. An HTTPS connection, on the other hand, hides which specific page on a website you navigate to—that is, everything “after the slash.”

Browser Extensions & Apps

Browser extensions are no-cost software you can install in your browser to customize your browsing experience.

- Privacy Badger
- uBlock Origin
- Disconnect.me
- HTTPS Everywhere!
- Firefox Focus for iOS
- Firefox for Android

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

Note

- Privacy Badger Is Not An Ad Blocker
  - Privacy Badger is not an ad blocker. Instead, it’s a tracker blocker.

- HTTPS Everywhere Doesn’t Encrypt Everything
  - It’s up to a website’s administrators to decide whether or not their site offers HTTPS

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

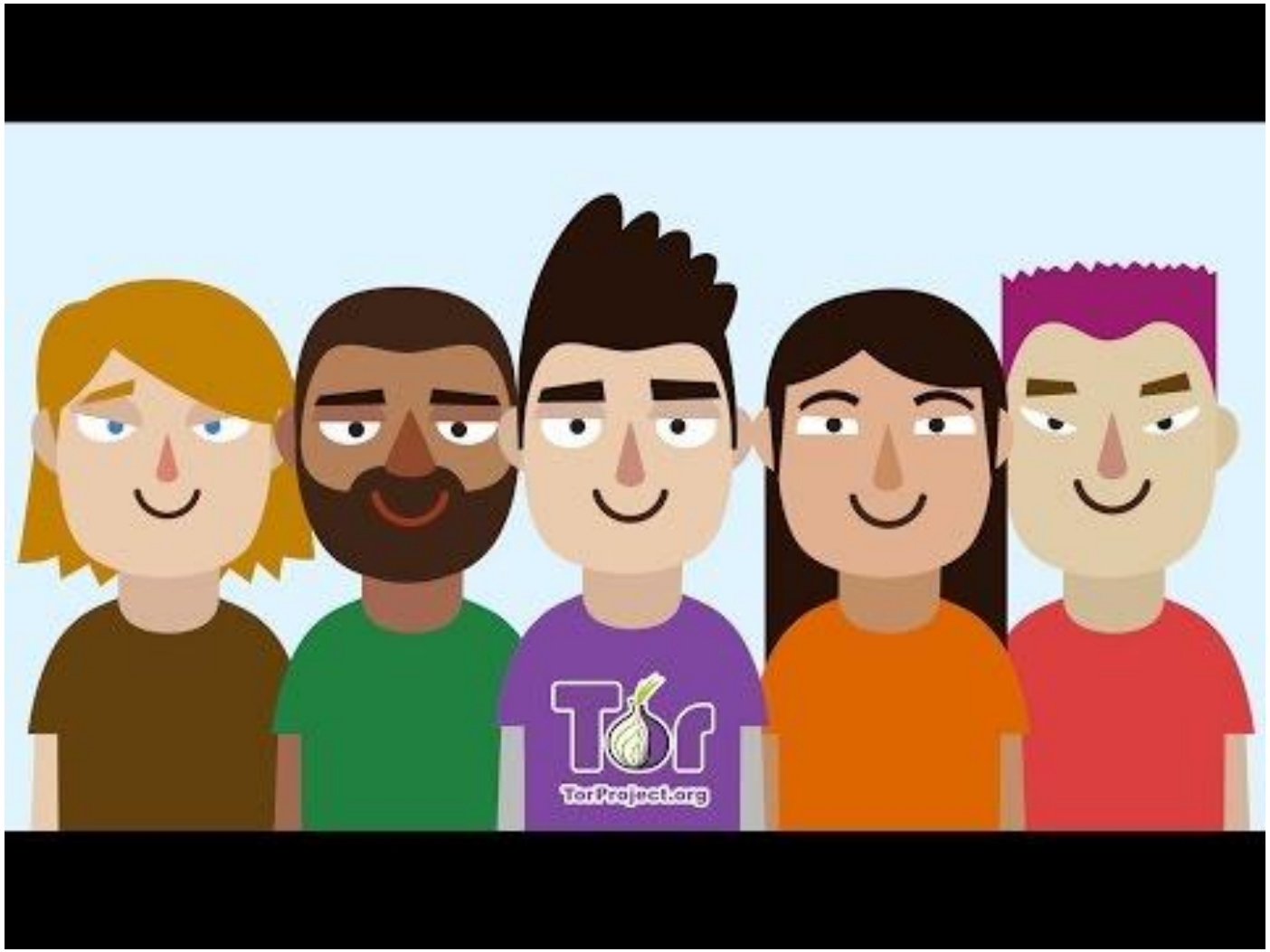
Anonymous Browsing

- The Tor network is an internet protocol that basically hides your identity by bouncing your web requests across the world in multiple layers of encryption before it is received by the website.

- A big disclaimer for the Tor browser is that it makes you anonymous, but not private. Although your web requests are anonymous, if you are posting on Facebook or sending an email through Gmail, that activity is still identifiable as “you”. So a good rule of thumb is that when using the Tor browser, do not visit sites or services associated with your private information if you are trying to be anonymous.

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

What is Tor?



What we know

- The Internet has made communicating with people easier than ever, but has also made surveillance more prevalent.
- Without taking extra steps to protect your privacy, every phone call, text message, email, instant message, video and audio chat, and social media message could be vulnerable to eavesdroppers.
- The most privacy-protective way to communicate with others is in person, without computers or phones being involved at all.
- Since this isn't always possible, the next best thing is to **use end-to-end encryption.**

What is Encryption?

Encryption *keeps unwanted people from reading your data. It does this by transforming your data into completely unintelligible nonsense so that no-one but the intended receiver can figure out what it is.* ***It's really just a secret code.***

Why Use Encryption?

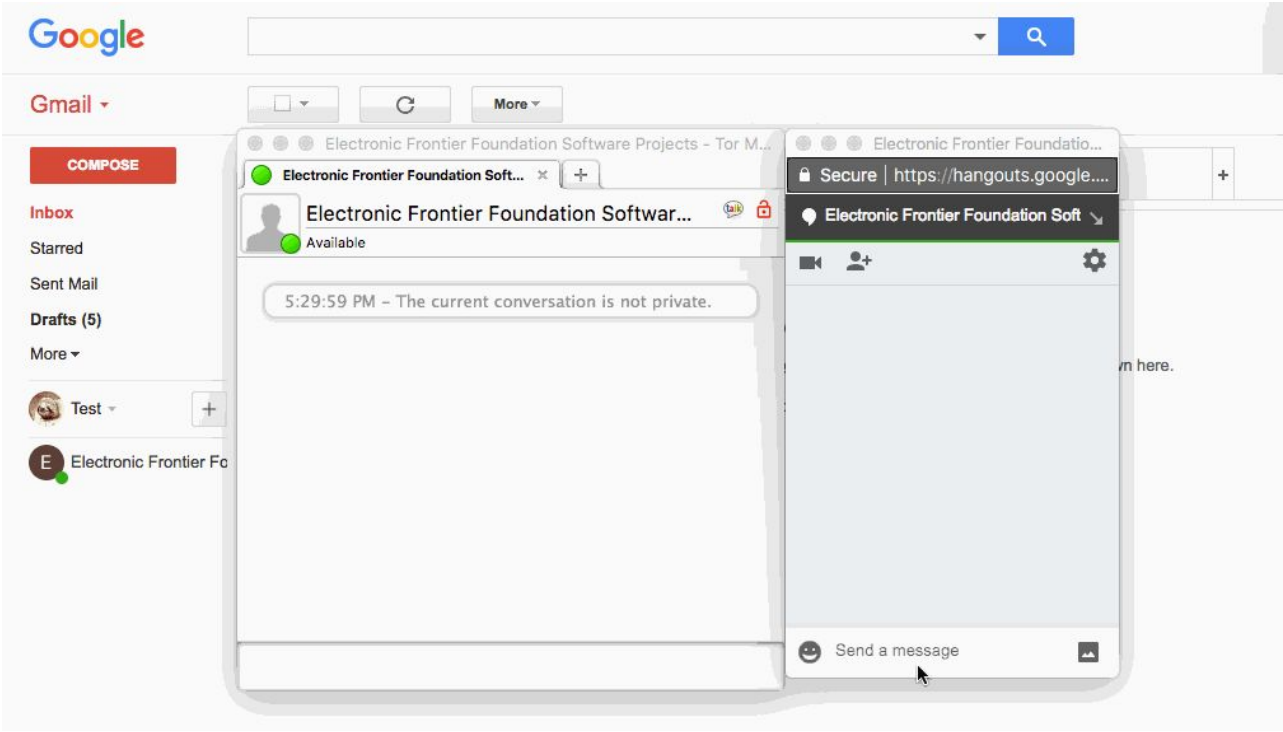
This is an example SMS Insecurity GIF

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?"

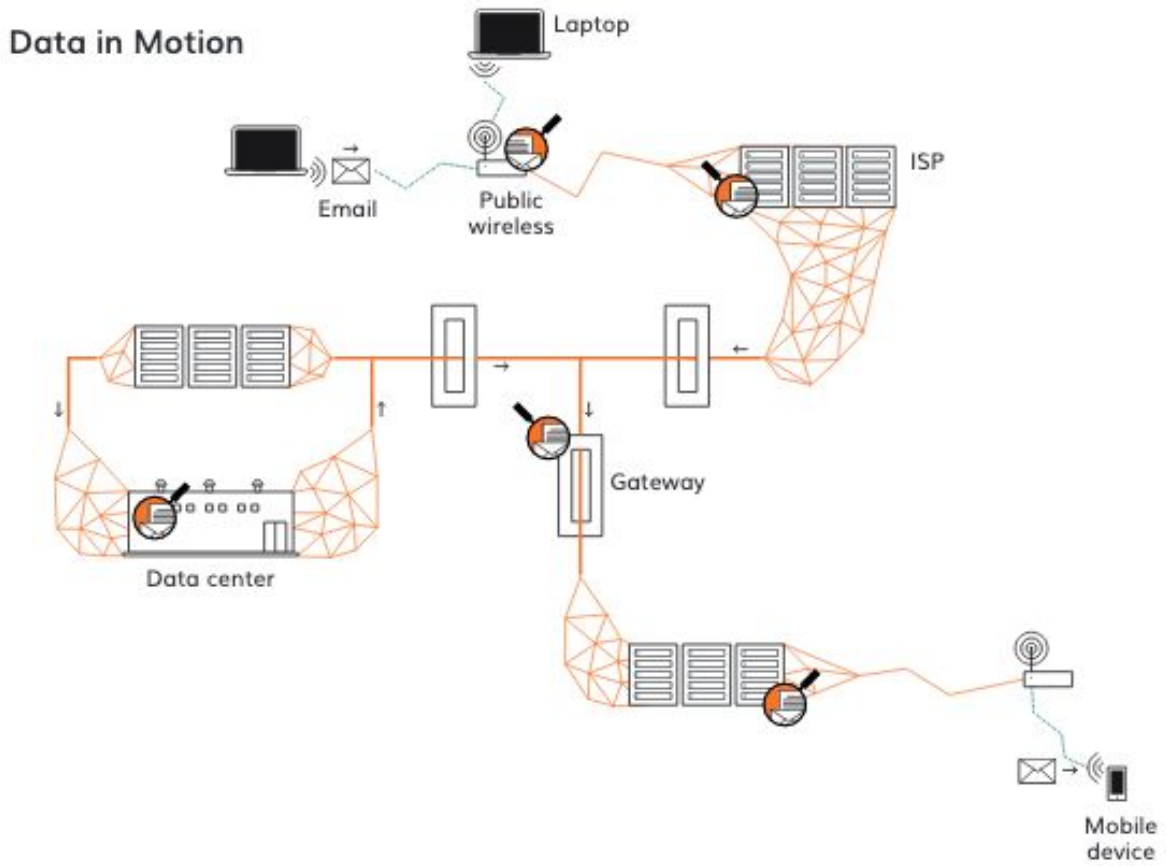
The other user responds: "It's 123caterpillar."

End-to-End Encryption



A core characteristic of good encryption: even the people who design and deploy it cannot themselves break it.

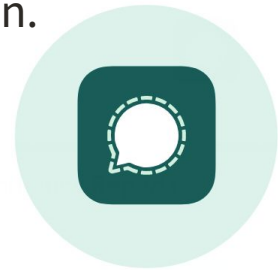
Meta Data: Information About Information



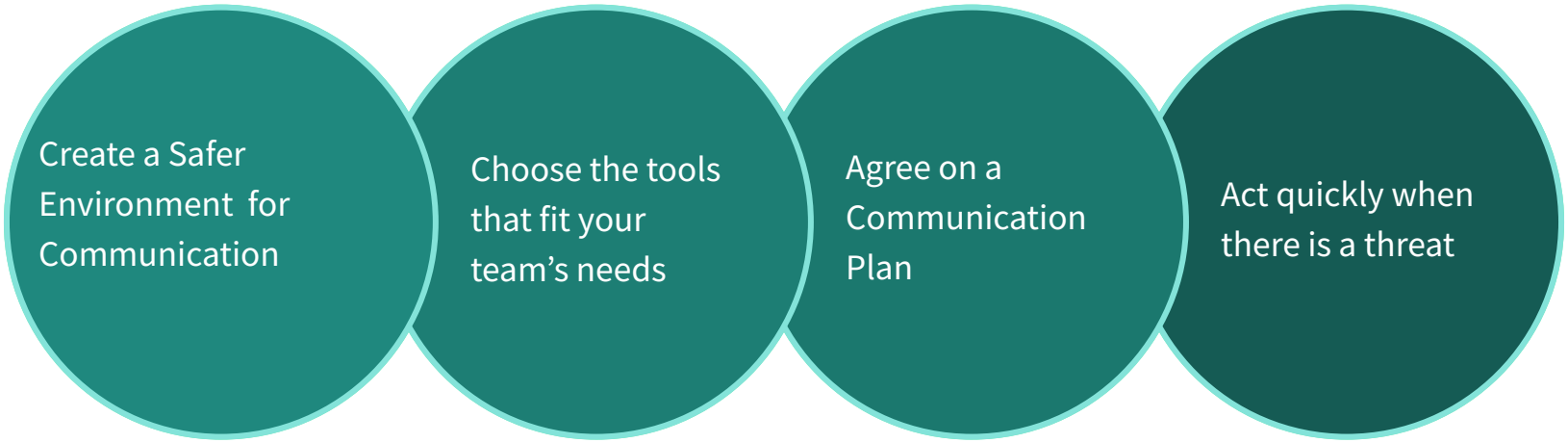
Source: https://ssd.eff.org/en/glossary

Signal App

- Signal is an easy-to-use app with state-of-the-art security that lets you privately talk, text, and share videos with your contacts.
- Install Signal on your phone by downloading Signal from your app store. Consider adding Signal to your Windows or Mac computer.
- The use of encrypted software such as Signal is legally restricted in some countries.
- When you use Signal, your messages and phone calls are encrypted end to end, meaning no one can read or listen to the content of your conversations unless they look over your shoulder, receive a copy from the person you're messaging, or physically access the device of one of the people in the conversation.



Action Steps



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

Digital Safety Workshop 4

Workplace Safety Planning: Home, Field or Office & How to Secure Networks & Devices


re: POWER
Reclaiming Our Power
for Radical Change