Mesa County LIBRARIES

Tech Table @ Central: every Tuesday from 12pm – 2pm

mesacountylibraries.org
(970) 243-4442

Introduction to Digital Privacy and Security

Learning Objectives:

- Know how to use threat modeling to assess potential risks in their digital privacy and security.
- Learn specific tools/strategies they can implement as part of a security plan.

Disclaimer

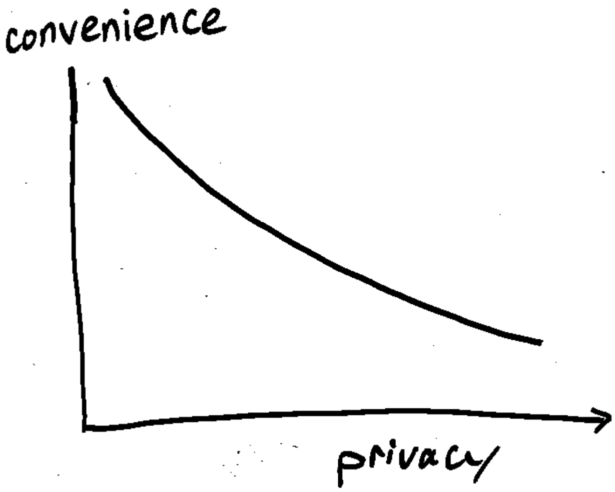
This lesson will not cover government surveillance conspiracy theories or how to evade paying taxes to the IRS; that is illegal.

1. Assessing Your Risks

- Everyone does risk assessment (aka threat modeling) in their everyday life.
    - For example, what are things you think about when….
        - You are deciding on which route to take when going for a walk?
        - You are deciding where you're going to sit on the bus?
        - You are deciding where to sleep when you don't have a bed to go to?
- The task during this class is to apply that kind of thinking to your digital privacy and security.

Risk assessment starts with five questions:

- What do I want to protect?
    - This can be anything important to you - from your physical safety to your emails. Often called "assets" in threat modeling.
- Who do I want to protect it from?
    - Often referred to as "adversaries" in threat modeling. These are the people who are either actively trying to hurt you (an ex-partner, a robber!), or who could accidentally do you harm (a clerk who leaves your private information out on a public desk).
- What are the consequences if I fail?
    - What will happen if you don't protect your assets? How bad will the impact be? Think about the difference between losing five dollars and losing all your identification.
- How likely are these consequences?
    - This helps us judge how much effort to put into things - a bear could break into the library and take my backpack, but it's not very likely. The chances of someone stealing it if I leave it on a bench in a park? Much higher.
- How much trouble am I willing to go through to try to prevent potential consequences?
    - In the end, we all have to make a call on the trade-off between safety/privacy and convenience. We'll all have different answers about that.



When it comes to online privacy, there's always a trade off between convenience and privacy.

With more convenience, you often give up more privacy. There is no perfect option for security. Not everyone has the same priorities, concerns, or access to resources. Your risk assessment will allow you to plan the right strategy for you, balancing convenience, cost, and privacy.

Why is this topic important?

Our “real” lives are so entangled with our digital lives that we need to take the time to do risk assessment. Understanding your risks and using tools to reduce those risks can help!

2. Passwords

Chances are you have multiple online accounts. It’s probably fair to say that you have a lot of passwords to keep track of (or maybe you only have one) both of which can lead to bad habits when it comes to password security hygiene.

What makes a strong password?

- Not re-using the same password for other accounts! Please don't do this! Reusing passwords means that if someone gets into one account, they can get into any other account you have.
- Lots of characters (8 characters *minimum*). Length is the single most important thing to keep your password safe from "brute force" attacks - where someone tries to guess your password.
- Mix of character types (upper and lower case letters, numbers, and special characters) is great.

Tips

- Use a pass*phrase* – a series of three or four words stuck together. This makes it easier to make long passwords and a lot easier to remember.
- Have a base password that’s strong (like a passphrase), and then add to it for each additional account.
  - Example:
    - Base: vampirelemoncar
    - Facebook: vampirelemoncarFB!
    - Gmail: vampirelemoncar2GMAIL

Activity

Go to www.security.org/how-secure-is-my-password to test a variant of one of your passwords (*DO NOT USE YOUR ACTUAL PASSWORD*). How long would it take a computer to crack your password?

Now try a passphrase, such as one of the examples above. How long would it take a computer to crack the passphrase?

3. Password managers

It's not good practice to reuse the same password for multiple accounts, yet many people do so because it's too hard to create unique passwords for each account. If you fall in this boat, you may consider using a password manager.

Digital password managers

- Use a password manager like Bitwarden, mSecure or Keepass (**these do cost money!**)

Analog password managers:

- If you're going to write your passwords down, make sure that you:
  - Keep everything in one place (it's easier to lose track of a bunch of slips of paper than a notebook)!
  - Keep it safe! Put it in a plastic bag to keep it safe from water damage, and always put it away in the same place.
  - Keep it "encrypted"! "Encryption" is when something is protected by a code so other people can't read or use it. You can simply encrypt your password notebook by picking a secret word that you stick on every password, *but don't write it down*.
    - For example: you choose the secret word "elephant". In your notebook, you write down the password to your email as "hairbrushpajamas". But if someone takes your notebook and tries the password, they won't be able to get in because your real password is "elephanthairbrushpajamas".

3. Browsers

Private browsing

- Most browsers have a feature that prevents information such as search history, passwords, and cookies from being stored locally on your computer. This does not mean you are anonymous; you can still be tracked via your IP address – which is your computer's and/or browser's specific "phone number".
- Google Chrome's privacy feature is called "Incognito"
- Mozilla Firefox's privacy feature is called "Private Browsing"

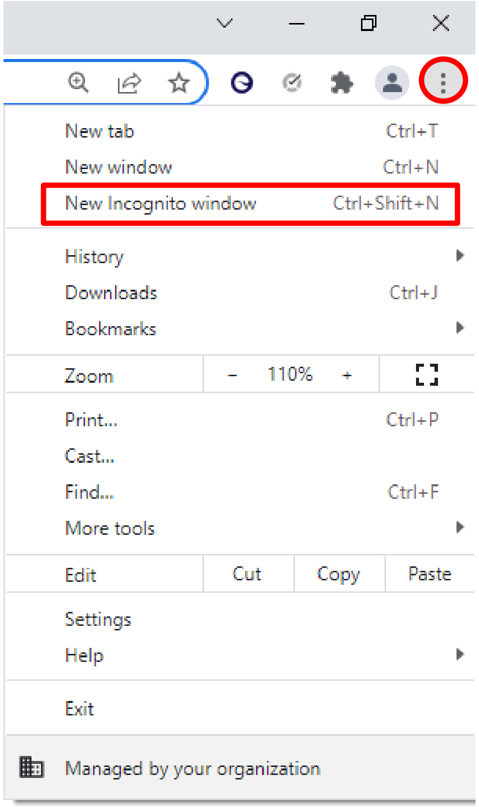
Activity

Turn on the privacy feature on either Google Chrome or Mozilla Firefox.

Google Chrome

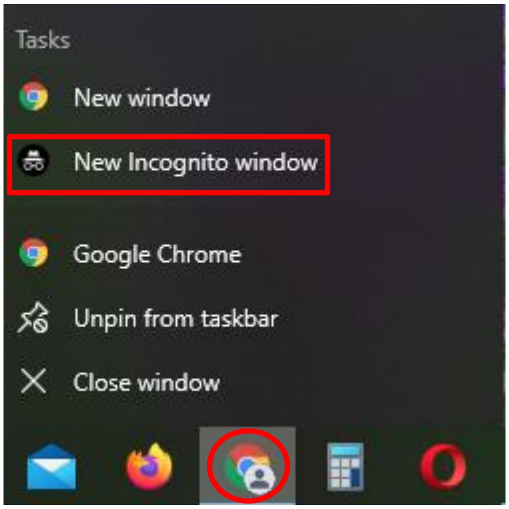
Option 1

- Open a browser window.
- In the top right corner, under the “X”, there are three dots. This is a menu. Click on these dots.
- Click the third option on the menu, “New Incognito window”
- This will open up a new private browsing window.

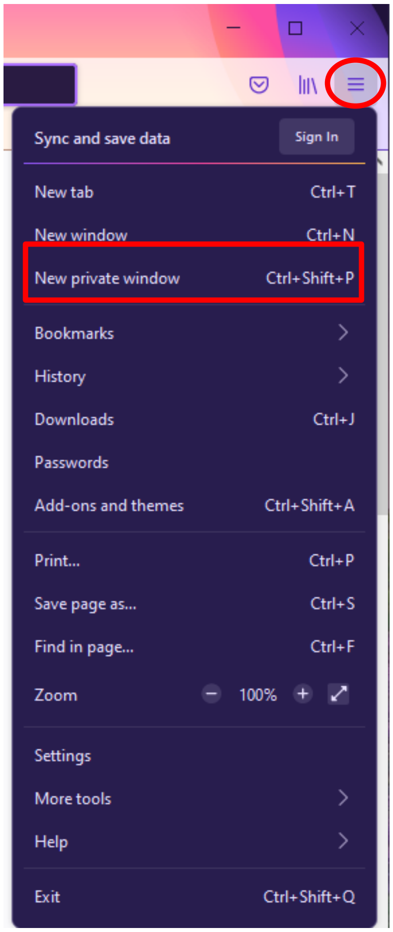


Option 2

- Right click the Google Chrome logo on your desktop.
- Click on the “New Incognito window” option to open a new private browsing window.



Mozilla Firefox

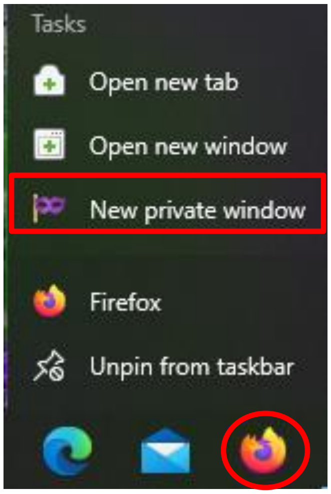


Option 1

- Open a browser window.
- In the top right corner, under the "X", there are three horizontal lines. This is a menu. Click on these lines.
- Click on the third option, "New private window"
- This will open up a new private browsing window.

Option 2

- Right click the Mozilla Firefox logo on your desktop.
- Click on the "New private window" option to open a new private browsing window.

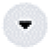


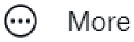
4. Social Media

It is impossible to maintain complete privacy when you're using private companies to connect with people online. The best way to maintain your privacy on social media **is to not use social media**. For a lot of people, though, social media may be their only way to communicate with friends and family. So keep some basic things in mind:

- Set a strong password to your accounts, and use different passwords for each of them.
- Watch out for geotagging! That's when location information is attached to each post you make. Many apps have ways to turn this off.
- Many sites have apps that will ask for access to your account–avoid using them. These often aren't written by the platform, they're made by some random person who you're now sharing all your personal information with, and who may not be a good enough programmer to protect the data you're sharing with them.
  - Games on Facebook that ask to use your Facebook information to login or ask you to create an account are an example.

<u>How to check your privacy settings on popular social networking sites</u>

- Facebook
  - Open Facebook.
  - Click the downward arrow at the top right. 
  - Click "Settings & privacy"
  - Click "Privacy Shortcuts"
    - From there, you can manage your location settings, turn on two-factor authentication, review your ad preferences, and more.

- Twitter
  - Open Twitter.
  - Click "More" on the left. 

  - Click "Settings and privacy"
    - From there, you can manage what information you allow others on Twitter to see, manage your ad preferences, manage your data sharing preferences, and more.

- Instagram
  - Open Instagram.
  - Click your profile picture on the top right.
  - Click "Settings"
  - Click "Privacy and Security"
    - From there you can make your account private, turn on two factor authentication, and more.

5. Data Breaches

A data breach is when information is accessed without authorization, and can harm businesses and consumers. Oftentimes, bad actors are interested in stealing that data with the intent to sell it. How do you know if your personal data has been compromised, and what can you do to mitigate this?

Activity

- Go to haveibeenpwned.com
- Type in your email address.
  - There's a decent chance that if you've had your email address for a long time and used it to create online accounts, your email has been compromised at some point.

What should you do if you think your email may have been compromised?

- Change your passwords
- Turn on two factor authentication (also referred to as 2FA). This adds another layer of security by requiring another step to login, such as security questions or a login code.
- Depending on the type of breach, you may want to contact your bank to freeze your credit score. This stops people from applying for new credit cards in your name.
- Tell your "trust circle" what happened. This is your close group of friends and relatives. It puts them on the lookout for any unusual phone calls or emails from scammers.

6. More resources:

- Visit the Internet Safety subject guide on the library's website for more resources to help you stay safe online.

Material for this class was borrowed from Denver Public Library's Digital Privacy and Security technology class.