Welcome to Digital Safety: Phishing, Malware and Social Engineering & An Introduction to the DigiSec Ecosystem

Thanks for Joining!

- Folx are on mute to keep background noise to minimum
- 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: If you had to delete all but 2 apps from your smartphone, which ones would you keep?*

In this workshop, we will...

- Learn the components that make up the digital safety and security as an ecosystem
- Understand how malware works and which tools can best protect you
- Learn to identify a phishing email or social engineering attempt

Trainer Intro: Seth Pinckney (he/him)

Workshop 1 Recap

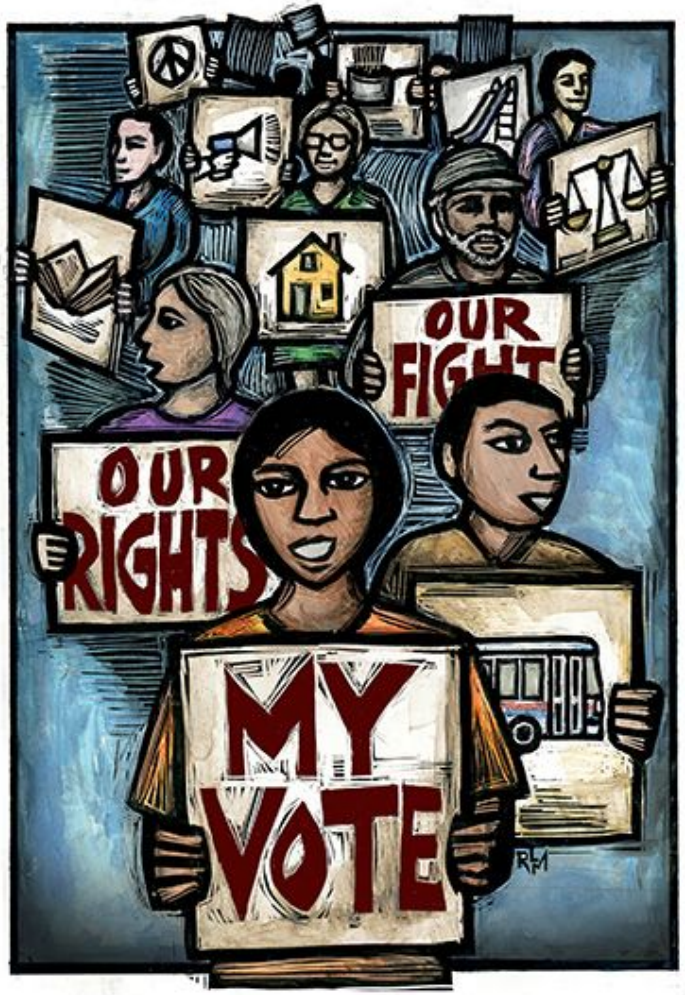


Image source: https://www.rlmartstudio.com/product/my-vote-notecard/

The Ecosystem

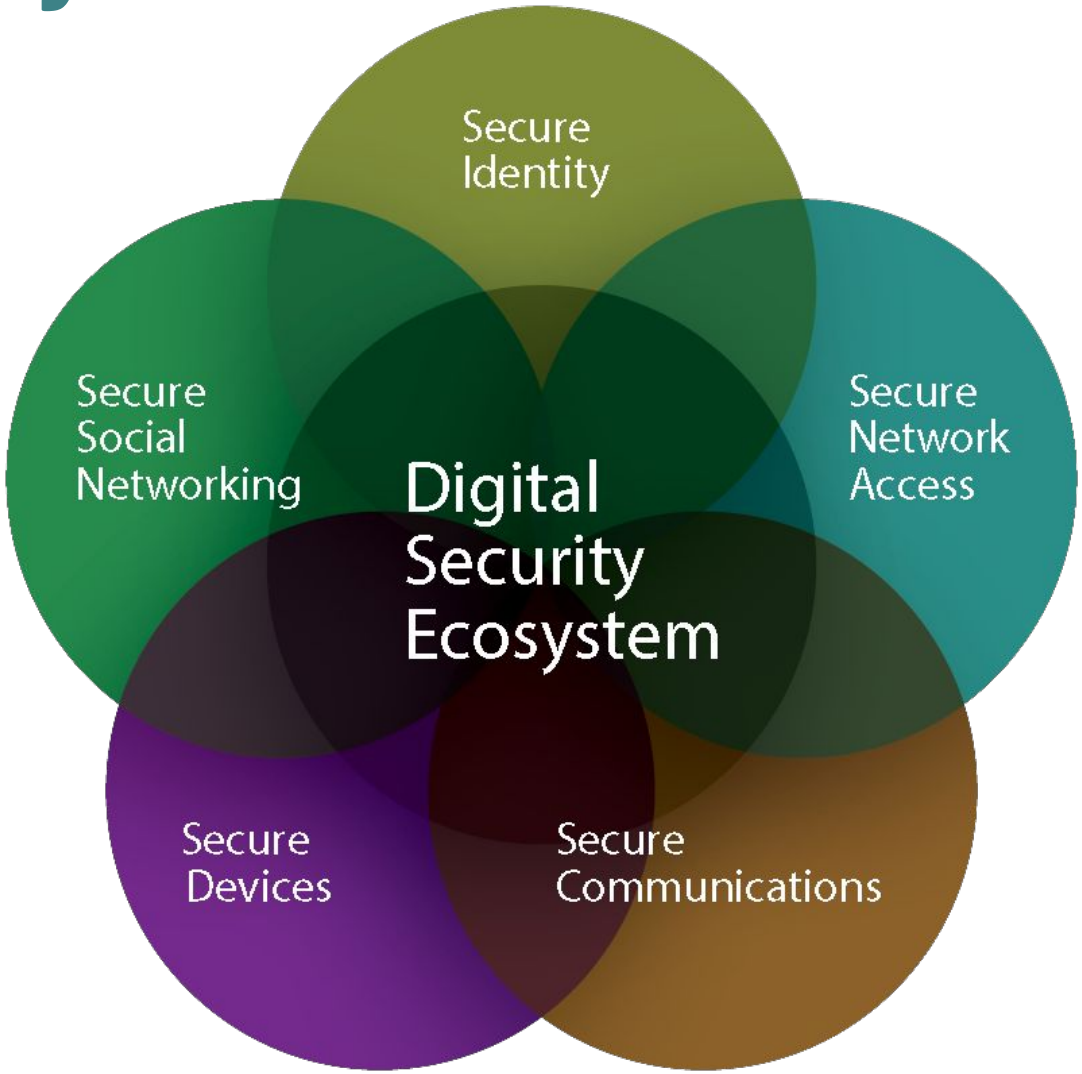
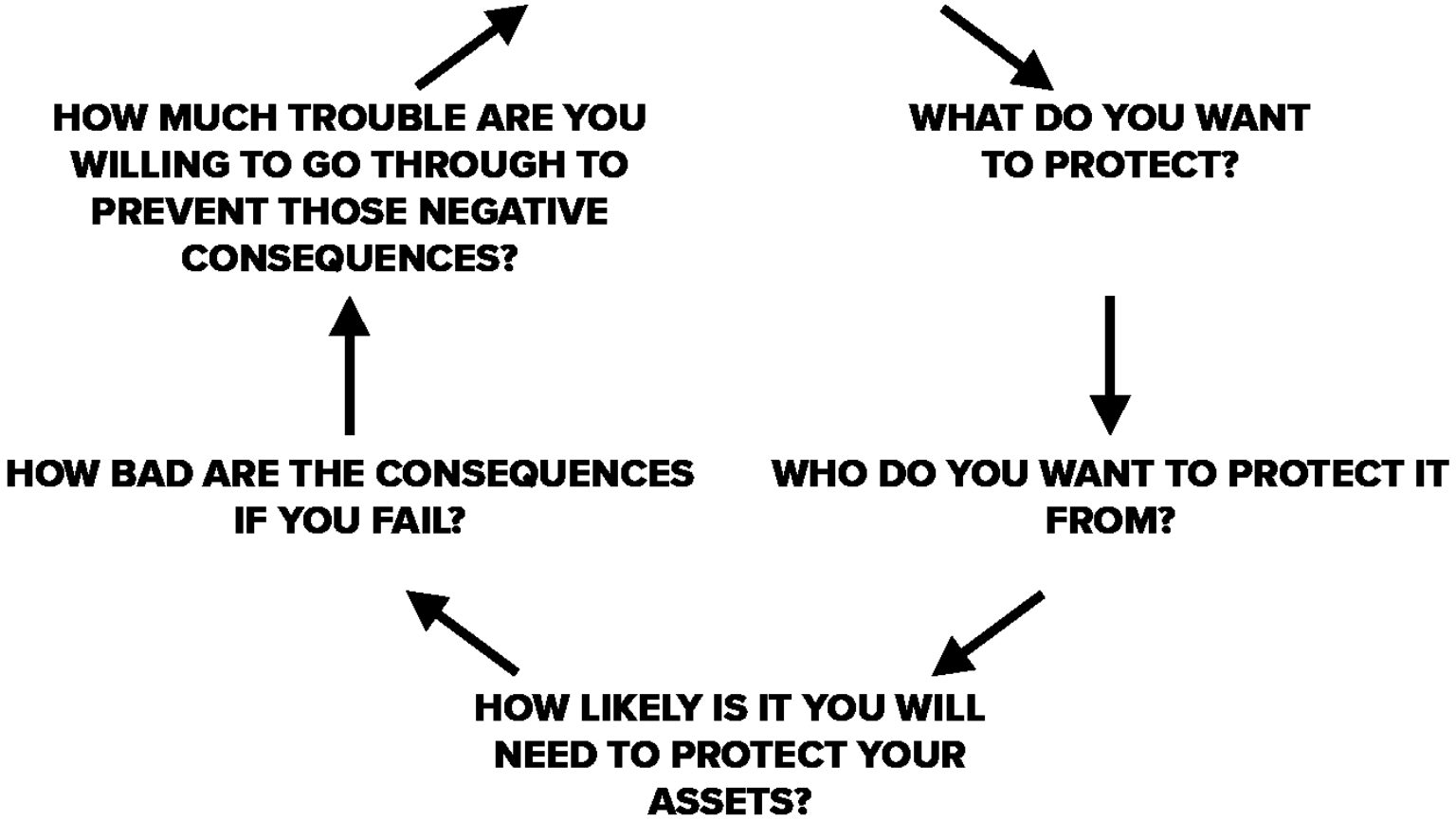


Image source: http://digitalsecurityforall.org/en/curriculum/what_is_digital_security

YOUR RISK ASSESSMENT



Threat & Risk

Threat

A threat is a potential event that could undermine your efforts to defend your people and data about them.

Risk Assessment

Risk assessment and analysis is the practice of calculating the chance that threats might succeed, so you know how much effort to spend defending against them.

Threat model

Threat modeling is a way of thinking about the sorts of protection you want for your people and the information you keep or track about them so you can decide which potential threats you are going to take seriously.

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

Concepts & Terms to Know

Social Engineering

Social engineering broadly refers to the psychological manipulation of human behavior in order to exploit our trust for the purpose of information-gathering, fraud, or system access.

Malware

Malware is short for malicious software: programs that are designed to conduct unwanted actions on your device. Computer viruses are malware. So are programs that steal passwords, secretly record you, or delete your data.

Phishing

Phishing is a form of digital attack with the objective of obtaining access to your email, social media or other online accounts.

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

Social Engineering

Image source:
https://www.realcleardefense.com/articles/2018/07/18/social_engineering_as_a_threat_to_societies_the_cambridge_analytica_case_113620.html

What to watch out for

- Things that are too good to be true
- Messages that convey a sense of urgency and ask you to act promptly
- Email addresses that don’t look quite right
- Messages from and about services you don’t use
- Suspicious links
- Unknown or suspicious files
- Unknown or suspicious devices
- Suspicious phone calls

Steps you can take

- Do not login to websites from a link in an email
- Always install software updates as soon as possible
- Try not to login to websites via Facebook, Twitter, or Google
- Don’t trust emails asking for personal information
- Use HTTPS connections whenever possible
- Beware public wifi

Malware

Malware, short for "malicious software," is software that is used to harm computer users.

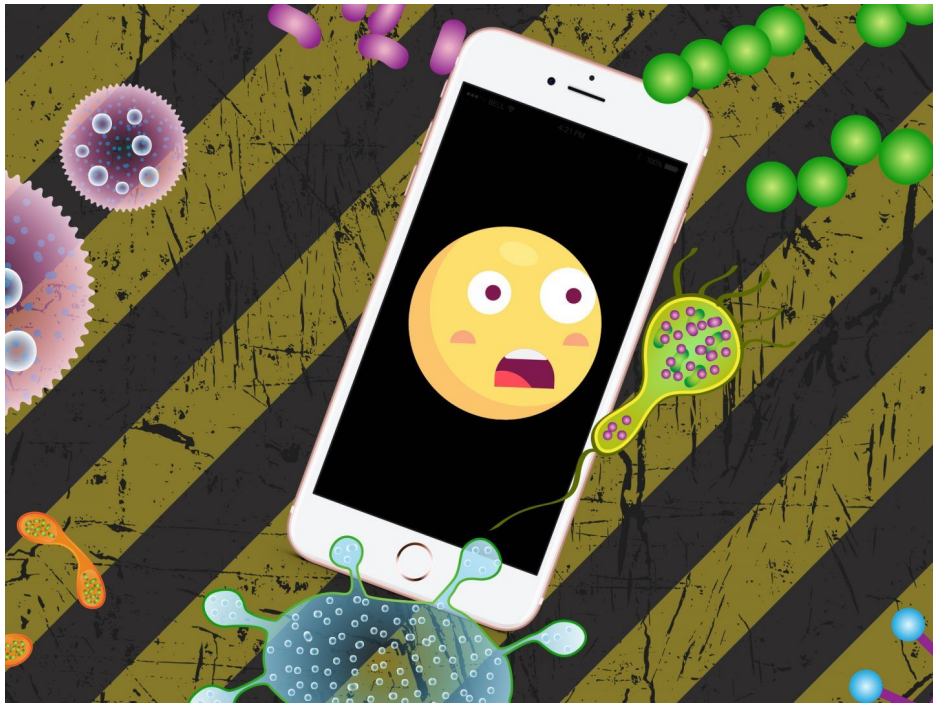
It has a wide-range of capabilities that typically encompass 4 general objectives:

- Disrupting computer (smartphone) operation
- Gathering sensitive information
- Impersonating a user to send spam or fake messages
- Gaining access to private computer systems

Source: https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware

How to prevent malware

The best way to deal with a malware attack is to avoid getting infected in the first place.



Source: https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware

What about antivirus software?

- Note that for antivirus software to work it has to have **deep access to your system** and vulnerabilities in these kinds of software may greatly increase the opportunity for potential attacks.

- Antivirus software, like antibiotics, may help inoculate against known malware (assuming your antivirus software detects it), but ultimately, the system-level patches that are delivered by your operating system's software updates are what give it innate immunity.

Install operating system updates

- **Windows 8 users**: *Start menu > Control panel > System and Security > Windows Update*
- **Windows 10 users**: *Start menu > Settings > Update & Security > Windows Update*
- **Chrome OS users**: *Settings > About Chrome OS > Check for updates*
- **Mac users (Mojave or newer)**: *Apple menu > Software Update*
- **iPhone and iPad users**: *Settings > General > Software Update*
- **Android users**: *Refer to your device's manufacturer's website to learn where to find your device's update settings.*

Addressing a malware attack

- If you find malware on your computer, unplug your computer from the Internet and stop using it immediately.
- Note that if you've found the malware, removing it does not guarantee the security of your computer.
- Log into a computer you believe is safe and change your passwords; consider every password that you typed on your computer while it was infected compromised.
- Reinstall the operating system on your computer in order to remove the malware. This will remove most malware, but some especially sophisticated malware may persist.

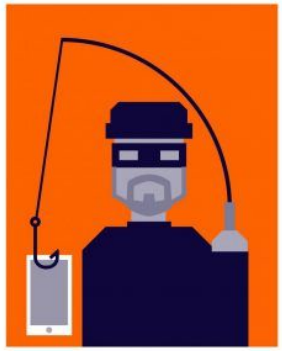
Phishing

Phishing is a social-engineering attack where an adversary crafts an email in such a way to trick you into divulging information that could be used against you or your network; gain access to, and ultimately commandeer your account; or introduce malware and/or viruses to your machine.

Spear phishing is just like phishing, except the attacker uses information they already knows about you to specially tailor their phishing email.

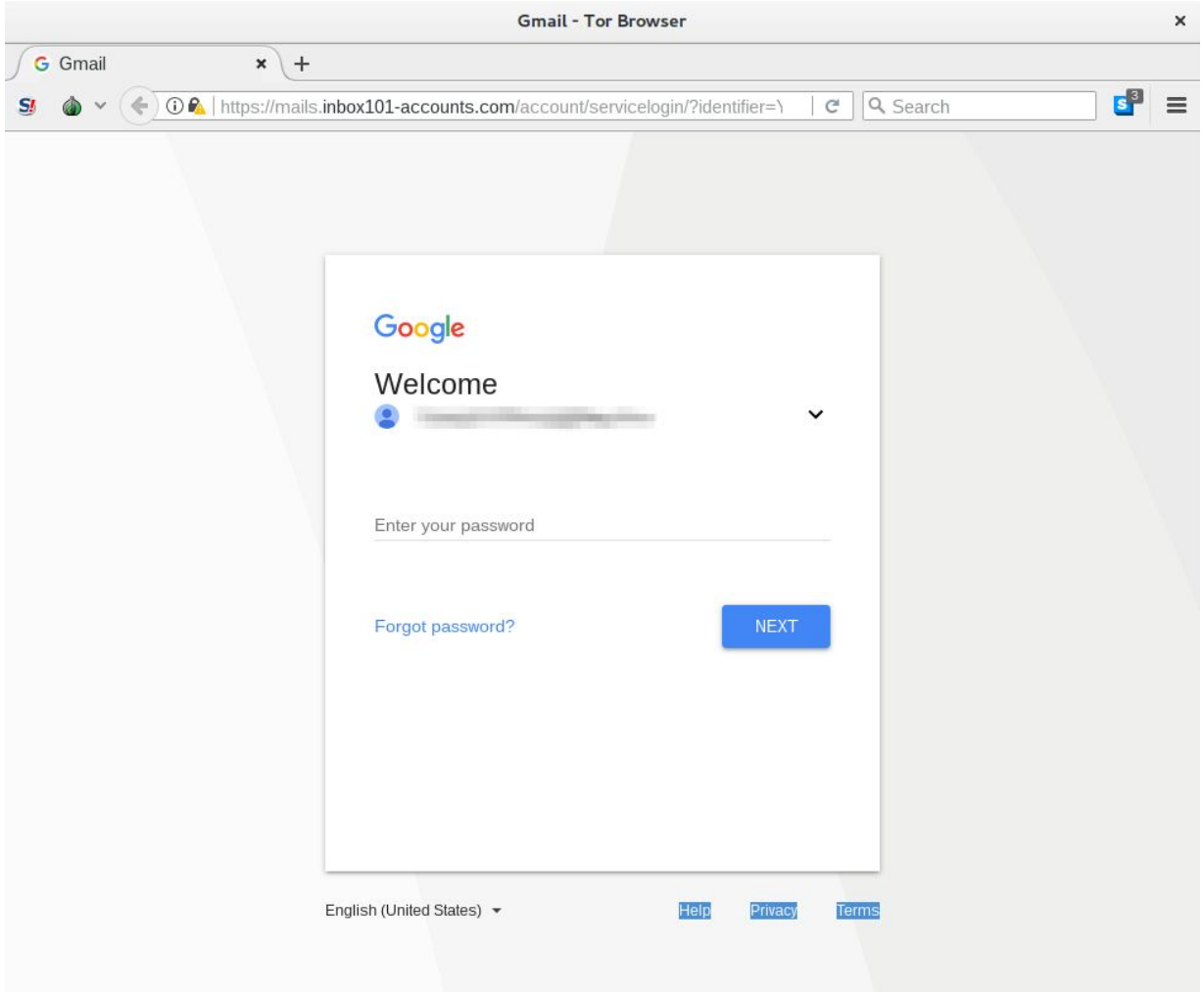
There are different types of phishing attacks, but essentially we can categorize them in two:

- Password-Stealing Phishing
- Open Authorization or “OAuth” Phishing (aka Third-Party Application Phishing)

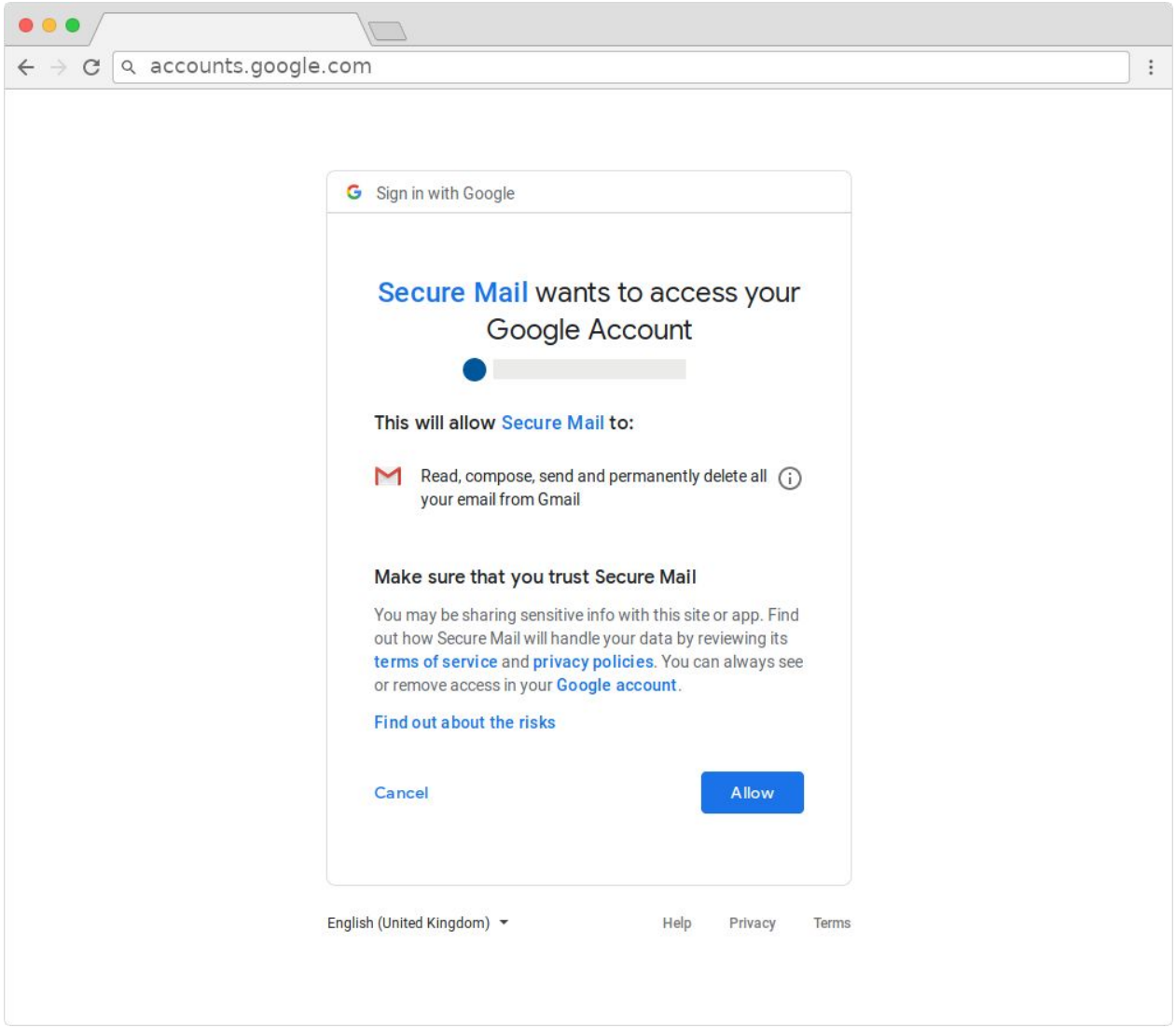


Source: https://freedom.press/training/email-security-tips/

Password-Stealing Phishing



OAuth Phishing



https://guides.securitywithoutborders.org/guide-to-phishing/password-phishing.html

Other Phishing Examples

Dear Sir or Madam,

I'm making contact with you to statea payment mistake in the amount $144 on mybank account. This amount is inaccuratebecause youliterally billed me twice. I amasking for the error endup being solved, that any funds and alsoother payments related to thedebated amount becredited too, and thatI get anappropriate statement.
Attached are the bank statement as well as theinvoice confirming mysituation. Pleasecheck out thisissue and solve theinvoicing mistake asquickly as possible.

My Bank Statement

Respectfully Yours,
Al Scogin

There's issue with your American Express account

AE American Express <administraciones@pentagon-seguridad.cl>
To hashedout@thesslstore.com

Reply | Reply All | Forward | ...

Fri 11/8/2019 5:29 AM

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

AMERICAN EXPRESS

Review Your Information.

Due to recent activities on your account, we placed a temporary suspension untill you verify your account. You need to review your information with us now on 11/8/2019 10:28:38 AM.

To continue using our American Express Online service, we advise you to update the information about your account ownership.

Click here to review your account now

For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit American Express Support.

Sincerely,
American Express Company. All rights reserved

Fri 3/15/2019 2:56 PM

AG Adelaida Gobin <gr8n8no@cox.net>

Job Application

To Billing - The SSL Store

VIRUS_DETECTED_AND_REMOVED.TXT
498 bytes

Hey,
My name is Adelaida Gobin and I'm interested in a position.

I've attached a copy of my resume.
The password for the document is 1234

Looking forward to hearing back from you!

--
Adelaida Gobin

Spoofed Internet domains pose cyber and disinformation risks to voters

From: Proud Boys <info@officialproudboys.com>
Date: October 20, 2020 at 9:44:59 AM CDT
To: [redacted]
Subject: Vote for Trump or else!

[redacted] We are in possession of all your information (email, address, telephone… everything). You are currently registered as a Democrat and we know this because we have gained access into the entire voting infrastructure. You will vote for Trump on Election Day or we will come after you. Change your party affiliation to Republican to let us know you received our message and will comply. We will know which candidate you voted for. I would take this seriously if I were you.

https://www.thesslstore.com/blog/phishing-email-examples-the-best-worst/

Phishing Quiz

How to Prevent Phishing

- Understand threat modeling
- Use two-factor authentication
- Understand how to identify the “from” field
- Beware of attachments (Change your settings so that certain files never execute, but instead open up in a text editor application. Ideally, whichever text editor you use should not sync to the cloud.)
- Be skeptical of links (mouse to hover over any link before clicking on it, to see what the actual URL is.)

˜StrONG~P@zzwords/.

Here are a few general rules to follow for creating good, strong passwords:

- A mixture of random letters, numbers, and special characters is best
- The longer, the better. 12 characters or more
- Consider using passphrases
- Don’t reuse passwords across multiple sites
- You should not (in most cases) share your passwords and passphrases with other people.

Password Managers

You can use a password manager (which is a digital encrypted vault) to drastically improve the security of your accounts and make the whole process of managing such sensitive information easier.

Well-regarded options when it comes to choosing one are:

- **1Password** – Support, Beginner's guide
- **Bitwarden** – Help Center
- **KeePassXC** and **Strongbox**/**KeePass2Android** – Beginner's guide
- **LastPass** – Help, Beginner's guide

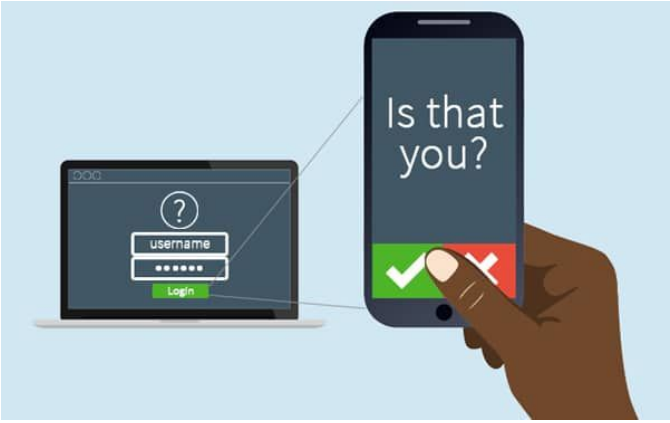
Source: https://preciselyprivate.wordpress.com/good-practices-guide/#password-management

2FA

Two-Factor Authentication (https://twofactorauth.org/)

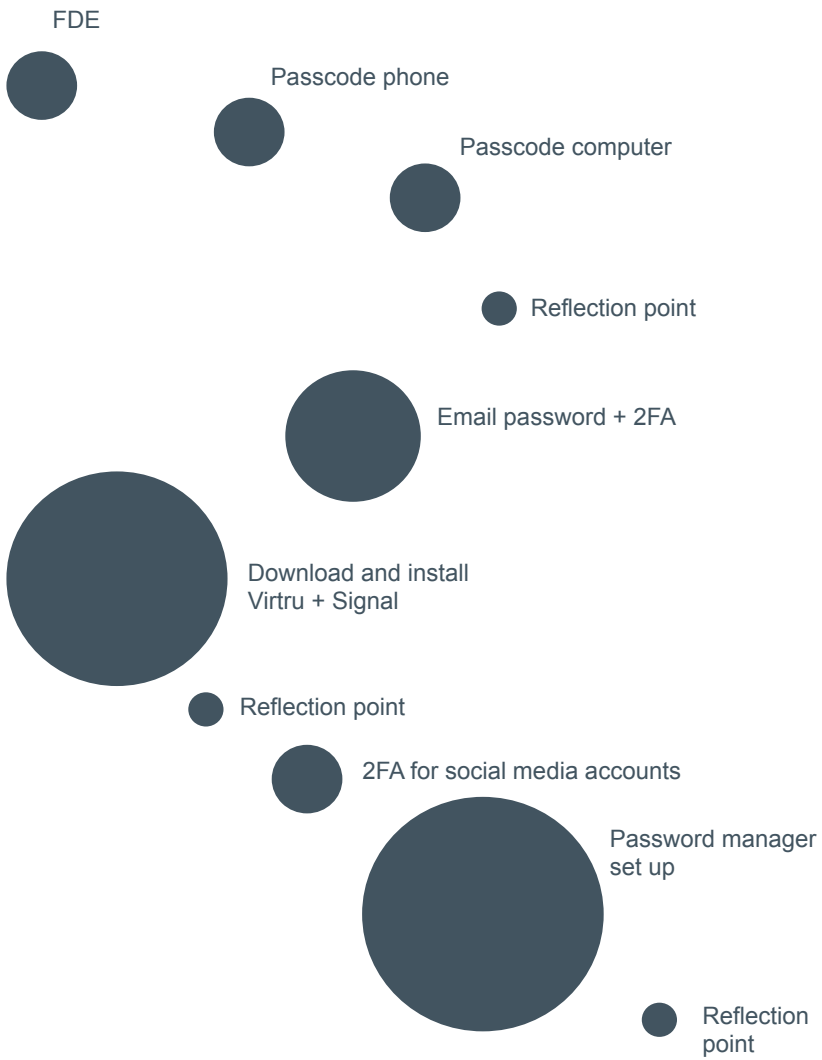
"Something you know, and something you have." Login systems that require only a username and password can be vulnerable to someone else obtaining (or guessing) those pieces of information. Services that offer two-factor authentication also require you to provide a separate confirmation that you are who you say you are.

The second factor could be a one-off secret code that is sent to you via email or text, a number generated by a program running on a mobile device, or a separate device, such as a USB authentication token that you carry and that you can use to confirm who you are.



Goal

Phases, Small Wins, Reflection Points



Tools, Accounts, Devices + Practices

	Virtru	Signal
Tool setup	Install + setup browser plugin	Install + setup browser plugin
	Download, install + setup phone app	Download, install + setup phone app
Account prep	Strong email password	
	Two-factor authentication	
Device prep	Passcode set	Passcode set
	Full disk encrypt	Full disk encrypt (if necessary)

Action Steps

1. **Update all the things**

   When you get a notification to update your operating system (on your mobile or computer), do it as soon as you can.

2. **Email**

   If you're on a webmail service, check that you're logging into it using an ***https:// URL***. And if there isn't one, find a new email provider.
   Turn on two-factor authentication for your email service (e.g. instructions for Gmail, Protonmail) through an authenticator app (e.g. Authy, Google Authenticator).

3. **Good passwords**

   Double check the security questions for your key online services (email, bank, Facebook, etc.) and make sure that they're not easy to answer by friends/looking you up on Google. Start using a different password for every service, because password leaks happen all the time. To make this easy, use a password manager .

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 3

Safer Communication & Internet Browsing

re: POWER

Reclaiming Our Power for Radical Change