



digital defense fund

Digital Security Essentials for Elected Officials

Digital Defense Fund
2021

Introduction

Amanda Bennett

she/her

Austin, TX

Project Manager

Digital Defense Fund

- Background in public policy & case management at a small non-profit
- Started using tech to implement a text hotline to better reach young people
- Used the same password for everything until two weeks before starting this job!

Kate Bertash

she/her

Los Angeles, CA

Director

Digital Defense Fund

- Background in public policy & startups, long ago campaign and congressional intern
- Started doing privacy and doxing-prevention work w/ victims of image abuse
- Has had passwords appear on 18 breach lists and counting. Happens to all of us!



Goals of today's workshop:

- Meet the moment: let's talk about IT infrastructure during a physical attack.
- Looking forward:
 - Learn how to use strong passwords & two-factor authentication to protect your accounts
 - Identify precautions you can take to keep private information private
 - Make safety plans before you need them

A quick note on physical vs. digital security

- This presentation will focus on digital security and on protecting IT infrastructure if you have to leave your office
- Make sure you pair this work with a physical safety plan as well

A quick note on physical vs. digital security

- This presentation will focus on digital security and on protecting IT infrastructure if you have to leave your office
- Make sure you pair this work with a physical safety plan as well
- A physical safety plan can include:
 - A security team, if your municipality/state provides one
 - Familiarizing yourself with your buildings' entry security, guest procedures, and policies
 - Safe place ready to go if you need to leave your home
 - A home security system
 - Support network of neighbors and friends

Take care of yourself!

We know digital security and physical security topics are scary, especially in light of the current threats elected officials are facing, and especially if you've faced online harassment, identity theft, or other online attacks before.

We're here to support you.

Feel free to take a break and remember to drink water, have a snack, and step away if you need to take care of any needs!



Agenda

- IT security during a physical breach
 - Things you can do to prepare
 - Topics to discuss with your IT & security teams
- Threat modeling for the most common digital threats
- Account security
 - protecting your accounts from getting hacked
- Online presence
 - what's out there & what you can control
- Harassment & online threat response

Office IT Security



Pwn All The Things

@pwnallthethings



Replying to [@pwnallthethings](#)

**When violent rioters break into your workplace, the 100%
right thing to do is leave immediately and go to safety.
People are more important than computers.**

10:24 AM · Jan 7, 2021 · Twitter Web App

51 Retweets **7** Quote Tweets **431** Likes

Our Device & Network Security Goals

- If someone steals a laptop or phone, ensure it's useless to them
 - Disc encryption
 - Strong unique password protection
- If someone gains unauthorized access to your office, ensure they can't access your network
 - Strong unique wifi/network password protection
 - Autolock for computer screens

Our Device & Network Security Goals

- If someone steals a laptop or phone, ensure it's useless to them
 - Disc encryption
 - Strong unique password protection
- If someone gains unauthorized access to your office, ensure they can't access your network
 - Strong unique wifi/network password protection
 - Autolock for computer screens

In summary: if you have to leave your office on short notice, you can focus on your people and their safety, knowing that the sensitive information you steward is safe by default.



IT Preparation

These tasks can be implemented by individual staffers, or at the network level if available. Coordinate with your Chief of Staff or related role:

- Full disc encryption
- Auto-lock on screens
- Keep your devices and software updated
- Know where to go to end active sessions (log out):
 - For your email
 - For your password manager
 - For other key accounts

IT Fire Drills

- Lock your computer whenever you step away from it
 - Some computers have a “hot key” or shortcut to do this – google your model of laptop and “quick log-out”
- Practice ending sessions on your desktop/laptop from your phone
 - This can vary by email service or other software service
 - This will often look like “log out of all other sessions” under a privacy or security section of the email service on your phone

IT Fire Drills

Look through the eyes of an intruder:

- Walk through the office after hours, or during a drill, and look around.
- What items, documents, devices are left out on desks? Which items are sensitive and can be moved into lockable storage when not in use?
- What document storage or filing cabinets are accessible? Can sensitive documents be moved into locking cabinets?

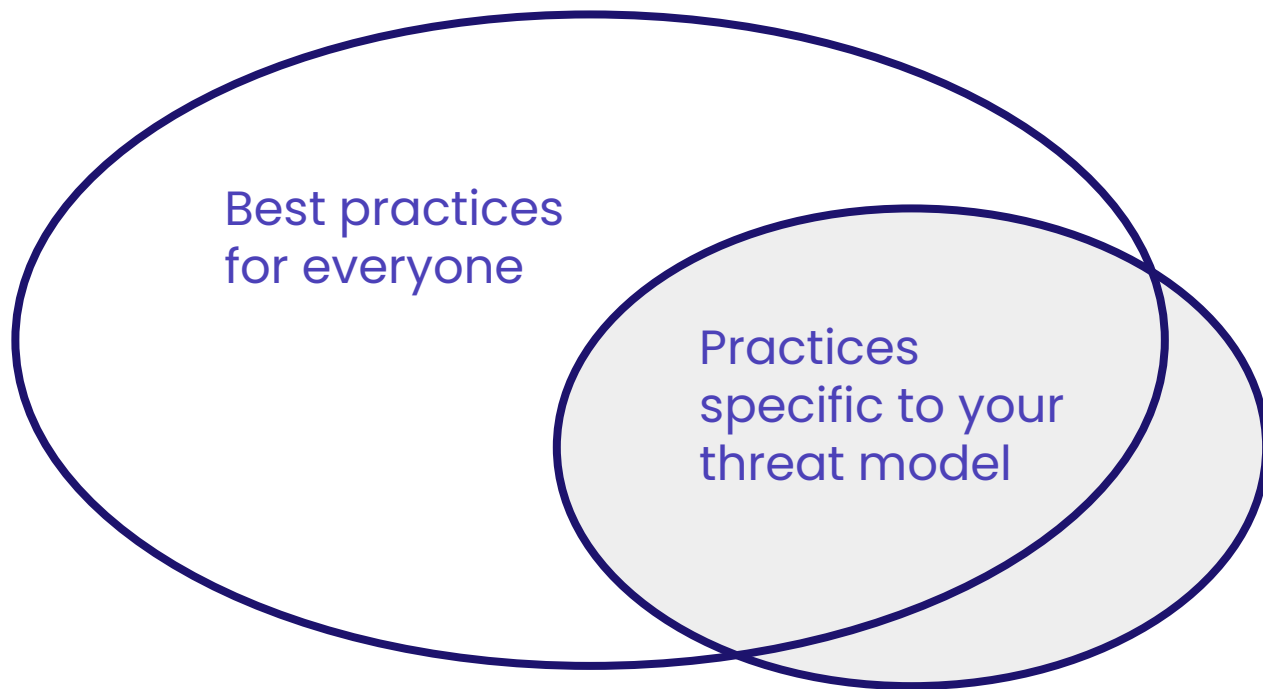
Questions to ask your IT team:

- Can we enforce auto-lock on screens in the office?
- Can we lock devices remotely?
 - If not: can we force logouts from important accounts remotely?
- Can we enforce full disc encryption on computers and phones?
- Can we auto-update devices and their software?
- What protocols are in place for IT infrastructure/devices if we need to evacuate the office?
- What protocols are in place to ensure devices have not been compromised in the case of unauthorized access?

Threats that were top of mind
before January 6th...

Overview of Common Digital Threats: Account Compromise & Harassment

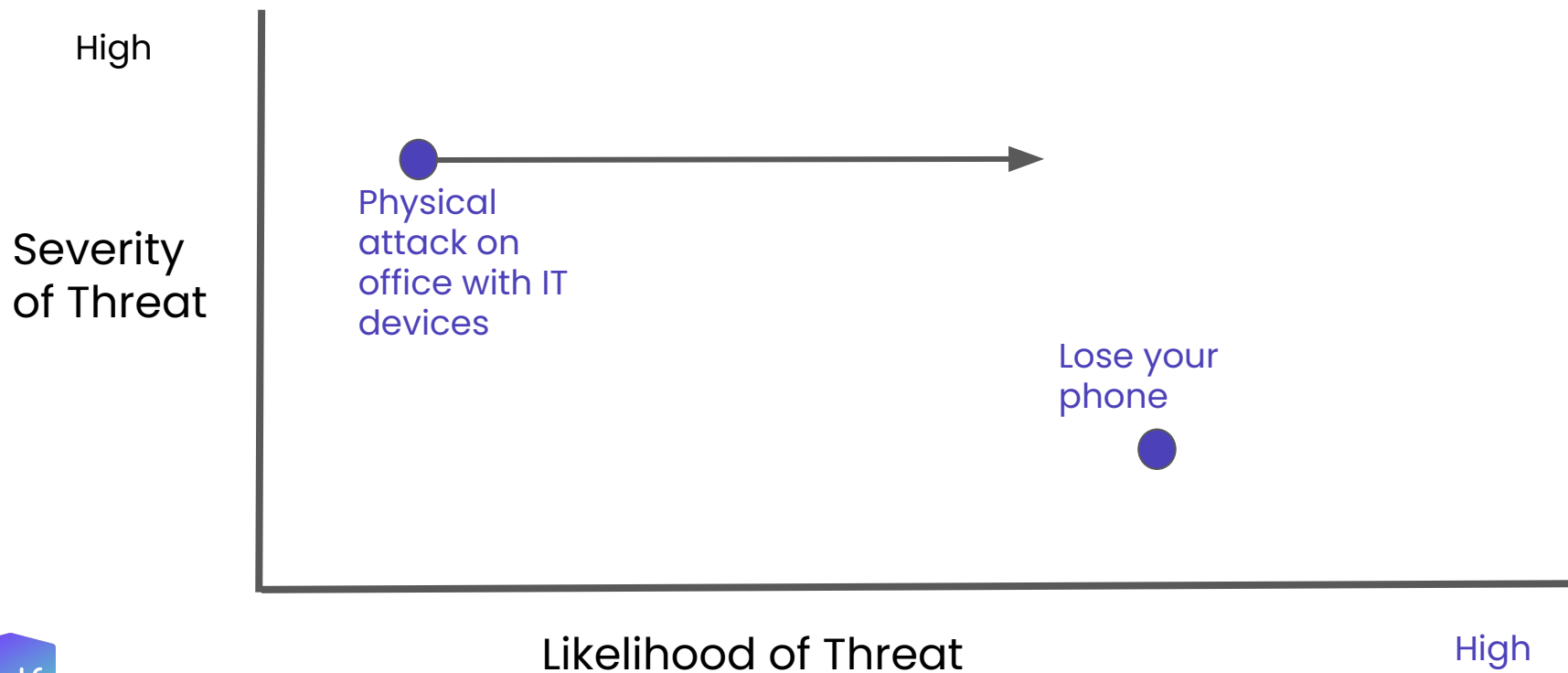
Threat Modeling:



Threat modeling helps us ground our fears in reality.

The best way to predict what can happen is by looking at what has happened in the past.

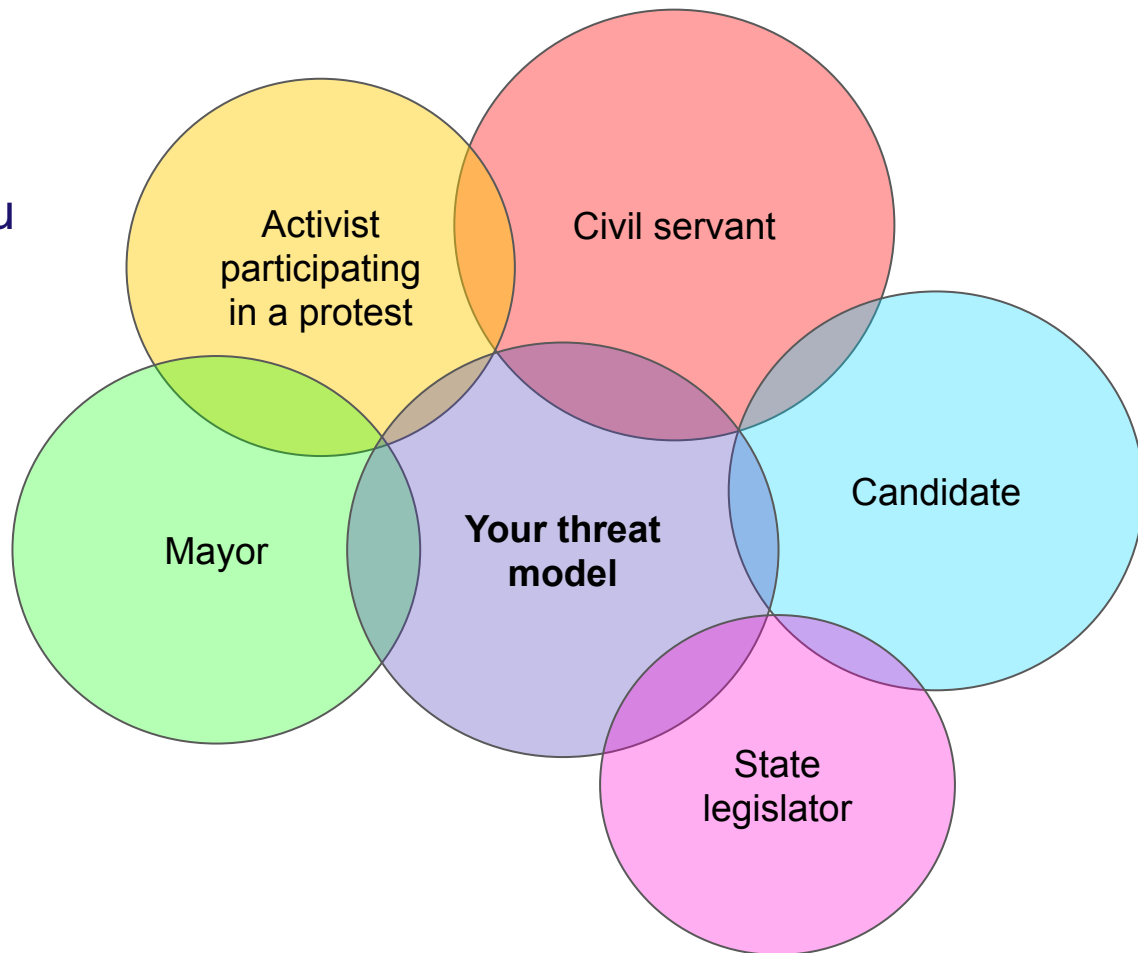
Threat Modeling Example: Device Compromise



Context is key!

What type of work are you doing?

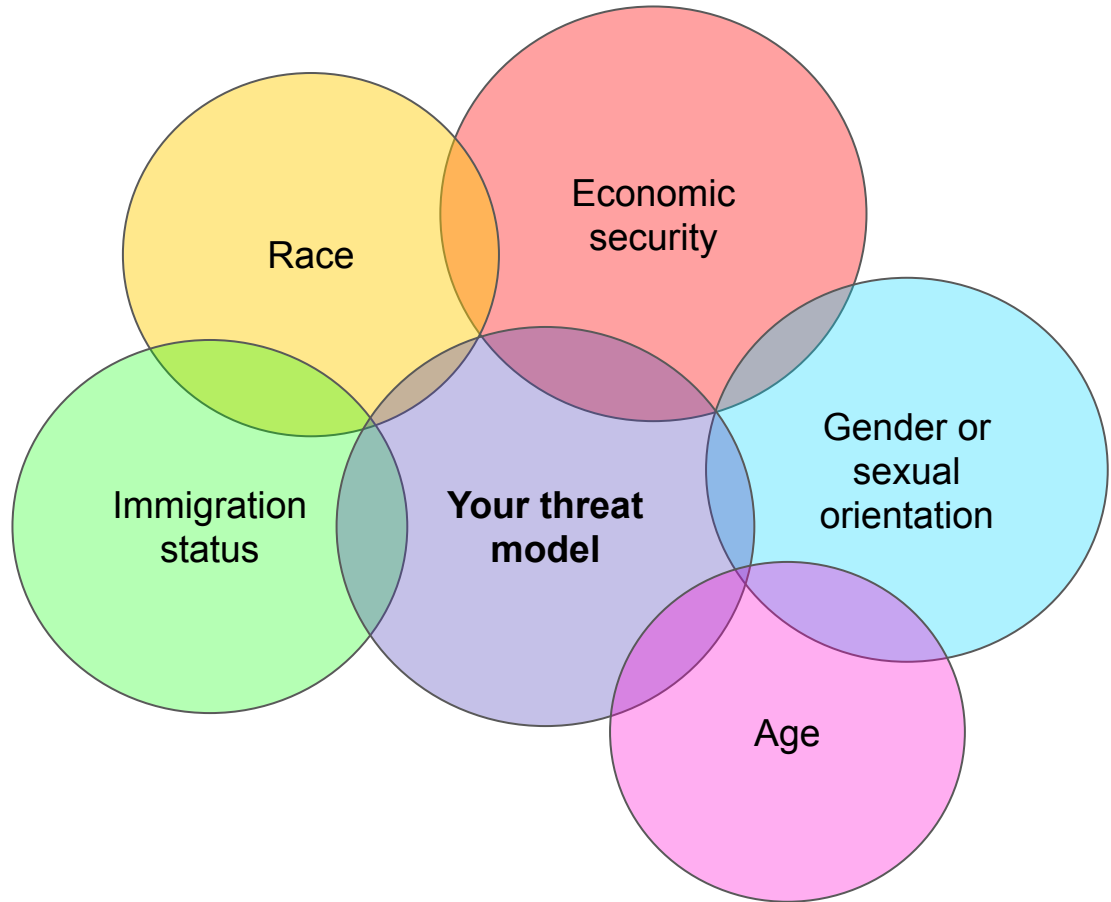
This affects the type of threat you'll face.



Context is key!

What about your identity affects how you move through the world?

This can affect how severe impact of a threat will be.



Digital Threat Modeling



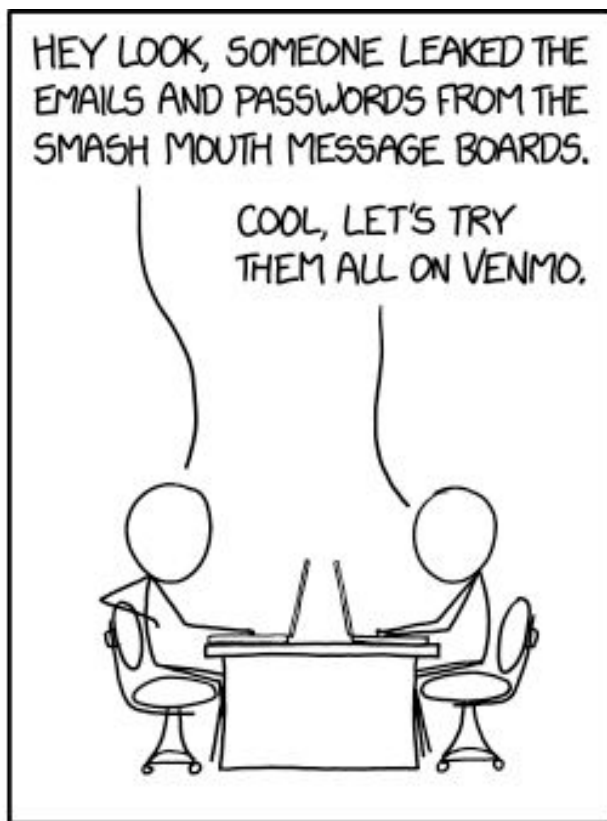
Paths of Escalation

- Taking a threat from one level to the next is called escalation
- Note that as the severity of a threat increases, its likelihood usually decreases
- **Our best defense is making escalation more difficult**

Solutions: Account Security & Preventing Hacking



HOW PEOPLE THINK
HACKING WORKS



HOW IT ACTUALLY WORKS

How does an attacker get your password?

- Guessing it
 - Dictionary attacks/brute force guessing
 - Easily searchable things about you (birthday, pets names)
- Finding it
 - Breach list + password reuse
- Tricking you into divulging it
 - Phishing
 - Social Engineering

```
Dictionary Attack
Trying apple      : failed
Trying blueberry  : failed
Trying justinbeiber : failed
Trying ...
Trying letmein    : failed
Trying s3cr3t     : success!
```


Know your risk:
Could someone have your
password right now?

Checking public breach lists

Let's check a trustworthy website that lists public lists of already stolen passwords and emails.

→ haveibeenpwned.com

Pro tip!

Subscribe your email address to haveibeenpwned to get an alert if you're in a breach!

What sites come up?

- Have you used the passwords from those sites anywhere else?
- ... Have you used those passwords for any work accounts?

Solutions: Password Security

The trick: a strong, unique password!

What makes a password strong?

→ howsecureismypassword.net

How Secure Is My Password?

 The #1 Password Strength Tool. Trusted and used by millions.

A white rectangular input field with a red border. On the left side, there is a blue arrow pointing right. Inside the field, the text "passw0rd" is displayed. On the right side of the field, there is a small grey icon consisting of three dots.

Your password would be cracked

Instantly

How Secure Is My Password?

 The #1 Password Strength Tool. Trusted and used by millions.

hg7Vtzy#



It would take a computer about

8 hours

to crack your password

How Secure Is My Password?

 The #1 Password Strength Tool. Trusted and used by millions.

hg7Vtzy#45fw2s



It would take a computer about

2 hundred million years

to crack your password

How Secure Is My Password?

✔ The #1 Password Strength Tool. Trusted and used by millions.

silly brutal safe travel



It would take a computer about

3 sextillion years

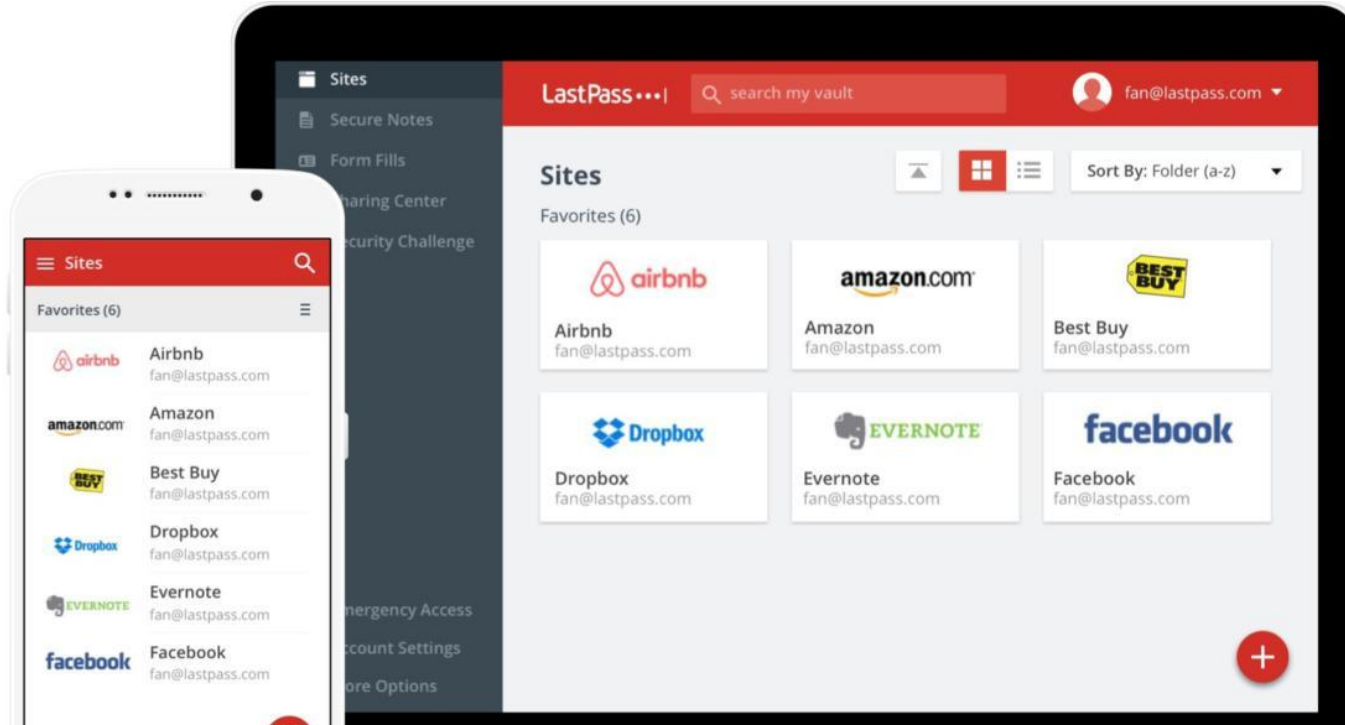
to crack your password

Remembering unique, complex passwords for every account is VERY hard.

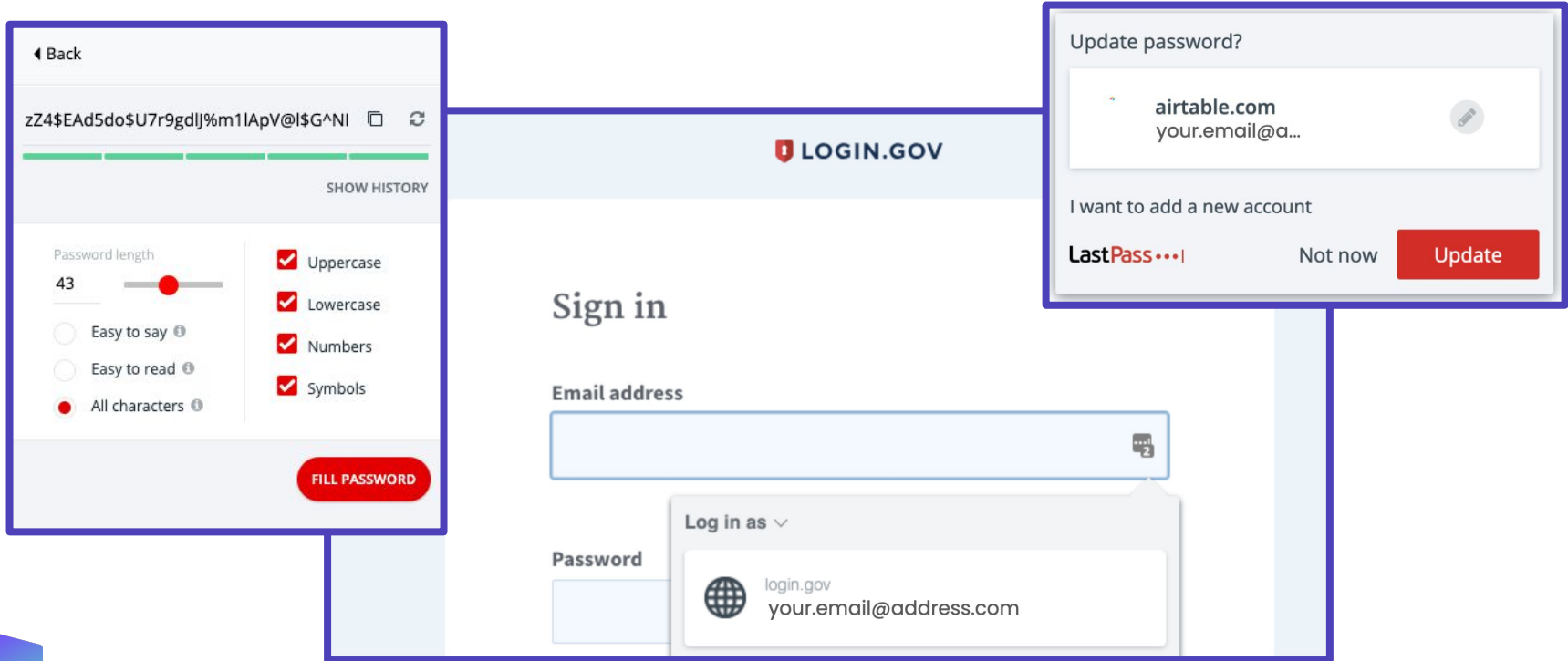
That's why password managers exist!

What's a password manager?

Password management services generate and hold diverse, strong passwords.



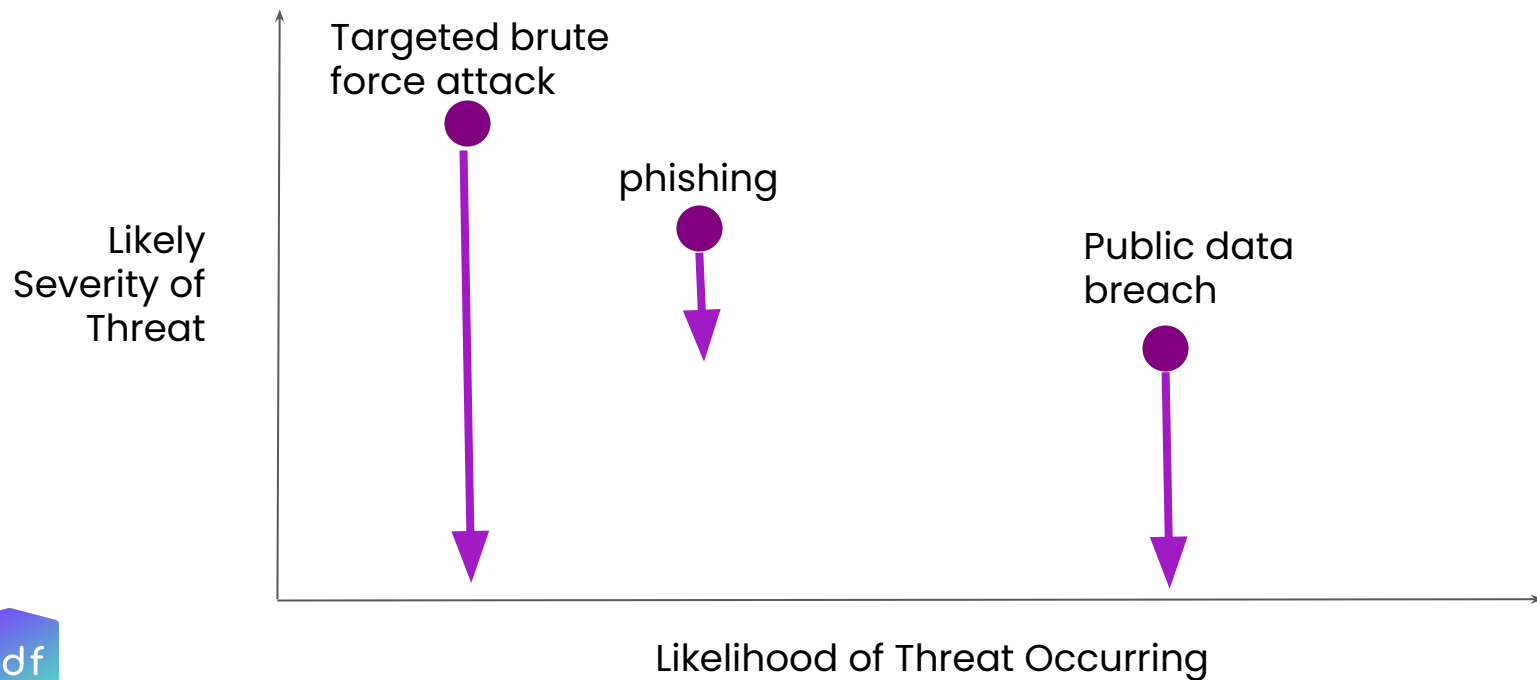
Password Managers are Convenient!



Harm reduction approach

- Implementing use of a password manager across an entire office can take some time.
- Some potential first steps you can take today include:
 - Prioritize changing passwords for your most important accounts
 - Start using a password manager yourself, making sure you store the access codes in a safe place (in case you forget your password to the password manager)
 - Configure the password manager to lock every 12-24 hours so you memorize your master password by re-entering it often

Using a strong, unique password for each account + a password manager



Key takeaway:

Do whatever you can to avoid password reuse and weak passwords!

Solutions: Multi-Factor Authentication



MFA keeps your
account safe even
if your password is
compromised

More than your password

“2 factor” or “multi-factor” authentication

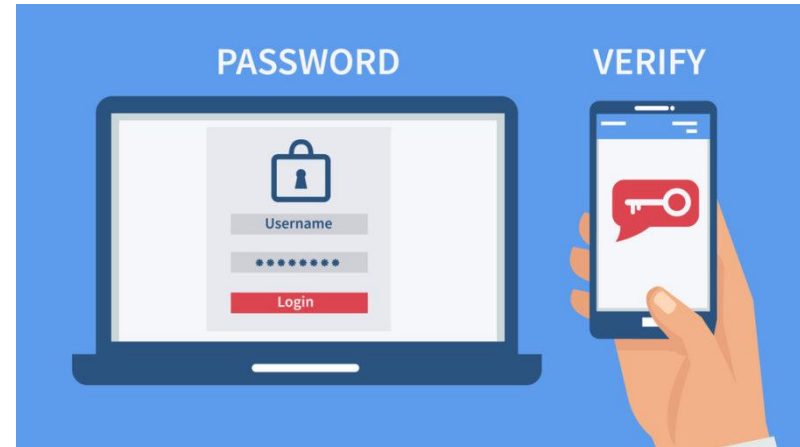
- Something I know (a good password) = good
- Something I know + something I have with me = even better!



Types of MFA

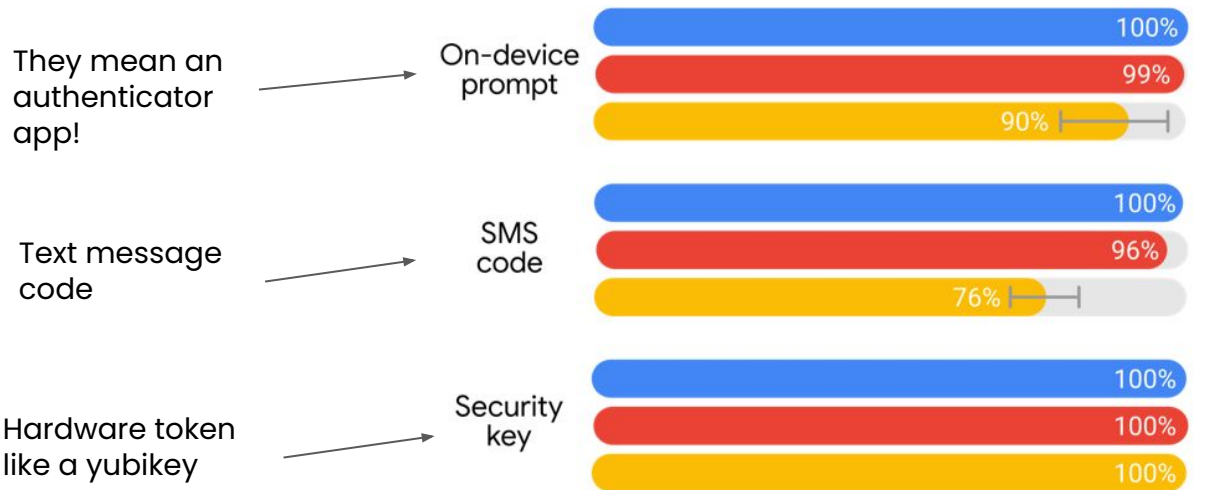
The second factor might be:

- A text to your phone
- A number in Google Auth or another authenticator app
- A yubikey or other physical key



How Effective is MFA? Account Takeover Prevention Rate

Device-based challenges



Hide notifications content from showing up when your phone screen is locked!

Risk for high profile targets: SIM Swapping



Yubikeys (aka hardware tokens) are strongest!

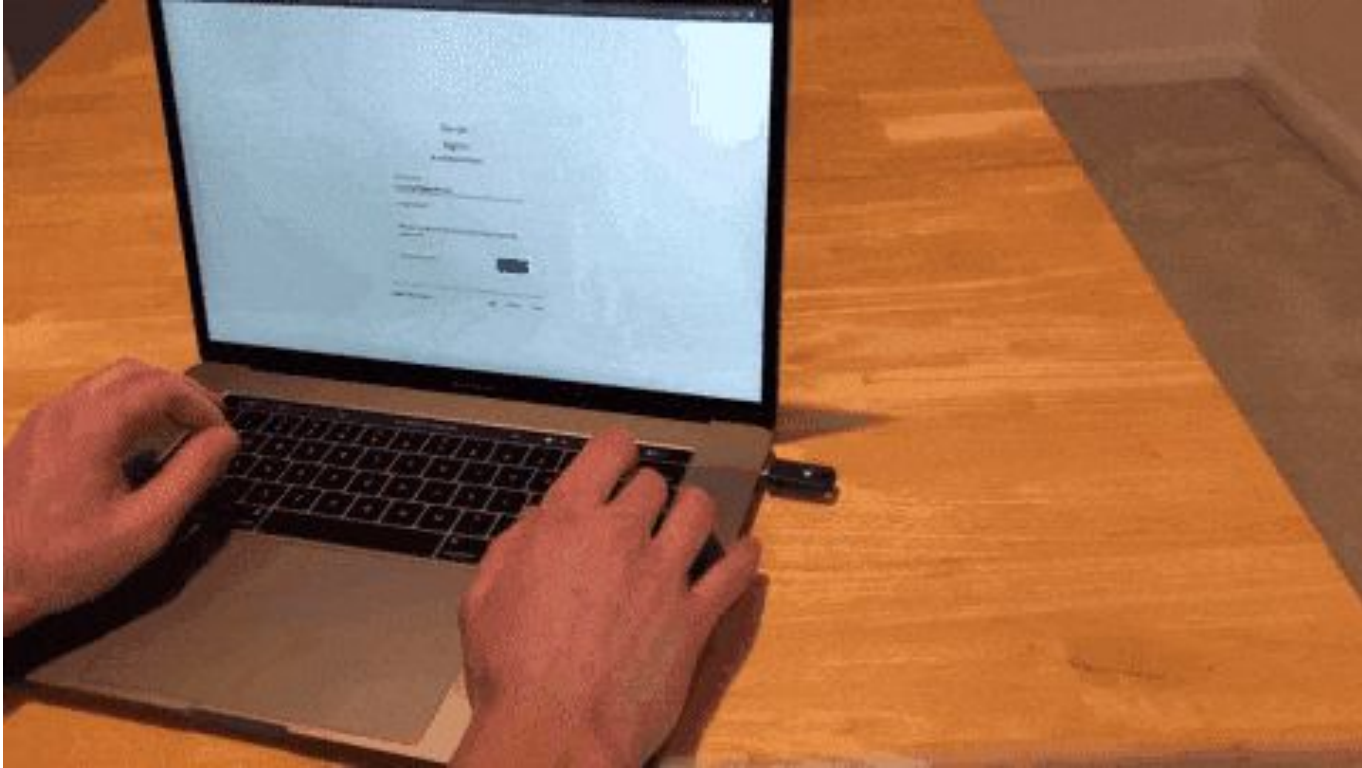
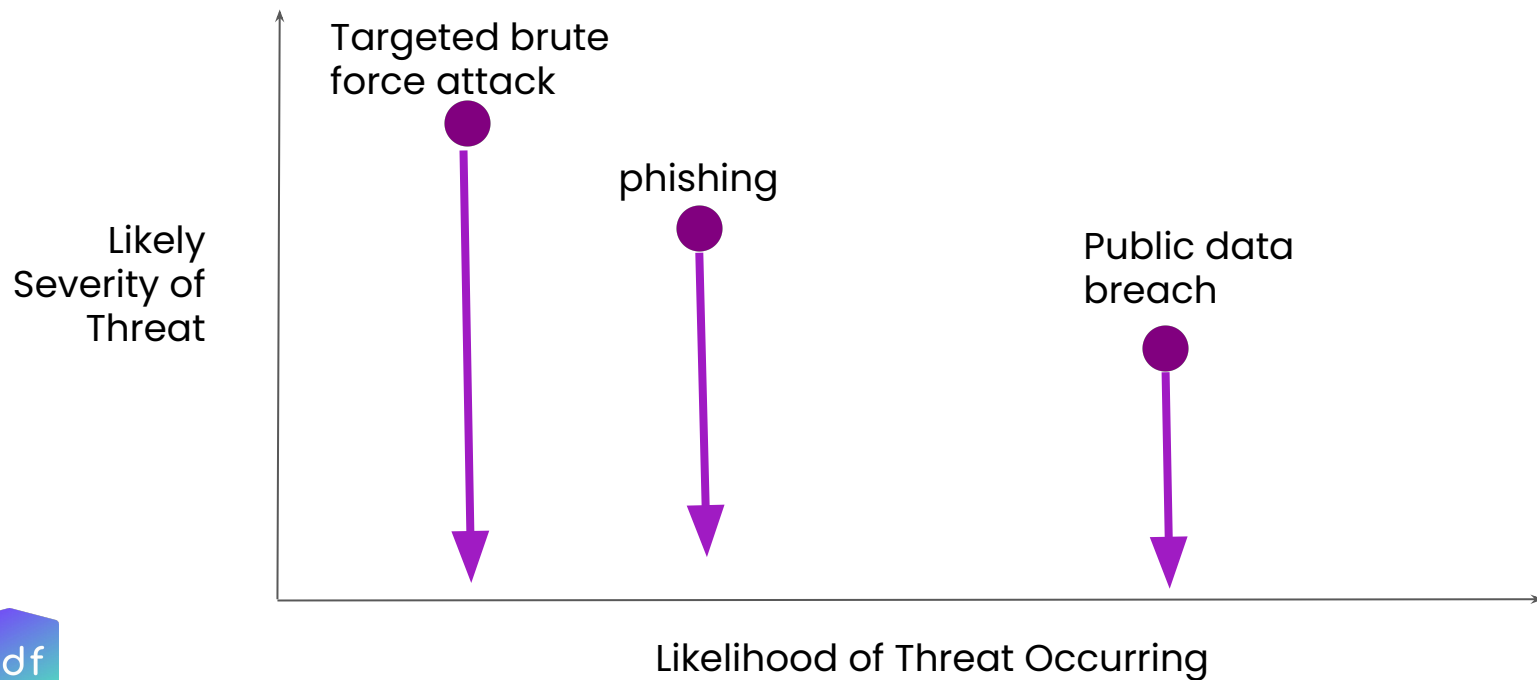


Illustration of security key from Solo (open source security key).

Create a recovery plan as you set up MFA

- We recommend saving recovery codes in your password manager, or printing them out and storing them in a locked cabinet or safe.
- If 2FA is managed by your IT team, ask your IT team if you can get into your account if you lose your phone or your yubikey.

What does turning on MFA do to the severity?



Key takeaway:

Turn on MFA -- this way even if you get pwned you won't get hacked!

Know your doxxing risk:
Search yourself!

Think like an attacker: Can you find your private personal info on Google?

- Google “[your name] + home address”
- Google “[your name] + phone number”



This will be different from people who aren't public officials!

- For the general public: It might be possible to disappear from the internet!

This will be different from people who aren't public officials!

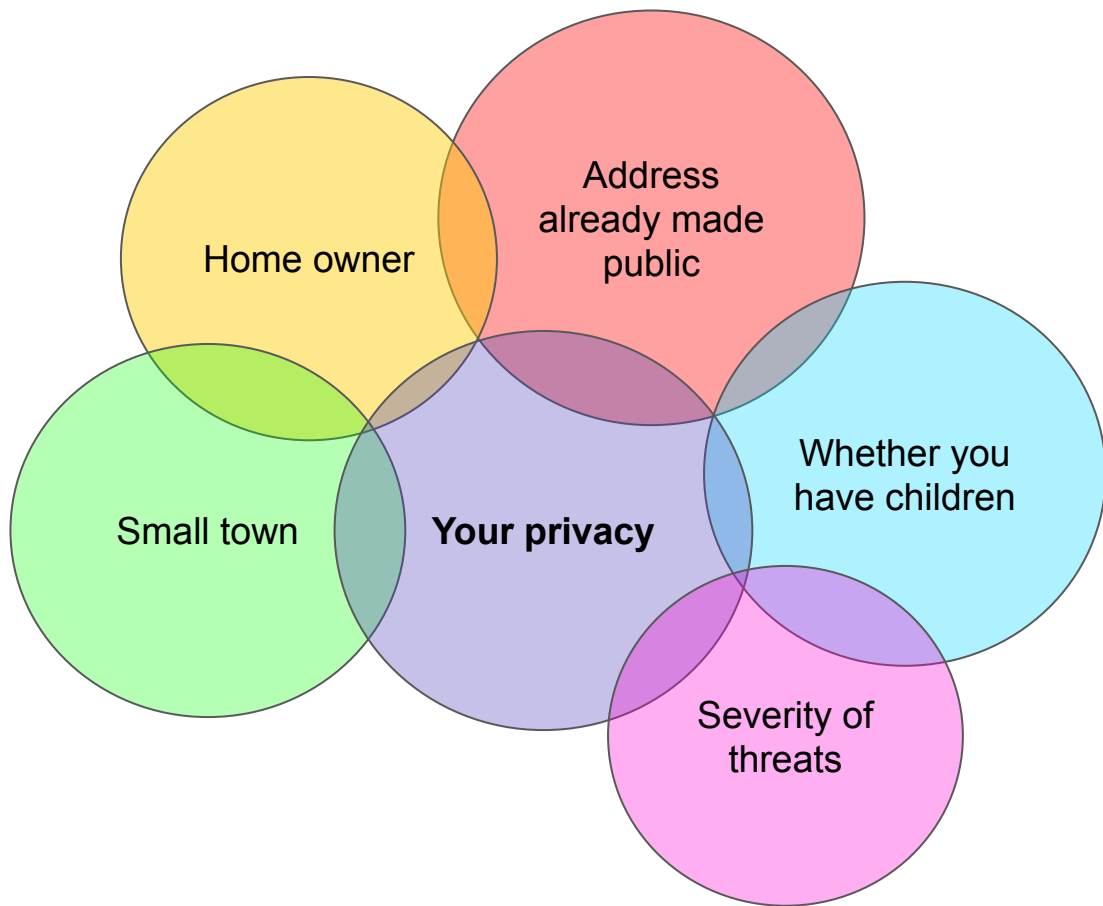
- For the general public: It might be possible to disappear from the internet!
- For public officials: There's a lot online about you that is out of your control, or that has to be public due to the nature of your job. You will want to focus on certain pieces of information you want to make harder to find!

Solutions: Keeping personal data private

Context is key!

How private you can be depends on your context.

These privacy suggestions are all potential tools for your toolbox – you get to decide which tools are most useful for you!



In some cases, your address will be public record.

- Do you own a home in your name? Property records are public.
- If you are involved with a non-profit or a business, are you one of the principal or registered agents with the Secretary of State or the IRS? This person's name and address are public.
- Did you file to run for office with your home address on public documents?

Find out what's out there, round 2

- If you own property: search your local government's property tax or real estate transaction databases to see what information is attached to your name.
- If you are involved with a nonprofit: check their tax documents on the IRS website and your state's business entity database to see what information is available about you on their paperwork.
- If you have ever owned a website: look up the website registration data at <https://lookup.icann.org/> to see if your address, email, or phone are publicly connected to your website.



Totally hiding your address is possible, but not realistic for most of us

In order to completely hide your address from the public, you'd have to:

- Buy your house in a trust
- Consider buying your car in a trust, too
- Always use a different name when ordering delivery
- Set up public utilities with a different name or address
- Have mail & packages delivered to a PO or CRMA box

You can do these things, and we'll talk about where you can learn more!
But all is not lost if it's too late or if you don't want to do them.

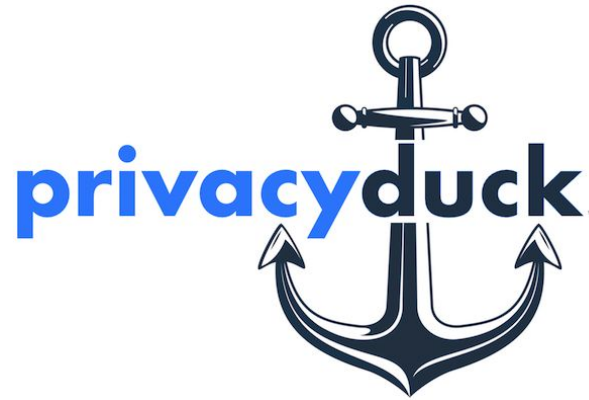


You can make it harder to find your address by removing it from data aggregator sites!

- Spokeo (remove listing [here](#))
- Whitepages (remove listing [here](#))
- For instructions on removing yourself from additional people listing sites, go to these guides:
 - Abine's <https://www.abine.com/optouts.php>
 - Michael Bazzell's Extreme Privacy [Opt Out Workbook](#)

Remove Your Home Address/Phone Number

- Consider a paid service like [DeleteMe](#) or [PrivacyDuck](#) that can remove this information for you
- These services cost \$150+/year and will take a few weeks to get your information removed



Treat your personal phone number like a password

Remember SIM swapping? It's lot harder to do for a VOIP number (like Google Voice).

- If your phone number is already widely shared:
 - Consider porting your phone number to Google Voice.
- If your phone number isn't widely shared:
 - Get a VOIP number to use publicly. This could be a Google Voice number or a paid VOIP service like Twilio, Grasshopper, or Sudo.
- Contact your phone company, and ensure they require a password or pin to complete porting requests.



Protection through state programs

- Many states have Address Confidentiality Programs or laws allowing certain people to have their addresses removed from the voter lists
- These laws and who can qualify vary drastically from state to state
 - Ex: In Oklahoma, district attorneys, assistant district attorneys, and judges all qualify
- If you've had legal issues with domestic violence or stalking before, you likely qualify.

Want to learn more about extreme privacy techniques?

[Privacy, Security, & OSINT Show](#): Podcast by Michael Bazzell

Pros: Really thorough podcast & materials about privacy. He's a leading expert on the topic.

Super dense, technical, and extreme tactics – your threat model may not require such extensive work.

Cons: He rarely has women on his show.

Key takeaway:

Identify what personal information you want to stay private, and take precautions to keep it that way.

Make your personal social media accounts as private as possible.

If you haven't already, **create a separation** between your professional social media accounts and your personal social media accounts.

Seek guidance from city/state resources about rules and public information laws that may apply to your professional social media accounts!

You may also need separation between your campaign social media accounts and your elected official social media accounts.

Did personal social media accounts show up in your Google search of yourself?

- Make sure your personal social media accounts aren't findable from Google
 - Almost every social platform has a way to hide your profile from search results.
- You may want to consider making sure your professional social media accounts *are* discoverable through Google searches, so that result pops up high on the results page.

Were any of your locations visible?

- Be mindful and careful with location sharing when you share posts
 - Could someone identify part of your routine (i.e. a coffee shop you frequent)?
 - Could someone identify where you live?
 - Your neighborhood?
- Consider saving photos to post later
 - Once you're home from vacation
 - Once you've left the event

Did you see an option to send yourself a message?

- Limit who can contact you on your personal social media
 - Consider only allowing friends or connections to send you messages
- Again, for professional accounts, seek guidance about your city, state, and applicable federal policies before blocking direct messages

Platform Specific Privacy instructions

Facebook	https://digitaldefensefund.org/2019/05/03/privacy-and-security-on-facebook/
LinkedIn	https://digitaldefensefund.org/2019/05/20/privacy-and-security-on-linkedin/
Twitter	https://digitaldefensefund.org/2019/05/03/privacy-and-security-on-twitter/
Instagram	https://digitaldefensefund.org/2019/05/03/privacy-and-security-on-instagram/
TikTok	https://www.tiktok.com/safety/resources/safety-videos

You don't have to delete social media!

In fact, claiming accounts on all the social media sites can help you prevent or take action against impersonation!

Are you eligible for verified accounts for your official legislator accounts on platforms like Twitter or Instagram?

Verifying your accounts can ensure more expedient response to impersonation issues, and other support requests.

Key takeaway:

Be mindful in your use of social media, and familiarize yourself with the privacy settings available.

Despite your best efforts, someone is
harassing you online.

What do you do next?

Doxxing & Harassment Response

Doxxing Response Steps

1. Make a physical safety plan
2. Tell your friends & family
3. Document before you delete
4. Block the bad actors
5. Lawyer up
6. Self care

Physical safety first!

From Michelle Ferrier, founder of Trollbusters:

“All the threats are “real”. Anytime someone makes a threat that intimidates or scares you is real, and has a real emotional and psychological impact.”

Suggestions for physical safety from Michelle Ferrier (Trollbusters)

Solve for the physical safe space.

This could mean:

- Telling neighbors & friends so they can keep an eye out.
- Installing a home security system.
- Having a safe place you can go to if necessary (a hotel or a friend with a spare room, for example).
- Asking a friend to come stay with you.

Is the threat actionable?

Treat all death threats as actionable.

Police sometimes use these questions to evaluate the severity of the threat:

- Is the threat specific?
 - time, place, names
- Do you know the person making the threat?
- Do they have a history of escalating violent behavior?
- Has it migrated from online to offline?
 - For example, are you getting packages or are people showing up where you live/work/travel?

Document before deleting comments

Resist the urge to delete material that is potentially crossing the line into threats. You will likely need to show documentation of these messages if you choose to escalate any actions to a police report or other legal response, contribute them to a database of bad actors, or to report them to the platform. Regardless of whether you can rely on the police for assistance, documenting evidence is important!

Be sure to screenshot & download & document as much as possible before deleting these kinds of comments (or before the bad actor deletes their abusive comment).

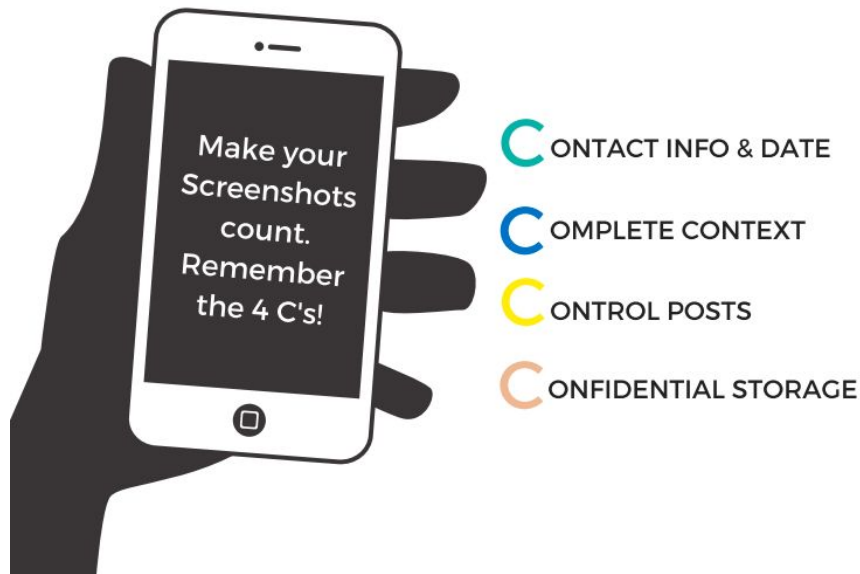


Delegate, delegate, delegate

Especially if you are dealing with harassment, can you delegate managing the messages and comments on your professional social media accounts?

Share the following resources on documenting threats to make sure the person you delegate can confidently save evidence as they manage your account.

More instructions on collecting evidence:



<http://www.endtechabuse.org/>

Documentation proves escalation.

Remember escalation paths?

Documentation helps show that one person has made increasingly serious threats, which can help you know when to take action, loop in law enforcement or community safety groups, etc.

Tell your friends & family

- Let them know you are being targeted
- Tell them to watch out for fake or imposter communications from you and decide on a reliable way to communicate (Signal, phone calls, etc)
- Tell family and friends to be on high alert for potential scams, phishing emails, or threats and to document any scams or threats they receive
- If you can safely tell your neighbors, landlord, or building manager/security, enlist their help to keep an eye out for your safety
- If you have children:
 - Check in with your children's school around their existing campus security procedures.

Note: Give friends & colleagues ways to help!

Some of these tasks can be overwhelming or just downright scary for the person experiencing a doxxing threat or attack.

- Share these resources with them and ask them to protect themselves as well.
- Delegate: Ask someone to help document harassing emails, tweets, comments, etc
- Ask a friend to be the main contact for people outside your core group, so you can focus on yourself & your loved ones
- Have a colleague look up the harassment & reporting rules for social media accounts and cross reference with public information requirements

Block, block, block!

(on personal accounts only - check before blocking on professional accounts!!)



Block or report a harasser:

Facebook	https://www.facebook.com/help/290450221052800/
Twitter	https://help.twitter.com/en/using-twitter/blocking-and-unblocking-accounts
Instagram	https://help.instagram.com/454180787965921
Snapchat	https://www.wikihow.com/Block-Someone-on-Snapchat
LinkedIn	https://www.linkedin.com/help/linkedin/answer/47081/blocking-or-unblocking-a-member?lang=en
Gmail	https://support.google.com/mail/answer/8151?co=GENIE.Platform%3DDesktop&hl=en

Lawyer Up!

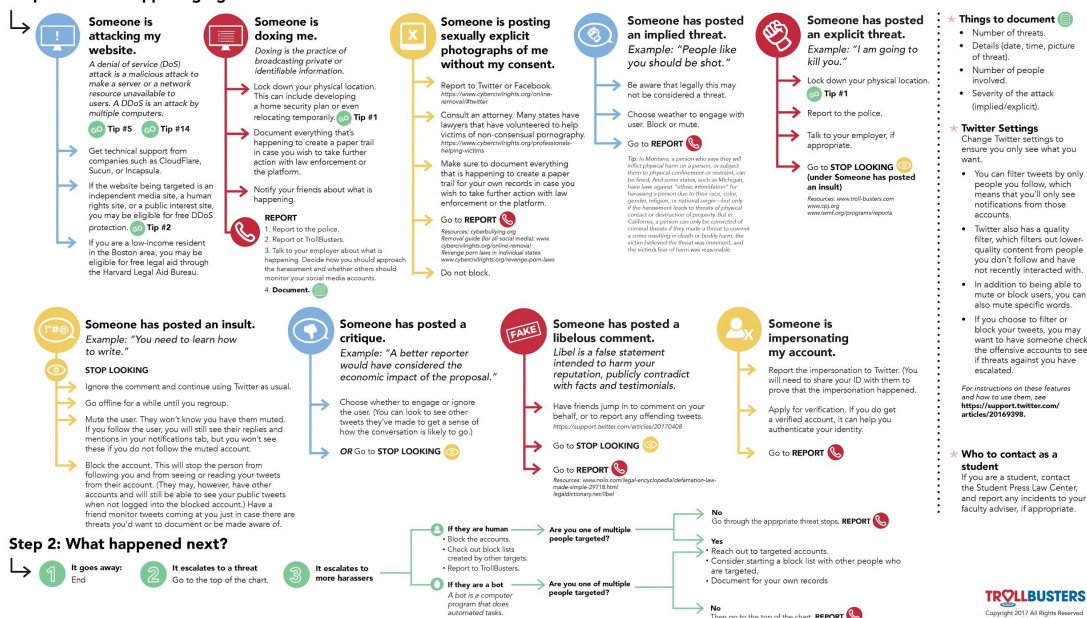
- Ask your state/county/municipal legal team if they can assist in these cases.
 - If not, find a private lawyer with whom you can establish a relationship now, before you need one.
- The legal team can also review comments you aren't sure about.
- It helps often to ask a teammate or friend to go through these for you to ensure you don't have to deal with abuse. Make sure your lawyer/legal team know who that person is.

Bookmark the Trollbusters Flowchart

ARE YOU BEING HARASSED ONLINE?

TrollBusters provides online pest control for writers, journalists and publishers. Report to www.troll-busters.com. If you are not a journalist, check out our Resources for more tips and information. [GO](#)

Step 1: What is happening right now?



TROLLBUSTERS


Copyright 2017 All Rights Reserved
Report to troll-busters.com

<https://yoursosteam.wordpress.com/what-to-do-infographic/>



Someone is doxing me.

Doxing is the practice of broadcasting private or identifiable information.

Lock down your physical location. This can include developing a home security plan or even relocating temporarily.  **Tip #1**

Document everything that's happening to create a paper trail in case you wish to take further action with law enforcement or the platform.

Notify your friends about what is happening.



REPORT

1. Report to the police.
2. Report to TrollBusters.
3. Talk to your employer about what is happening. Decide how you should approach the harassment and whether others should monitor your social media accounts.
4. **Document.** 

Self care & community care

From Michelle Ferrier, founder of Trollbusters:

“All the threats are “real”. Anytime someone makes a threat that intimidates or scares you is real, and has a real emotional and psychological impact.”

Trust Your Gut - Extreme Messages

Legislators' offices often receive extreme communications that don't cross the line into "threat" but still may give you pause.

- Make a log of these communications, a timeline with dates, key phrases, and whether the sender is previously prone to high volumes of calls or letters.

Ensure your coworkers/staff know about these frequent messages, even if you feel silly bringing it up. They may have additional context, or can help you keep an eye out for escalation.

We often have the urge to "be polite" or "not be a bother" but you do not have to deal with disturbing calls or messages alone.

Final Note

It might go without saying, but we like to remind everyone to **trust their gut about an interaction or message feeling "off."** Your instinct built from your expertise and experiences with your work, your space, your community, is one of the most irreplaceable assets in best security practices.

What has worked for you, both for handling threats and taking care of yourself? Please share in the chat!



Key takeaways:

- Do whatever you can to avoid password reuse and weak passwords!
- Turn on two-factor authentication
- Take precautions to keep private information private
- Be mindful in your use of (personal) social media
- Make safety plans before you need them

Questions?

Resources

- [Speak Up & Stay Safe\(r\): A Guide to Protecting Yourself From Online Harassment](#)
- [A DIY Guide to Feminist Cybersecurity](#)
- [Big Ass Data Broker Opt-Out List](#)
- [OnlineSOS](#)
- [Cybersecurity Campaign Playbook](#)
 - By the Belfer Center [Defending Digital Democracy Project](#) (D3P)

Connect with local digital security experts

Find a helpdesk near you:

Chicago area: [Chi Hack Night Helpdesk](#)

Progressive campaigns/elected officials: [Ragtag Help Desk](#)

Hire the experts:

[Security Positive](#): security services, specializing in gender-based harassment and campaigns of all sizes

[C.A. Goldberg PLLC](#): Victim's Rights Law Firm specializing in online harassment

Questions about this presentation?

Amanda Bennett

amanda@digitaldefensefund.org

Nicole Lopez

nicole@digitaldefensefund.org

