Steve Hall - Oct/Nov 2025

Protecting Your Digital Life

Click with Confidence

Being a security expert is hard. In fact, I even wonder if someone can ever attain that title…”security expert”. Every type of security is hard. You want to secure a door, you put a lock on it. Then discover someone can just insert a credit card to unlock it. So you put a better lock on the door, and now someone just removes the hinges. Physical security is difficult, but at least someone has to actually be physically present at the location in order to try to break in.
Digital security has a different set of rules. With devices connected to the internet 24x7, an intruder doesn’t have to be in the same room as the device. They can be anywhere in the world. If they are successful at opening the right digital door, they might not just get access to one person’s belongings, but thousands or millions of people’s digital belongings. This makes digital theft much more appealing to bad actors, even state-sponsored bad actors, who have financial backing and the resources and personnel to cause a lot of problems for people.

In 2024, Adults over 60 lost $4.8B to tech support fraud, phishing, and identity theft.

For the most part, there isn’t someone across the world singling you out. That is, they aren’t usually targeting Guy Beaumont directly. The tactics and approaches they use are typically done at scale, meaning they are targeting 1000s of people simultaneously with the same approach. When you get that text message “Hey, what’s up”. That’s not a person on the other end, it is a computer…sending 100s of these to 100s of numbers. If you respond, it will also most likely be a computer that responds to you, particularly now in the age of Artificial Intelligence where the attackers can use AI to try and coerce information from you.

In this course, we’ll cover some of the strategies hackers use, learn a little bit about the systems that help keep you safe, give you some of the steps to help you configure your devices, and help you understand how to keep your information safe.

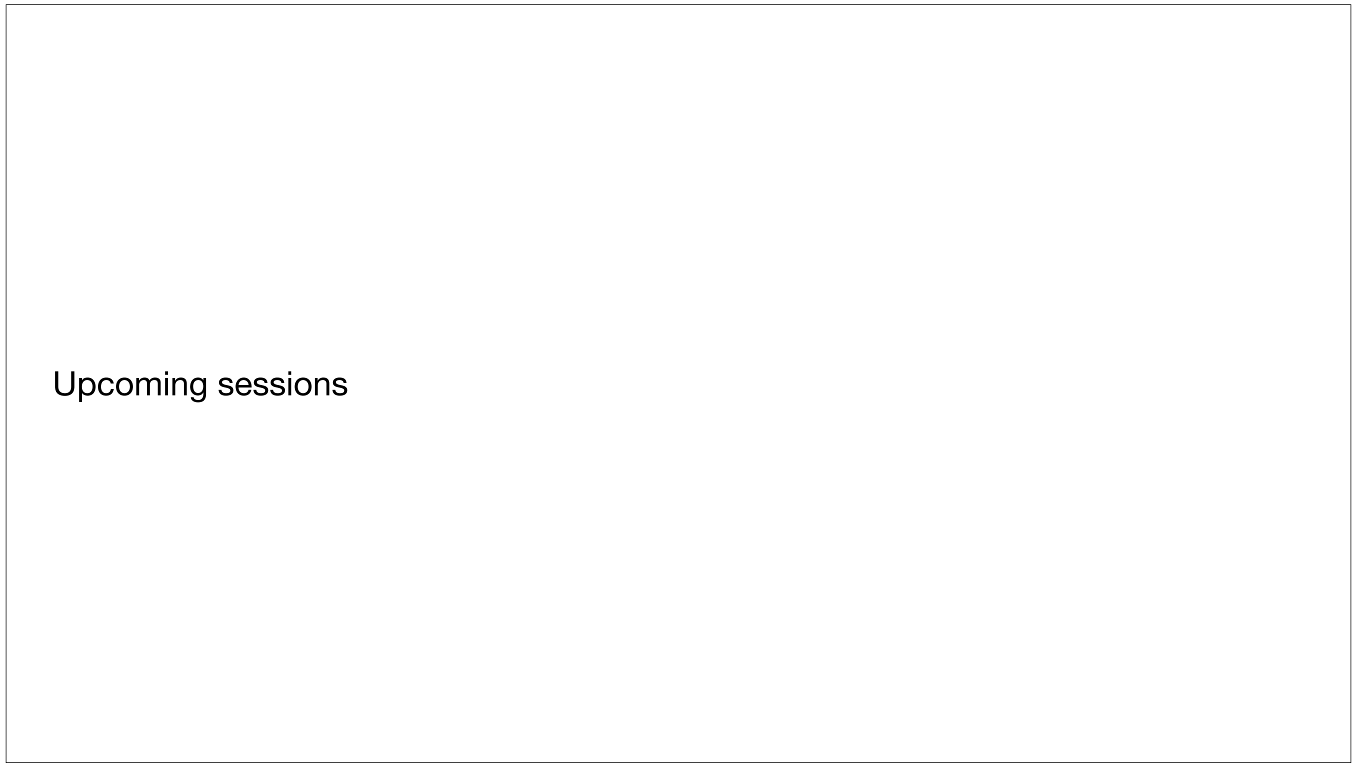
We will not be able to cover everything in this course. Would be like trying to teach the entire Roman history in a couple of days. Computer systems are complex. They are designed by different companies and individuals, so they do not all work the same, despite the many standards in place.

Why, if we have standards, don’t things operate the same? (XCKD)

Many of you might have been or currently are the go-to person for your friends and family for your particular expertise. If you’re a doctor, I’m sure you’ve had hundreds of people ask you about a rash, or if a bone looks broken or not. If you’re a lawyer, I’m sure you’ve been consulted numerous times about legal this and legal that. I’m a software engineer and I’m also someone who needs to find out how and why things work the way they do. If something isn’t working, I’ll figure out why, possibly taking it completely apart to do so.

So, a lot of people end up asking me for help when it comes to their computer issues. And I say computer in a very broad sense. Could be their PC or Mac. Might be their mobile device. Or software running on it. Or their email, internet, WiFi, router, printer, or any number of other devices that power on and connect to something.

The thing I’ve taken away from all of those sessions, is that, in general, these digital services and devices are way too difficult to use, are frustrating for users, and open up a lot of opportunities for things to go wrong…particularly with respect to protecting someone’s digital assets, accounts, and important files.



Upcoming sessions

Before we start, here’s a sneak peek into the rest of the schedule.

Next week we dive into some tools and ways to combat many of the potential risks we face each day.
The last two sessions are specific to devices and operating systems. You can attend the sessions that are relevant to you.

For the most part, they will be very similar, but if you bring your devices on those days we can attempt to get everyone familiar with the process that will help you from here on out.

Today, in the spirit of Halloween…we [click]

…We are going to go through many of the spooky attacks on our digital lives.

[ice breaker]
Go around room, introduce yourself, your favorite hobby, and “What was the first piece of technology you ever used that felt futuristic at the time?”

(Touch-tone phone, remote control)

I was visiting Microsoft's security operations center in Redmond, WA.

It was quite late, maybe 9 or 10PM in Seattle. They run 24-hours a day.

The center looks kind of like you would think. Huge monitors on the wall. Maps and dashboards displayed everywhere.

While we were there, this country (anyone?) started lighting up. It went from more or less dark to little lights everywhere on the map.
The person showing us around looked at it, and said, "Oh! It must be morning in Vietnam"

Why?

- Everyone turned on their PC (you left it off at night)
- Vietnam had one of the highest proliferations of pirated copies of Windows
- Windows copies were for the most part, full of malware and viruses
- Someone would copy a CD, which was probably already full of malware, maybe add a few of their own, and then sell it on the street.

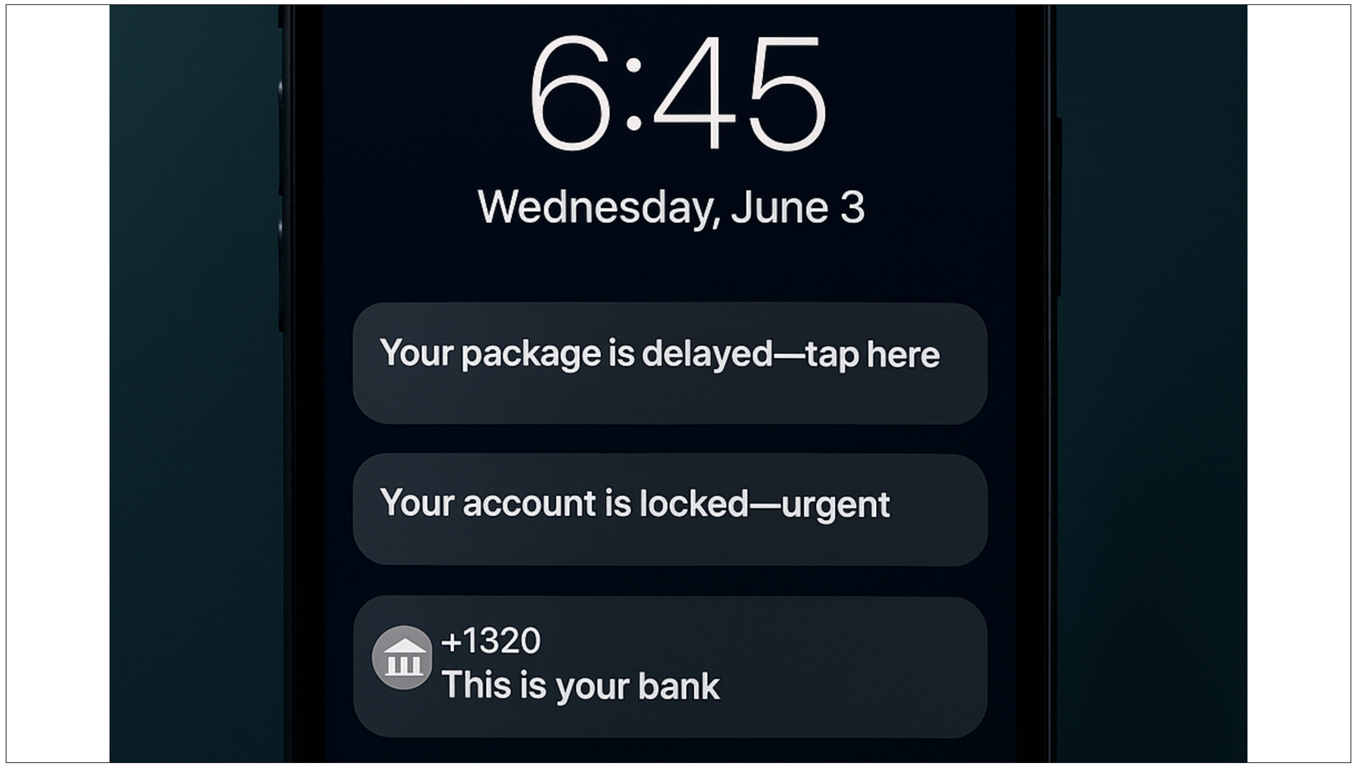
In a 2023/24 report, Microsoft details that its customers face 600 million attacks daily from cyber criminals and nation-state actors.
Companies, like Microsoft, Apple, Google, and others, have a critical role to play in reducing these bad actor's abilities to attack our computers and accounts. But, in truth, the surface area is just too large. There are too many opportunities for people to bypass security and attack our personal systems.

Which means, at the end of the day, it is up to each of us to protect our digital lives.

https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

So today, we're going to start by exploring some of the many ways, we get attacked across our digital footprint.

Let's walk through a "day in our lives."



Your package is delayed—tap here

Your account is locked—urgent

+1320
This is your bank

A text message represents urgency. People typically read text messages within 3 minutes.

Why and how do attackers use text messaging?

Why
Cheap - Legitimate business typically use A2P (Application to Person) messaging.
Doctor's office: Their appointment scheduling system sends reminders to people before their appointment. To do so, they interface with a messaging provider that sets up legitimate messaging channels to all of the mobile carriers. This costs money. Not much, but it does add up.

Using P2P (person to person) messaging, is much cheaper, but can be illegal. In this case, someone buys a bunch of mobile SIM cards and plugs them into their computer. They sell the ability to send messages for very little, because it costs them almost nothing.
You can buy a $15/month mobile plan and send unlimited messages.

Doing this also removes a revenue stream from mobile companies. They aren't making money on A2P messaging. They estimate that this costs the companies somewhere between 15-20% of their messaging revenue.

How
Like a lot of hacking, they are either trying to get information from you, or have you perform an action which gives them account information.

So you need to be very careful that the text message you respond to is someone you know.
You need to be very careful that the link in the message is something you should click.

Shortened URLs

One of the challenges here, is that URLs in the messages, even legitimate messages, are often shortened. This doesn't necessarily mean the link is harmful at all. But it does make it somewhat harder to know if the link is real or not.

Why Smart Speakers Are Security Risks?

Always Listening

The device is constantly monitoring for wake words (“Alexa,” “Hey Google”).
The device is supposed to only record after hearing the wake word, but mistakes can happen.
Conversations near the device could accidentally be recorded and uploaded.

Internet Connected

Direct gateway into your home network
If compromised, hackers could access other connected devices
Requires constant security updates that users may not install

Stores Personal Information someone else could ask

Shopping history and payment methods
Connected to your calendar, contacts, and email
Smart home controls (locks, cameras, thermostats)

My WiFi router from 8 years ago keeps on running. No issues.

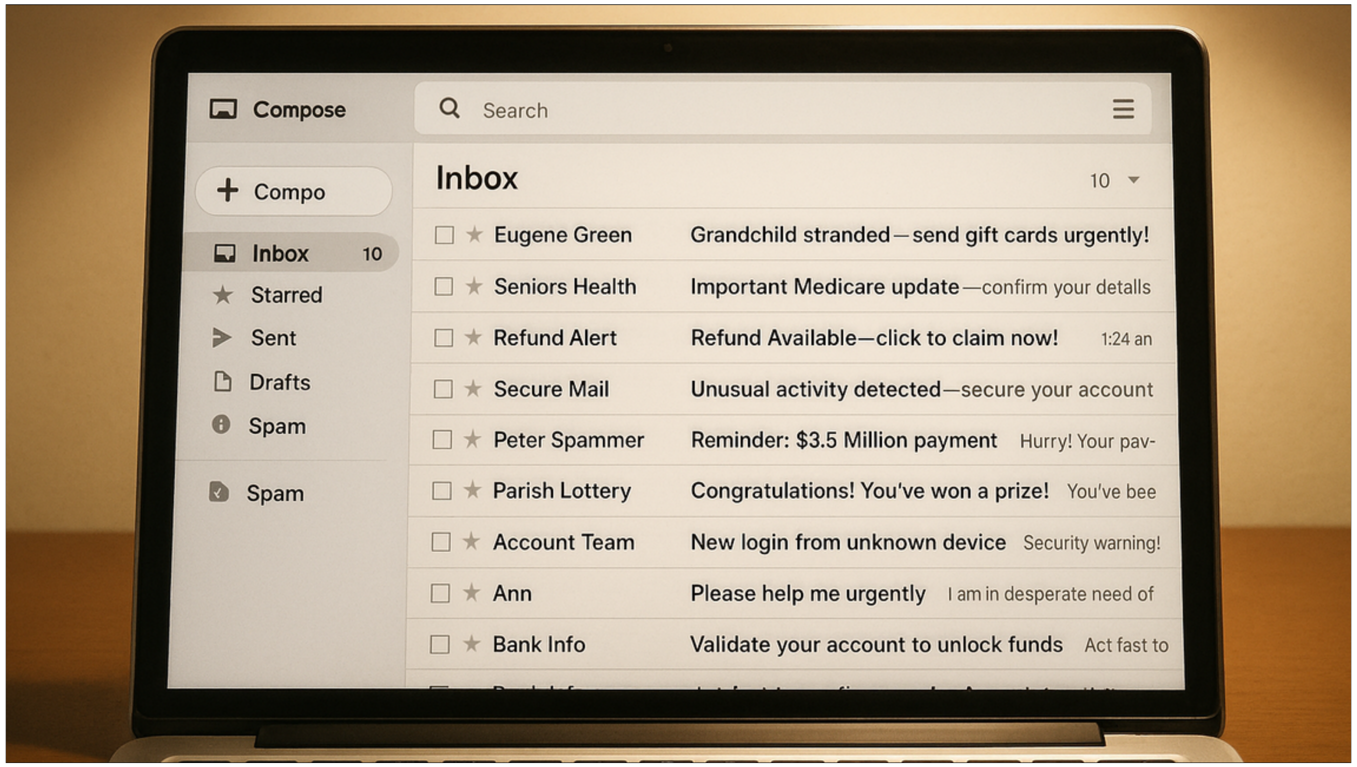
The Risks of Old WiFi Routers

Known Security Holes
Older routers have discovered weaknesses that hackers know how to exploit
Manufacturers stop providing security updates after 3-5 years
It's like continuing to use a lock after everyone knows where you hide the spare key

If your router is compromised, you are open to a tremendous amount of security risk. In a sense, anything you send or receive over the internet could be viewed by someone else.

- software updates requires you to login to router usually

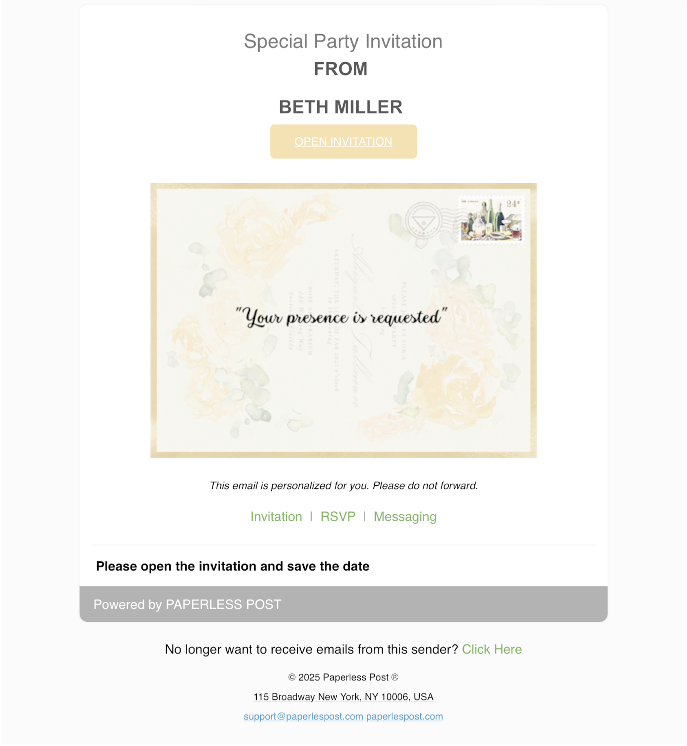
Outdated software is the #1 way viruses and scams get onto your device



Eugene Green	Grandchild stranded—send gift cards urgently!	
Seniors Health	Important Medicare update—confirm your detalls	
Refund Alert	Refund Available—click to claim now!	1:24 an
Secure Mail	Unusual activity detected—secure your account	
Peter Spammer	Reminder: $3.5 Million payment	Hurry! Your pav-
Parish Lottery	Congratulations! You've won a prize!	You've bee
Account Team	New login from unknown device	Security warning!
Ann	Please help me urgently	I am in desperate need of
Bank Info	Validate your account to unlock funds	Act fast to

Checking email, I see a couple of important updates I better look into.

What percent of your email is spam, malware or phishing attempts?



Special Party Invitation
FROM

BETH MILLER

OPEN INVITATION

This email is personalized for you. Please do not forward.

Invitation | RSVP | Messaging

Please open the invitation and save the date

Powered by PAPERLESS POST

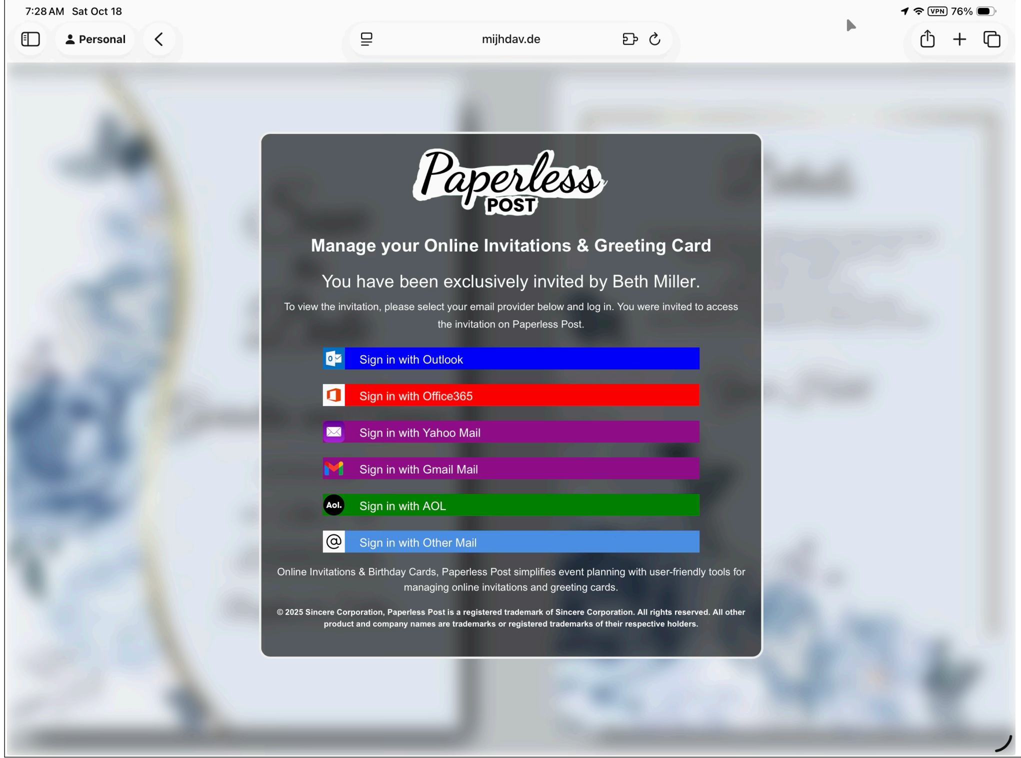
No longer want to receive emails from this sender? Click Here

© 2025 Paperless Post ®

115 Broadway New York, NY 10006, USA

support@paperlesspost.com paperlespost.com

What's wrong with this email?



Manage your Online Invitations & Greeting Card

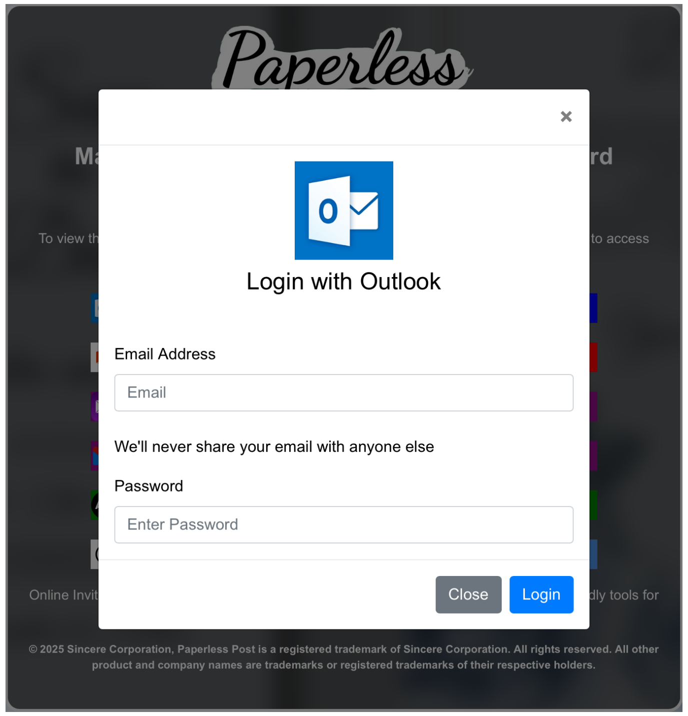
You have been exclusively invited by Beth Miller.

To view the invitation, please select your email provider below and log in. You were invited to access the invitation on Paperless Post.

Online Invitations & Birthday Cards, Paperless Post simplifies event planning with user-friendly tools for managing online invitations and greeting cards.

© 2025 Sincere Corporation, Paperless Post is a registered trademark of Sincere Corporation. All rights reserved. All other product and company names are trademarks or registered trademarks of their respective holders.

What's wrong with this web page?



Paperless

Login with Outlook

Email Address

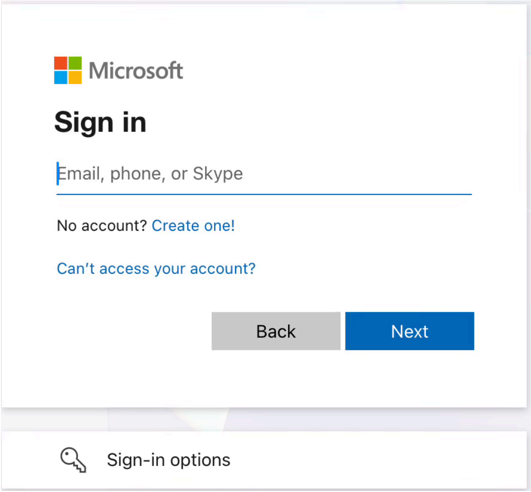
Email

We'll never share your email with anyone else

Password

Enter Password

© 2025 Sincere Corporation, Paperless Post is a registered trademark of Sincere Corporation. All rights reserved. All other product and company names are trademarks or registered trademarks of their respective holders.



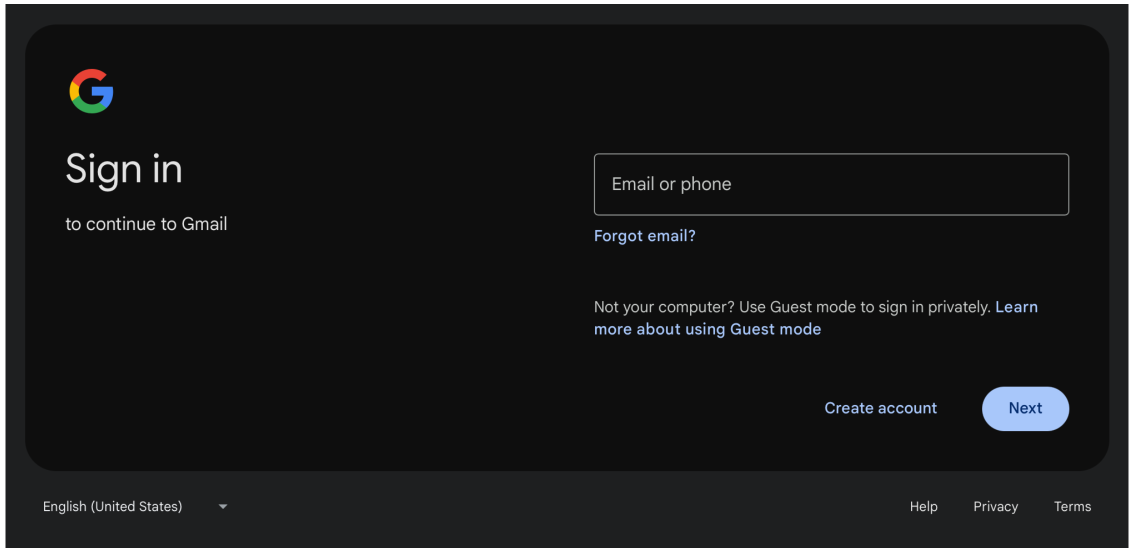
Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?



Sign in

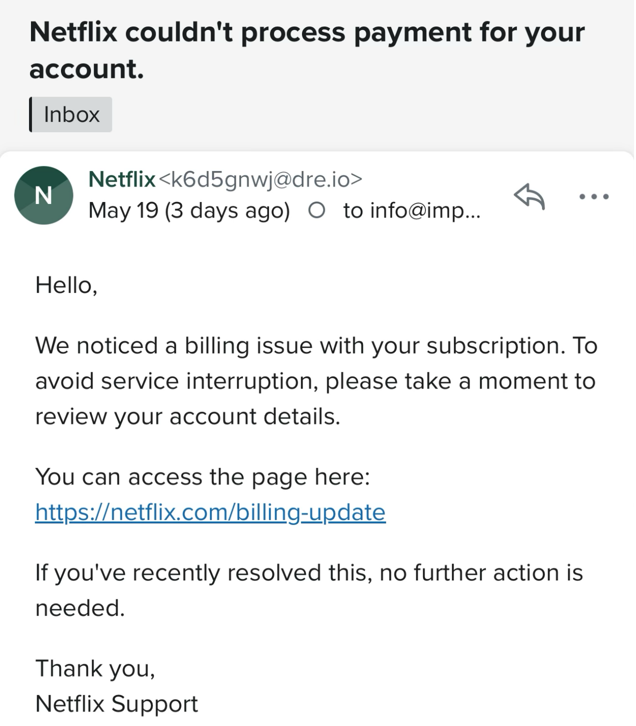
to continue to Gmail

Email or phone

Forgot email?

Not your computer? Use Guest mode to sign in privately. Learn more about using Guest mode

Another phishing example



Netflix couldn't process payment for your account.

Netflix<k6d5gnwj@dre.io>

May 19 (3 days ago) ○ to info@imp...

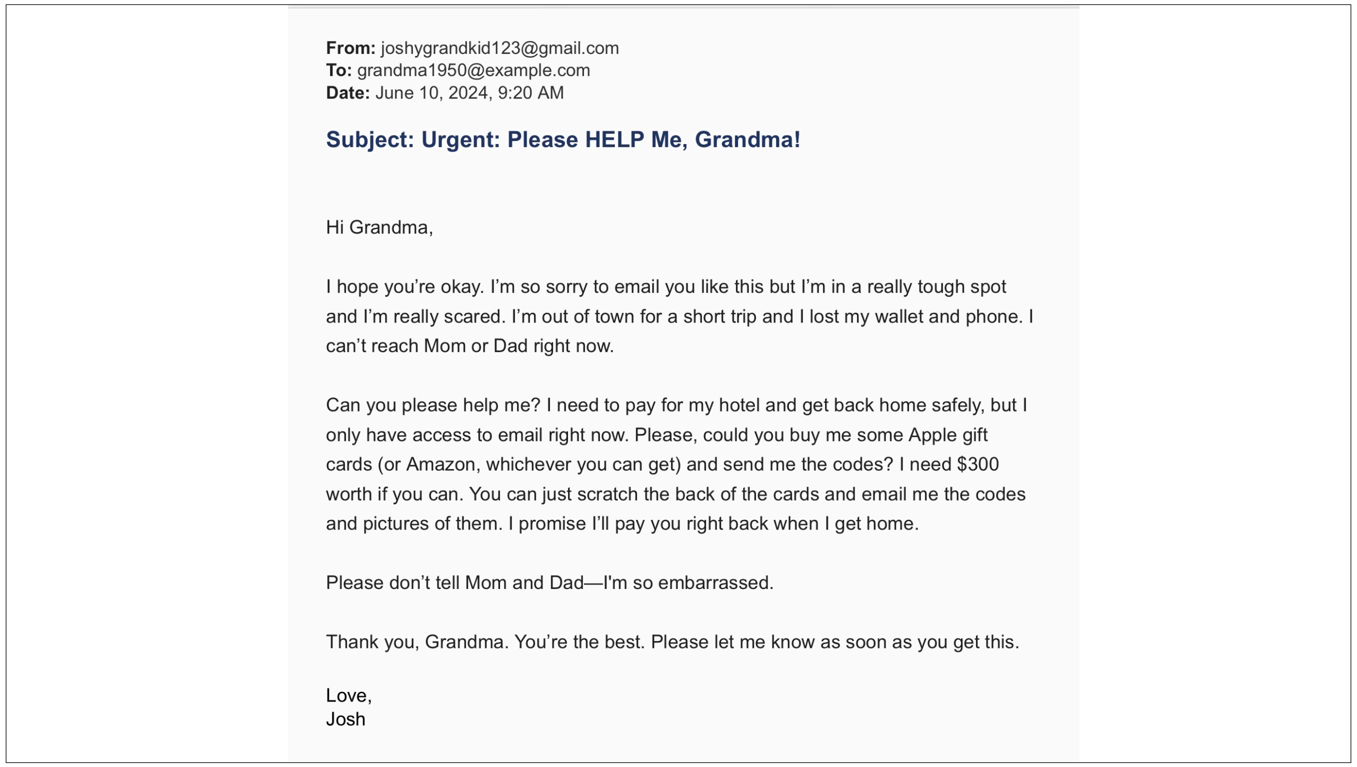
Hello,

We noticed a billing issue with your subscription. To avoid service interruption, please take a moment to review your account details.

You can access the page here: https://netflix.com/billing-update

If you've recently resolved this, no further action is needed.

Thank you,
Netflix Support



From: joshygrandkid123@gmail.com
To: grandma1950@example.com
Date: June 10, 2024, 9:20 AM

Subject: Urgent: Please HELP Me, Grandma!

Hi Grandma,

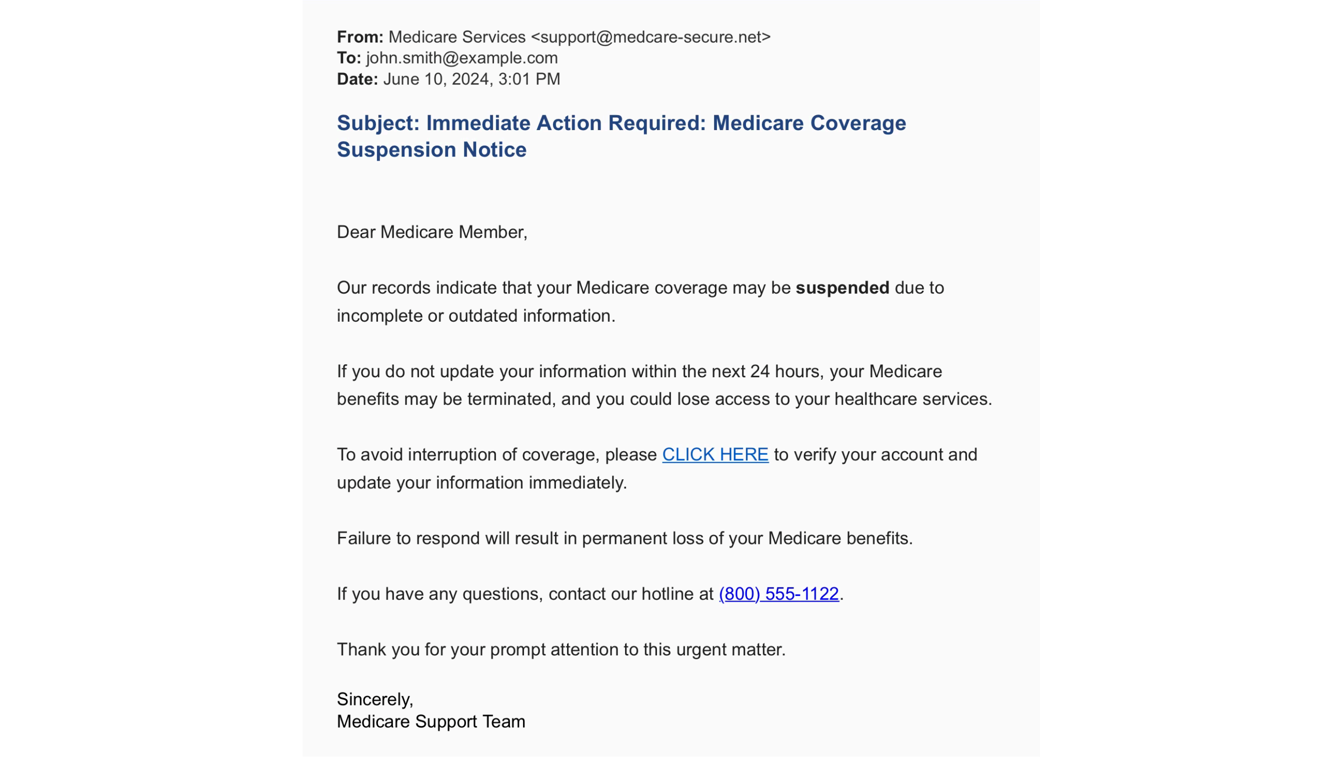
I hope you're okay. I'm so sorry to email you like this but I'm in a really tough spot and I'm really scared. I'm out of town for a short trip and I lost my wallet and phone. I can't reach Mom or Dad right now.

Can you please help me? I need to pay for my hotel and get back home safely, but I only have access to email right now. Please, could you buy me some Apple gift cards (or Amazon, whichever you can get) and send me the codes? I need $300 worth if you can. You can just scratch the back of the cards and email me the codes and pictures of them. I promise I'll pay you right back when I get home.

Please don't tell Mom and Dad—I'm so embarrassed.

Thank you, Grandma. You're the best. Please let me know as soon as you get this.

Love,
Josh



From: Medicare Services <support@medcare-secure.net>
To: john.smith@example.com
Date: June 10, 2024, 3:01 PM

Subject: Immediate Action Required: Medicare Coverage Suspension Notice

Dear Medicare Member,

Our records indicate that your Medicare coverage may be **suspended** due to incomplete or outdated information.

If you do not update your information within the next 24 hours, your Medicare benefits may be terminated, and you could lose access to your healthcare services.

To avoid interruption of coverage, please CLICK HERE to verify your account and update your information immediately.

Failure to respond will result in permanent loss of your Medicare benefits.

If you have any questions, contact our hotline at (800) 555-1122.

Thank you for your prompt attention to this urgent matter.

Sincerely,
Medicare Support Team

How do you know?

When you receive a notification like this, don’t click the links. Instead, login through the main web page for Medicare. If you have a notification, it will be there, in the inbox.

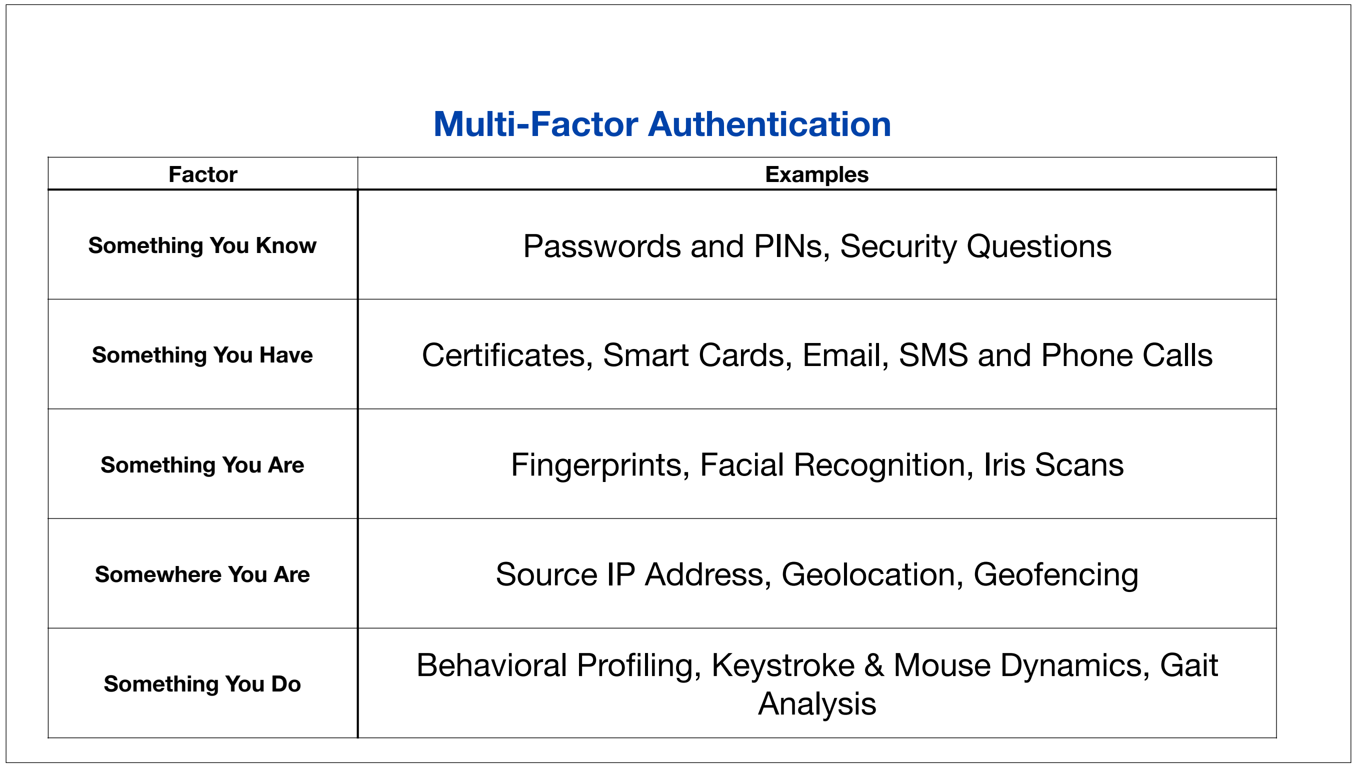
I would take a guess that at some time in our life, we’ve all encountered a website that put up a message like this, or one that you couldn’t close…it just kept opening window after window?

Your web browser will not tell you if you have a virus. It doesn’t know.
It can’t tell you if your low on disk space…it doesn’t know.
It can’t tell you if you memory ball bearings require grease…it doesn’t know!

Browsers run in a sandbox on your computer. It’s a Secure Enclave that prevents the browser from doing all but specific actions on your computer. And anything it wants to do that is extra, it must ask permission.

- Use your camera?
- Use your location?
- Use your microphone?

Sometimes knowing what a piece of software can and can’t do can help you determine if a threat is real or not.



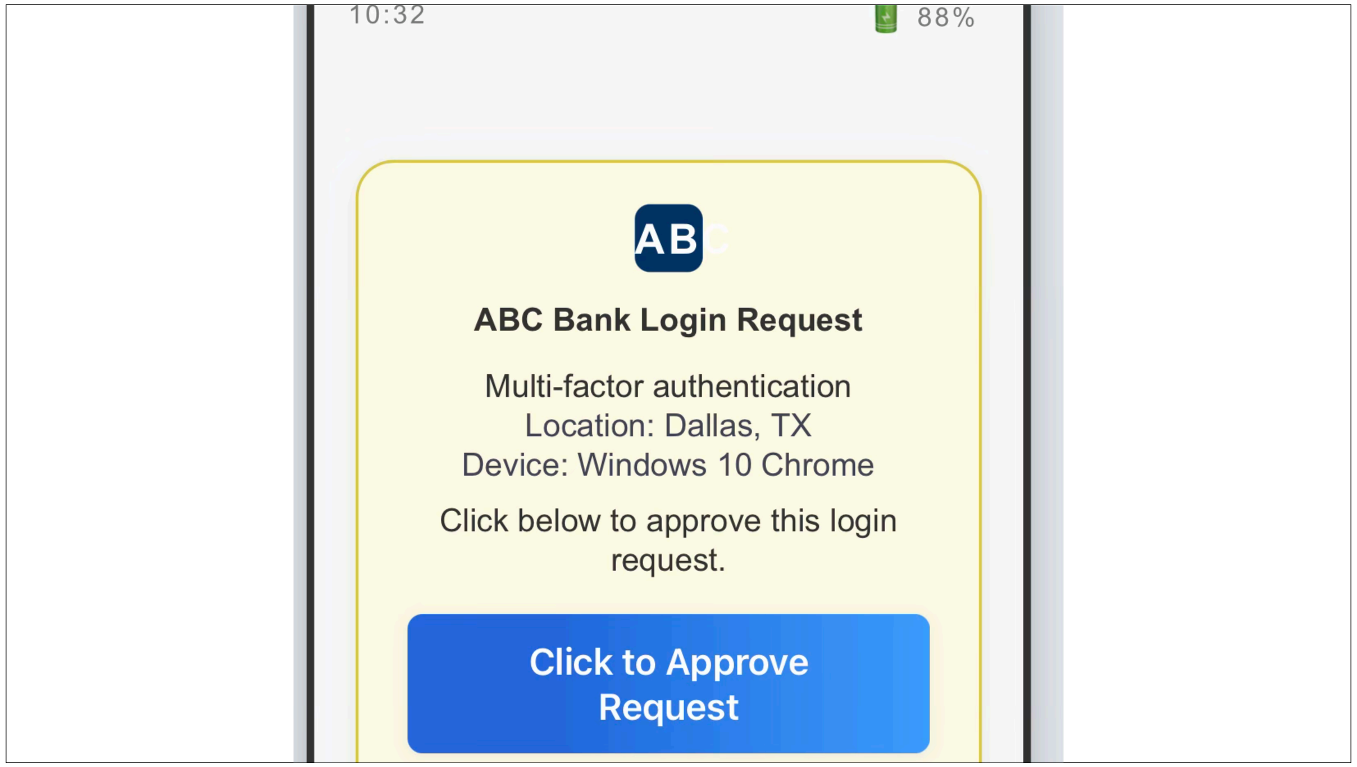
Multi-Factor Authentication

Factor	Examples
Something You Know	Passwords and PINs, Security Questions
Something You Have	Certificates, Smart Cards, Email, SMS and Phone Calls
Something You Are	Fingerprints, Facial Recognition, Iris Scans
Somewhere You Are	Source IP Address, Geolocation, Geofencing
Something You Do	Behavioral Profiling, Keystroke & Mouse Dynamics, Gait Analysis

How many of you are familiar with MFA?

MFA is a way of further securing your account beyond just a username and password.

It uses a second, and sometimes more, way of ensuring you are who you say you are.



10:32 88%

ABC Bank Login Request

Multi-factor authentication
Location: Dallas, TX
Device: Windows 10 Chrome

Click below to approve this login request.

Because MFA is more and more common, so are MFA scams.

We might get a message that looks like this. And you might think, oh! My bank needs me to approve this.

But it could be someone who knows your login and password, and tried to login in, and your bank send a MFA request through for you to approve it. If you do, then someone is in your account in seconds after your approval.

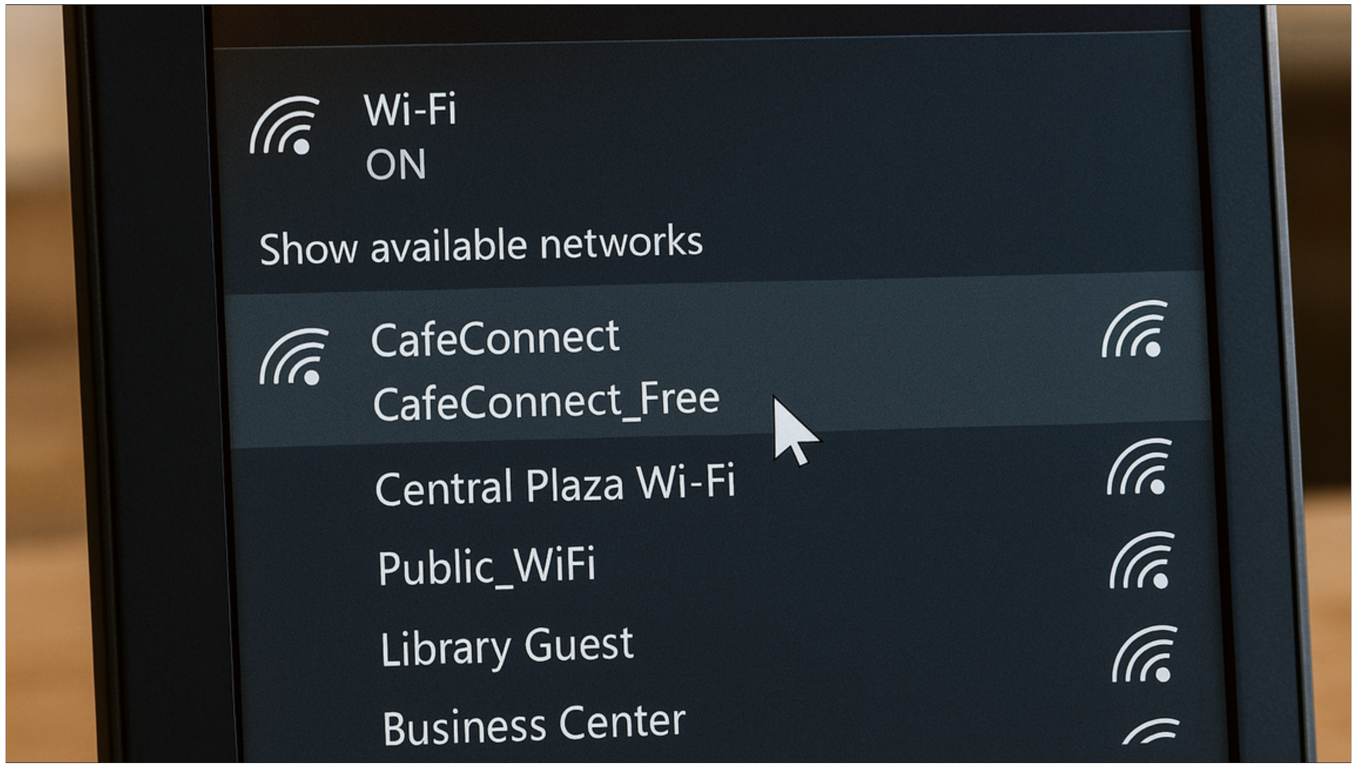
It’s really important that you do not approve any MFA request that you did not just request.

QR codes are super convenient, but you also want to make sure you are scanning a legitimate code.

Do we all know what this is?

- If the QR code isn’t part of a printed poster, card, or sign. Be careful.
- If you see just a QR code, all alone, posted somewhere, it might be tempting to see what it is. Leave it alone!

Fun fact, QR codes have different levels of error correction. In some cases, if 30% of the QR code is missing, it will still be functional.



Evil twin network

Ask the venue which network to use.

Use phone hot-spot
Use VPN

Phone scams have been around as long as the telephone.

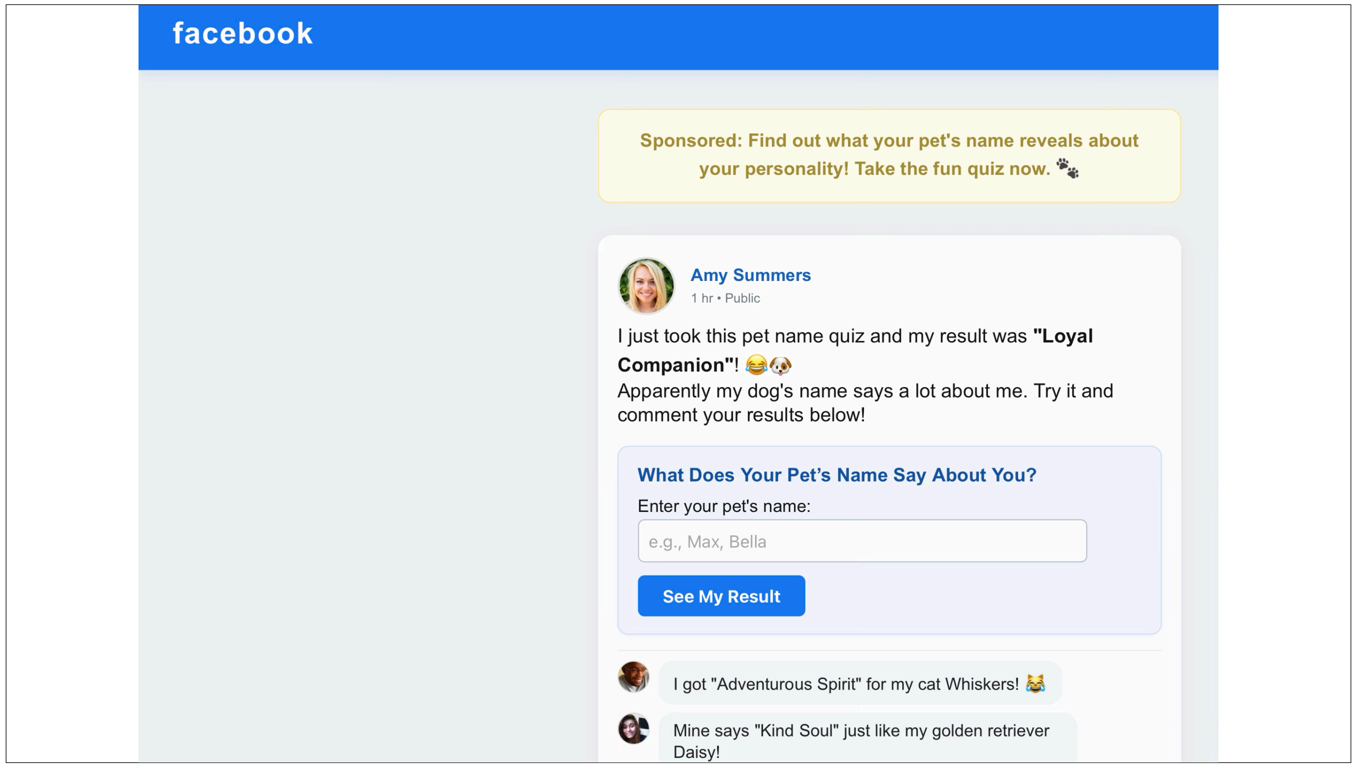
But because of AI, these scam calls are much cheaper to operate. It doesn't have to be a person on the other end, it can be AI.

Often the best defense is to never answer the phone of a number you do not recognize. 9 times out of 10, no message will be left, and you can then be fairly certain it is a scam.

Uploaded pictures of my grandkids to the church web site.

There is relevant data stored in your picture.

Picture metadata
GPS coordinates, date, time



Sponsored: Find out what your pet's name reveals about your personality! Take the fun quiz now. 🐾

Amy Summers
1 hr • Public

I just took this pet name quiz and my result was **"Loyal Companion"**! 😂🐶
Apparently my dog's name says a lot about me. Try it and comment your results below!

What Does Your Pet's Name Say About You?
Enter your pet's name:
e.g., Max, Bella
See My Result

I got "Adventurous Spirit" for my cat Whiskers! 😹

Mine says "Kind Soul" just like my golden retriever Daisy!

Social media

Ever see a quiz like this on Facebook or other social media?
What does your pet's name say about you?
What your favorite food says about you!

These are, in a sense, identify theft. They are gathering information about you. What can they gather?
- your IP address
- The name of your internet service provider
- Your browser type and all of the extensions it has installed
- What operating system, the type of CPU you have (Intel, etc.)
- Even your screen resolution

In truth, any website you visit can obtain all of this information as well, but legitimate websites typically don't…and/or they have a published privacy policy that enumerates the information they collect an what they do with it.

Every time you take one of these surveys, that organization learns something more about you. If you take enough surveys, they can create a considerable profile about your behavior, preferences, patterns, etc. and use it against you for different types of attacks - email, accounts, etc.

If you wouldn’t run down the street shouting it, why would you post it on social media? Truth is, I could run down a busy street screaming my bank password and my money would still be just fine. I certainly couldn’t do that on social media.

On another note:
Let’s remember that a good percentage of social media users and posts are fake.

Anyone have any of these?

Anyone ever find one of these and plug it in?

Also, charging cables at airports. [click]

Most devices will ask if you want to connect to a USB device
Don’t depend on it
Only charge devices on your cables and chargers
USB-C cables come in multiple flavors, if you bring a “charge only” cable it only have conductors on the power connections, so no data can be transferred at all.

End of session 1

I hate to say it, but the list of potential threats we've gone through isn't exhaustive. There are others too!

I asked if you would put together a list of devices in your house. Anyone have any internet devices that were not covered earlier?

- can the software be updated?
- Is it still supported?

I hate to say it, but so many digital devices have an incredibly short life-span before they become a liability. It should make you think twice whether you want (or really need) a wi-if connected coffee maker.

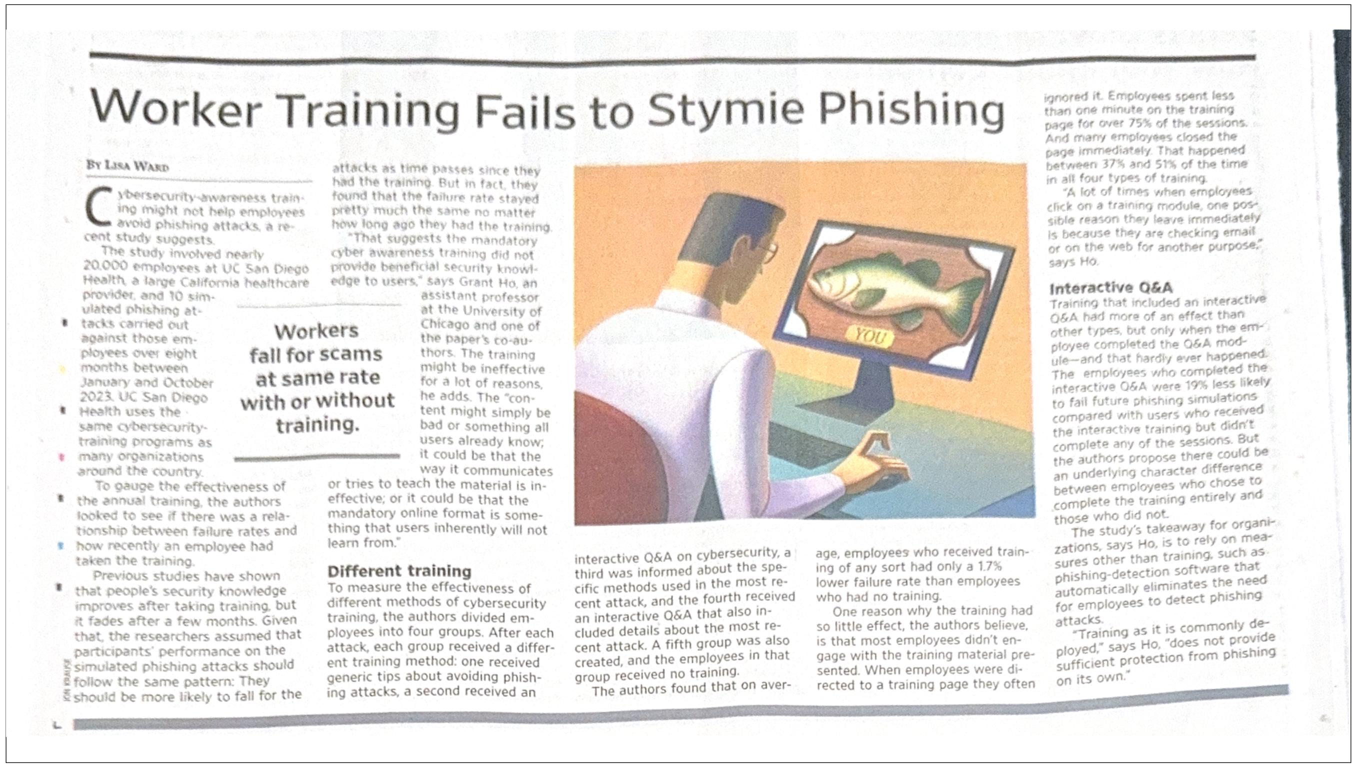
Next week, we're going to look at some of these same threats, but at that time we're going to talk about what you can do to prevent them from causing harm.

[Homework]
Something to think about…
1) What if you lost your computer and everything on it? How would it impact you. What would you do? Same for phone.

2) Are all of your devices up to date?

Protecting Your Digital Life

Click with Confidence - Session 2



Worker Training Fails to Stymie Phishing

By Lisa Ward

Cybersecurity-awareness training might not help employees avoid phishing attacks, a recent study suggests.

The study involved nearly 20,000 employees at UC San Diego Health, a large California healthcare provider, and 10 simulated phishing attacks carried out against those employees over eight months between January and October 2023. UC San Diego Health uses the same cybersecurity-training programs as many organizations around the country.

To gauge the effectiveness of the annual training, the authors looked to see if there was a relationship between failure rates and how recently an employee had taken the training.

Previous studies have shown that people's security knowledge improves after taking training, but it fades after a few months. Given that, the researchers assumed that participants' performance on the simulated phishing attacks should follow the same pattern: They should be more likely to fall for the attacks as time passes since they had the training. But in fact, they found that the failure rate stayed pretty much the same no matter how long ago they had the training.

"That suggests the mandatory cyber awareness training did not provide beneficial security knowledge to users," says Grant Ho, an assistant professor at the University of Chicago and one of the paper's co-authors. The training might be ineffective for a lot of reasons, he adds. The "content might simply be bad or something all users already know; it could be that the way it communicates or tries to teach the material is ineffective; or it could be that the mandatory online format is something that users inherently will not learn from."

Workers fall for scams at same rate with or without training.

KEN ORVIDAS

Different training

To measure the effectiveness of different methods of cybersecurity training, the authors divided employees into four groups. After each attack, each group received a different training method: one received generic tips about avoiding phishing attacks, a second received an interactive Q&A on cybersecurity, a third was informed about the specific methods used in the most recent attack, and the fourth received an interactive Q&A that also included details about the most recent attack. A fifth group was also created, and the employees in that group received no training.

The authors found that on average, employees who received training of any sort had only a 1.7% lower failure rate than employees who had no training.

One reason why the training had so little effect, the authors believe, is that most employees didn't engage with the training material presented. When employees were directed to a training page they often ignored it. Employees spent less than one minute on the training page for over 75% of the sessions. And many employees closed the page immediately. That happened between 37% and 51% of the time in all four types of training.

"A lot of times when employees click on a training module, one possible reason they leave immediately is because they are checking email or on the web for another purpose," says Ho.

Interactive Q&A

Training that included an interactive Q&A had more of an effect than other types, but only when the employee completed the Q&A module—and that hardly ever happened. The employees who completed the interactive Q&A were 19% less likely to fail future phishing simulations compared with users who received the interactive training but didn't complete any of the sessions. But the authors propose there could be an underlying character difference between employees who chose to complete the training entirely and those who did not.

The study's takeaway for organizations, says Ho, is to rely on measures other than training, such as phishing-detection software that automatically eliminates the need for employees to detect phishing attacks.

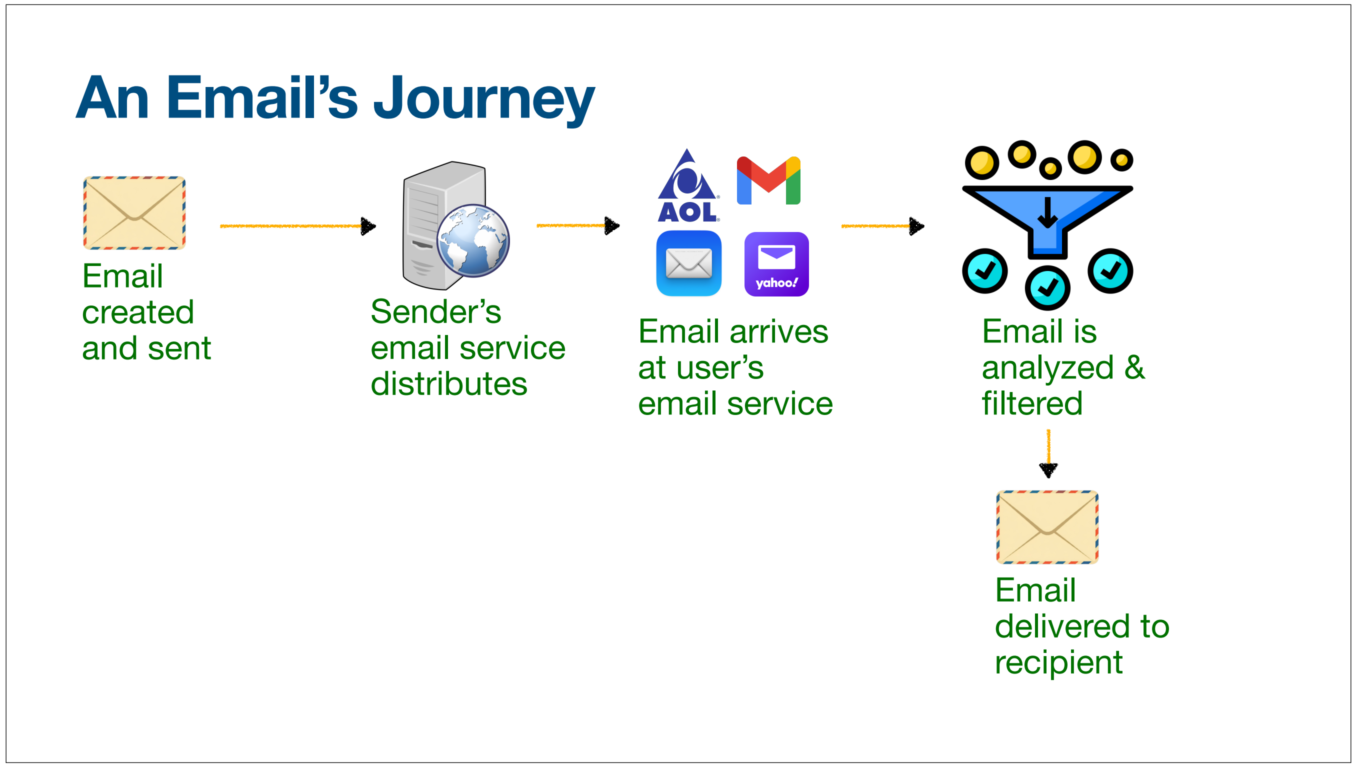
"Training as it is commonly deployed," says Ho, "does not provide sufficient protection from phishing on its own."

Here's some bad news.

According to a study of nearly 20,000 employees at UC San Diego Health, employees with security training fall for phishing scams at the same rate as those without.

Why did you bother coming to class?

Today, we’re mostly talking about ways to prevent threats to your data and devices. But there is one more threat I wanted to cover before we move on, with respect to hyperlinks in emails and web pages.



An Email’s Journey

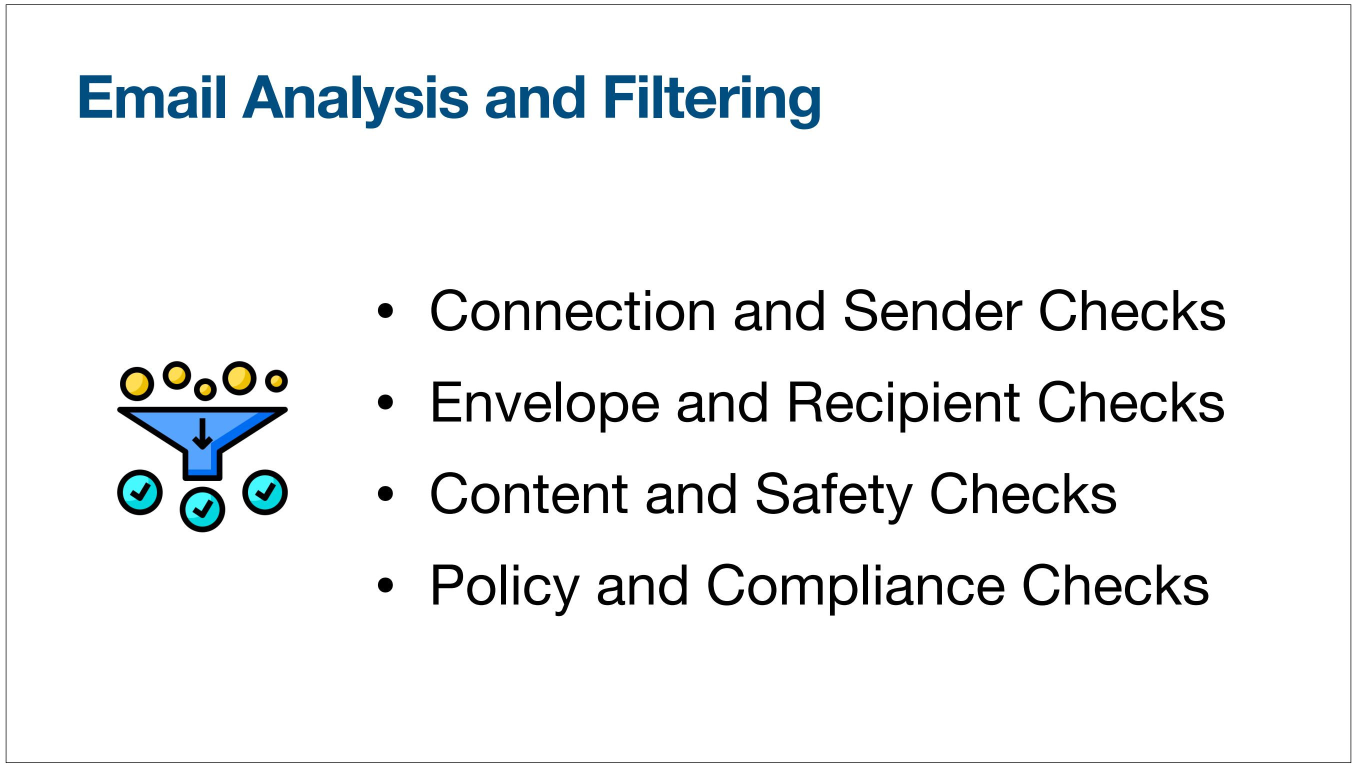
Email created and sent

Sender’s email service distributes

Email arrives at user’s email service

Email is analyzed & filtered

Email delivered to recipient



Email Analysis and Filtering

- Connection and Sender Checks
- Envelope and Recipient Checks
- Content and Safety Checks
- Policy and Compliance Checks

Connection and sender checks

IP reputation: The server checks whether the computer that sent the message is known to send spam. If it has a bad reputation, the message may be blocked.
Reverse DNS / HELO check: The server verifies that the sending machine identifies itself properly. If the sender looks fake, that’s suspicious.
Rate limits: If the sending server is sending lots of messages too fast, the mail may be slowed or rejected.
Envelope and recipient checks

Recipient exists: The server checks that the address you sent to actually exists. If it doesn’t, the message bounces back.
Mailbox quota: If the recipient’s mailbox is full, the server may defer delivery or bounce the mail.
Authentication checks (making sure the sender is who they claim to be)

SPF (simple): The server checks a list published by the sender’s domain to see if the sending computer was allowed to send mail for that address. Think of it as checking a list of approved post offices.
DKIM (simple): A digital “seal” on the message is checked to see if the message was altered in transit and really came from the sending domain.
DMARC (simple): Uses SPF and DKIM together to decide whether mail that appears to come from a particular domain should be trusted, quarantined, or rejected.
Content and safety checks

Spam filtering: Automated systems look for signs of spam (bad wording, suspicious links, unusual formatting). Many providers use machine learning to score messages.
Malware and virus scanning: Attachments and message content are scanned for viruses or malicious software. Dangerous attachments may be stripped or the message

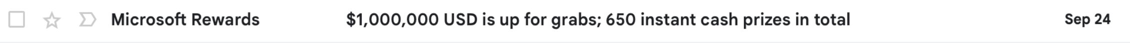
blocked.
Phishing detection: The service looks for fake login pages or tricks to steal information and may flag or quarantine such messages.
URL checking: Links in the message are checked against known dangerous sites; some services rewrite links to check them at click-time.
Policy and compliance checks

Blocklists / allowlists: The sender's domain or IP may be explicitly blocked or allowed by the recipient's settings or organization policy.
Attachment and file-type rules: Certain file types (executable files, macros) are often blocked automatically. Large attachments may be rejected.
Heuristic and behavioral checks

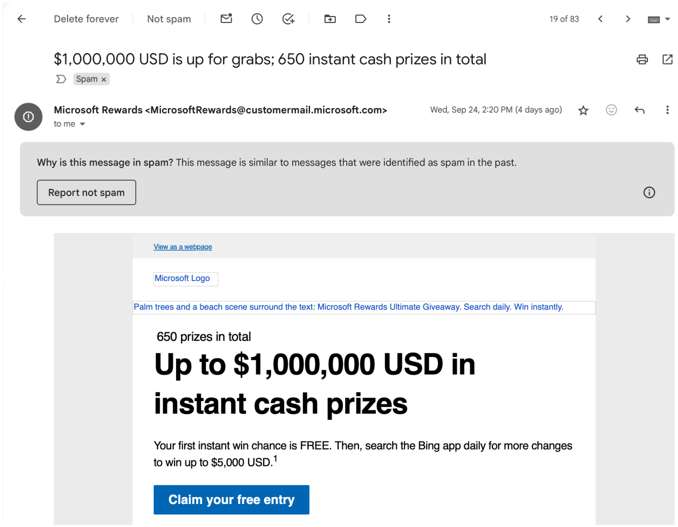
Content scoring / reputation scoring: The server gives the message a score based on many signals; very low scores get routed to Junk, very high scores to Inbox.
Greylisting: A server may temporarily refuse mail from an unknown sender and accept it only if the sending server retries after a delay (spammers often won't retry).
Post-acceptance processing

Sieve / user filters: The server can run user-specific rules (move to folders, auto-delete, forward) after accepting the message.
Quarantine: Suspicious messages may be held in a quarantine where a user or admin can review them instead of delivering to the inbox.
Logging and notifications: The system records why messages were accepted or blocked and may notify admins or users of bounced or quarantined mail.
Special cases and protections

Sandboxing: Suspicious attachments can be opened in a safe environment to see if they do anything harmful before delivering.
Forwarding and authentication preservation (ARC): When mail is forwarded, authentication can break; ARC is a system that tries to preserve trust across trusted intermediaries.
TLS encryption check: The server may require an encrypted connection (TLS) from the sender or may note whether the transport was encrypted.



☐ ☆ Microsoft Rewards $1,000,000 USD is up for grabs; 650 instant cash prizes in total Sep 24



$1,000,000 USD is up for grabs; 650 instant cash prizes in total

Microsoft Rewards <MicrosoftRewards@customermail.microsoft.com>
to me

Wed, Sep 24, 2:20 PM (4 days ago)

Why is this message in spam? This message is similar to messages that were identified as spam in the past.

View as a webpage

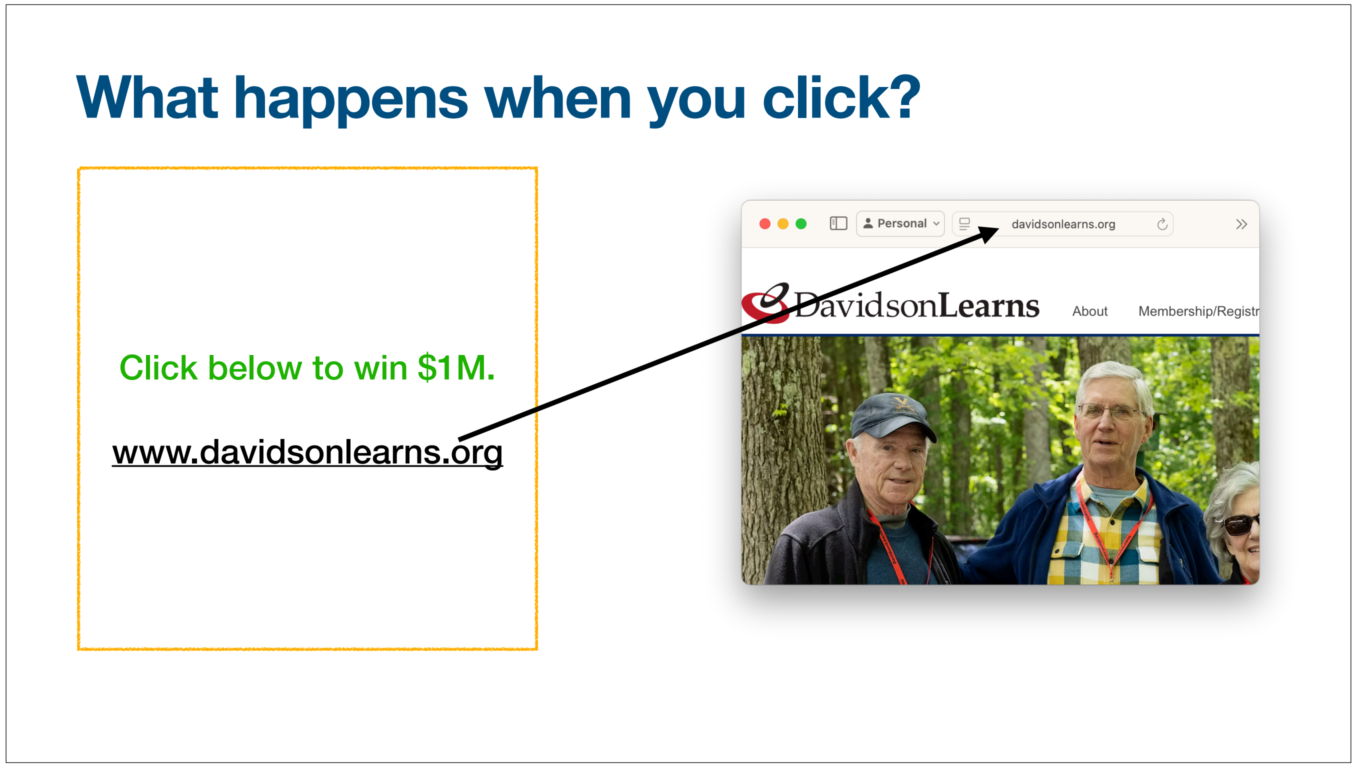
Microsoft Logo

Palm trees and a beach scene surround the text: Microsoft Rewards Ultimate Giveaway. Search daily. Win instantly.

650 prizes in total

Up to $1,000,000 USD in instant cash prizes

Your first instant win chance is FREE. Then, search the Bing app daily for more changes to win up to $5,000 USD.[1]



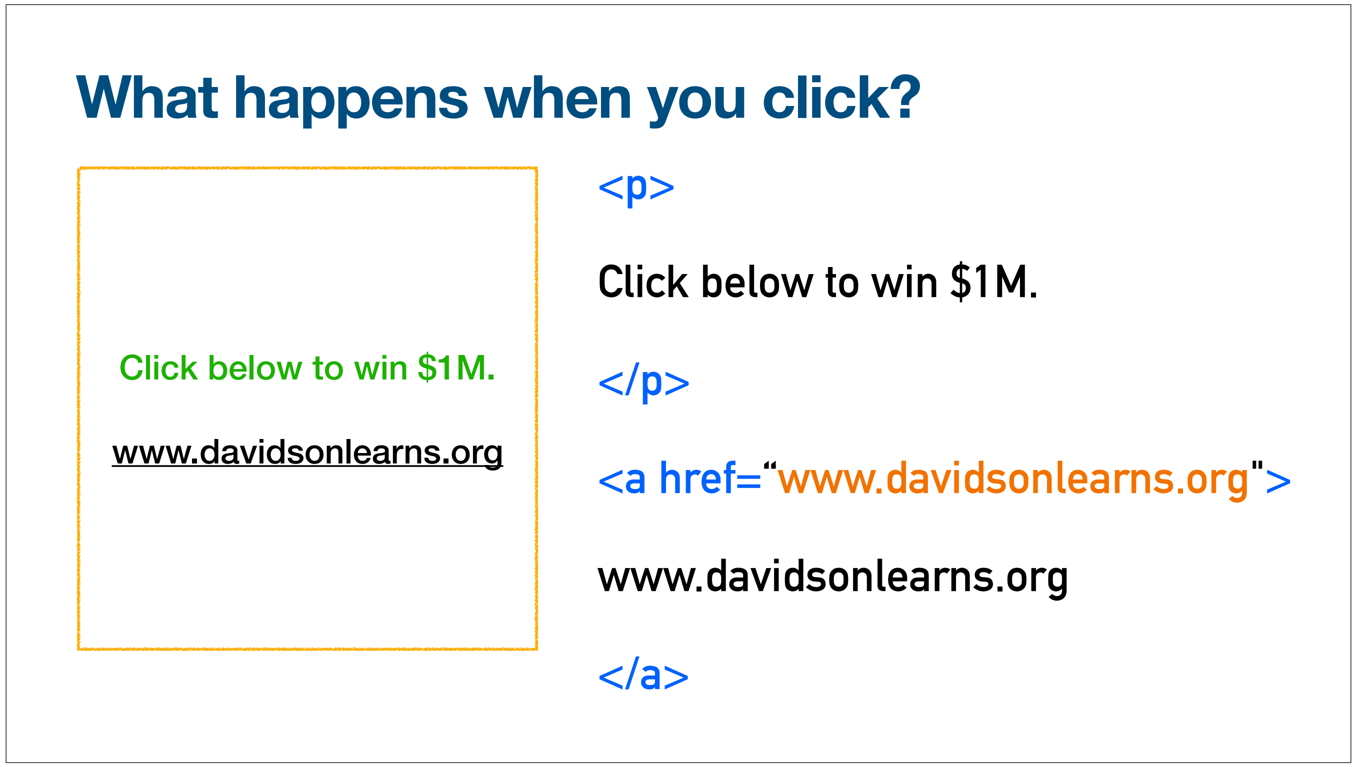
What happens when you click?

Click below to win $1M.

www.davidsonlearns.org

When you see an email, you only see part of it.
Behind each email is HTML - the same language that is used to create web pages
Each email, in a way, is a miniature web page
Like web pages, emails can have images, different fonts and layouts, and you can click on links

Click on URL
Browser takes you to that web-page



What happens when you click?

Click below to win $1M.

www.davidsonlearns.org

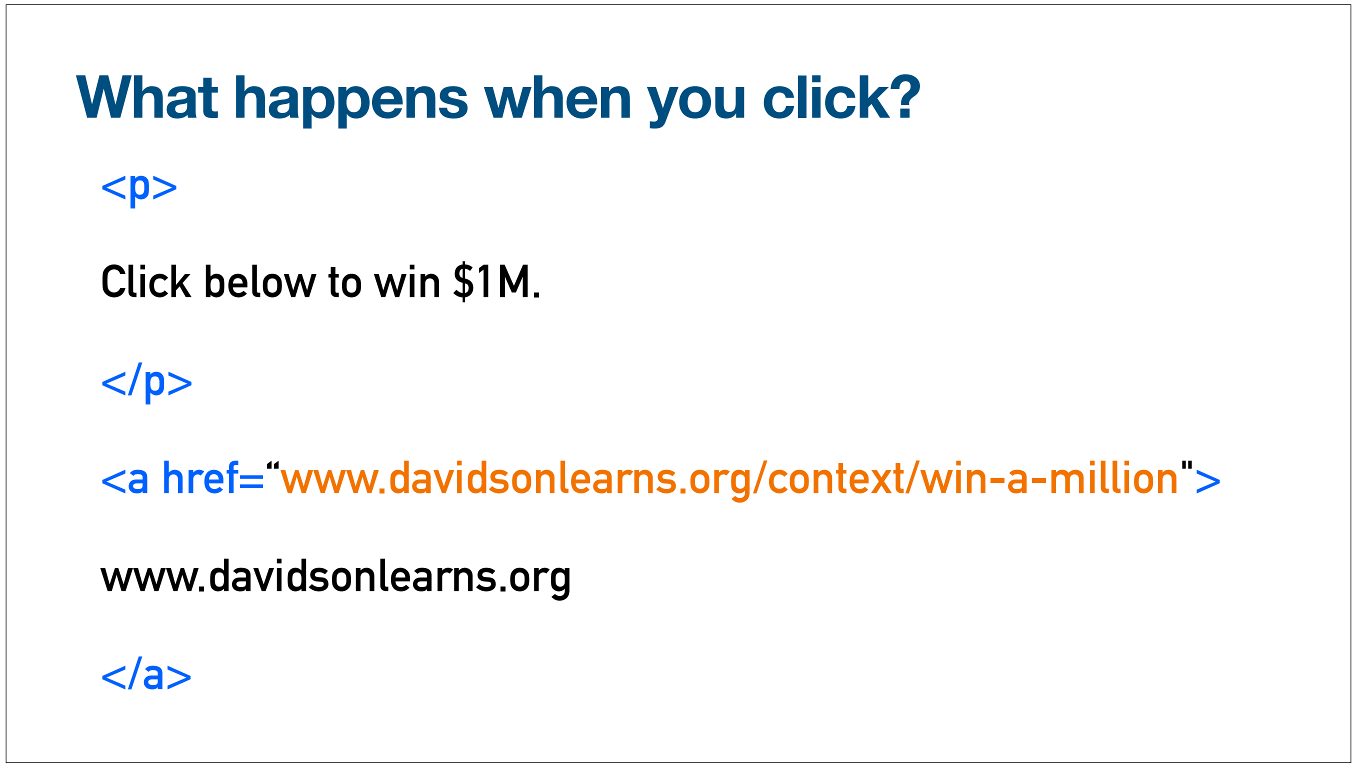
```
<p>

Click below to win $1M.

</p>

<a href=“www.davidsonlearns.org">

www.davidsonlearns.org

</a>
```

Let’s go a little deeper and really look at the link to Davidson learns.

When you see a link, there is code that defines that link…it’s not just the text itself.

<p>
<a>
HREF
Text within link

I can make that link text say anything I want.

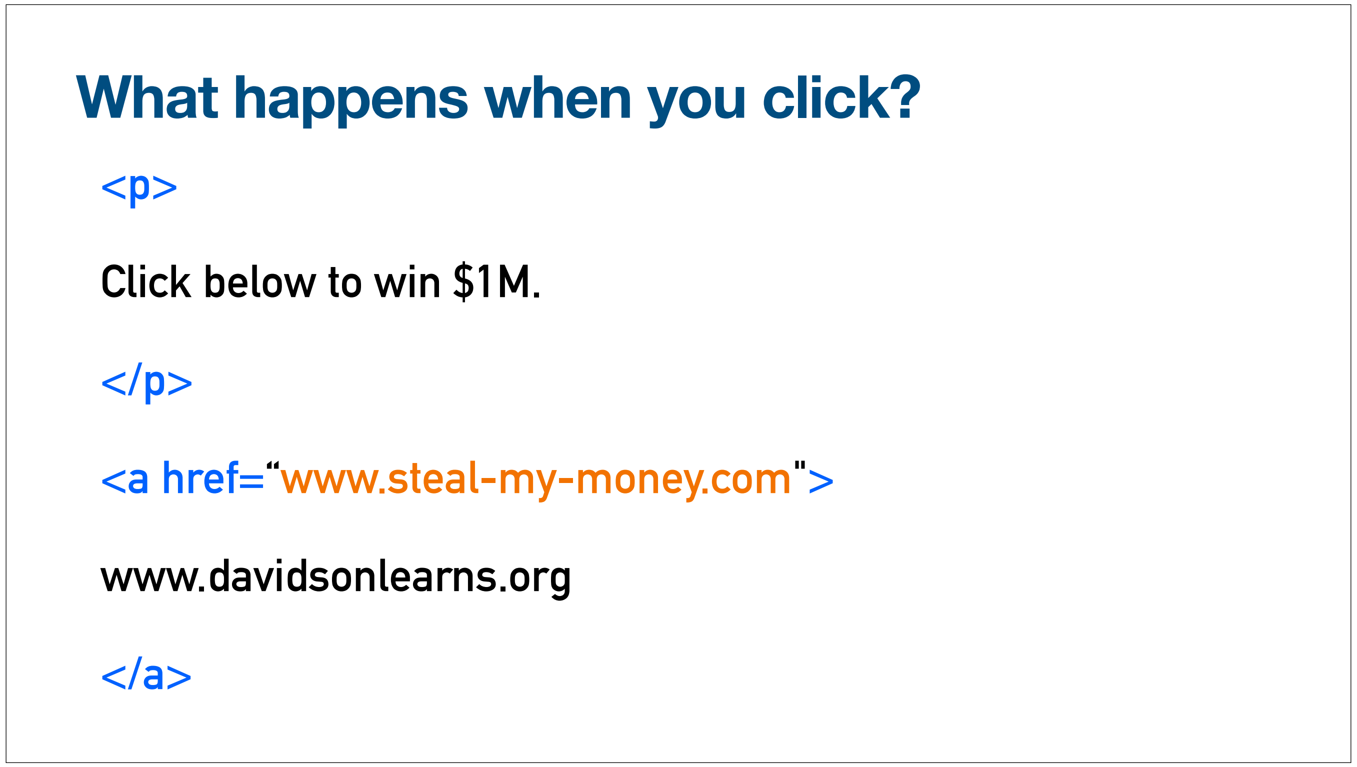


What happens when you click?

```
<p>

Click below to win $1M.

</p>

<a href=“www.davidsonlearns.org/context/win-a-million">

www.davidsonlearns.org

</a>
```

This is really useful, because sometimes the website we want to send people to is cumbersome.

But it also means we could display something that looks legitimate, but when they click, takes them somewhere else entirely.



What happens when you click?

```
<p>
Click below to win $1M.
</p>
<a href=“www.steal-my-money.com">
www.davidsonlearns.org
</a>
```

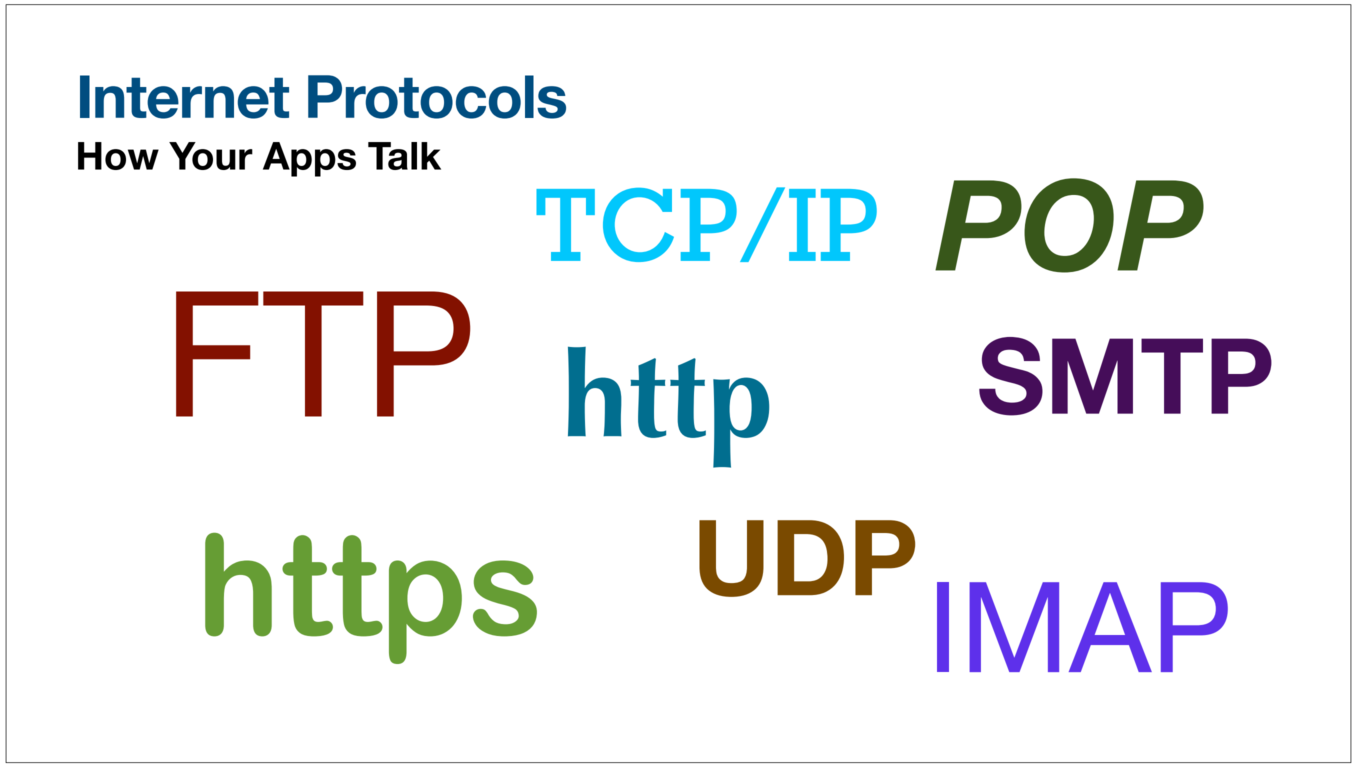
So even though the link you clicked, says something…like Davidson learns.org, in reality, it could take you to another website entirely.

This is why it is super important to check the URL after you click a link…

OR BETTER YET, type in the URL yourself!

Virtual Private Network
How do they work?

Isn’t my internet traffic already encrypted?



Internet Protocols

How Your Apps Talk

TCP/IP POP

FTP http SMTP

https UDP IMAP

You may be familiar with some of these. In general, HTTPS is the one that matters for most things we do
Hyper-Text Transfer Protocol - Secure
It's the communication protocol our web browsers use to talk to web servers, that provide us the content for any web page.

Originally, there was no S. It was just HTTP. That worked fine for a while, in the early days of the web, but then people started using their web browsers to make purchases, and do online banking, and other transactions that require a little, or a lot, of security.

So HTTPS was, and still is the answer.

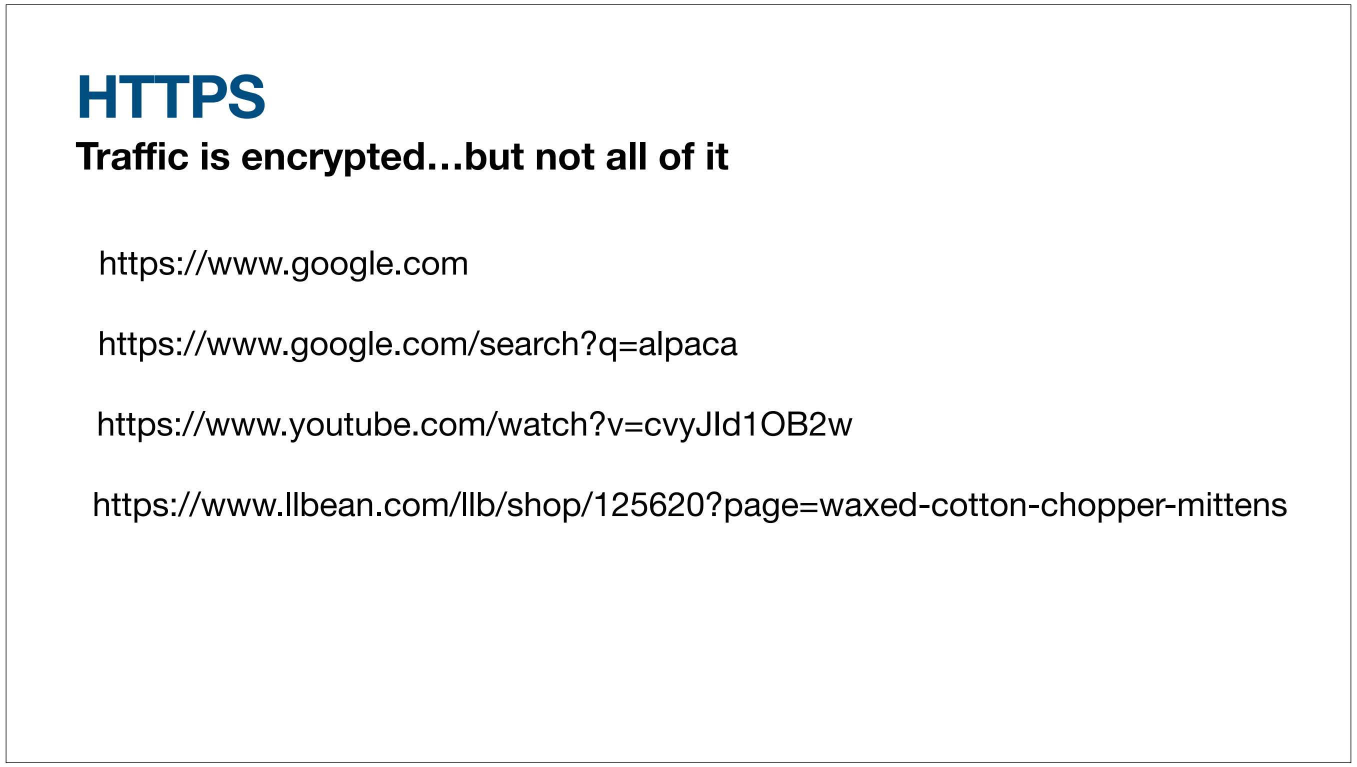
In general, you should only use websites that are secured through HTTPS. There are some sites, that really make no difference if they are encrypted or not. Checking the weather really doesn't matter if it's encrypted.

But it's better if everything behaves similarly, so having everything encrypted is better than some that are and some that are not.

We're getting pretty close to that dream. Some 90% of web sites or more are HTTPS.

In October 2026, Google Chrome will "mandate" https traffic, and warn users if they are not browsing a site encrypted via https.

This will certainly help convert the other 10%.



HTTPS

Traffic is encrypted…but not all of it

https://www.google.com

https://www.google.com/search?q=alpaca

https://www.youtube.com/watch?v=cvyJId1OB2w

https://www.llbean.com/llb/shop/125620?page=waxed-cotton-chopper-mittens

When you are on a website that uses https, all of that information you type into a form (Credit Card, Address, Phone number, email) is encrypted when transmitted to the web servers. This protects your information.

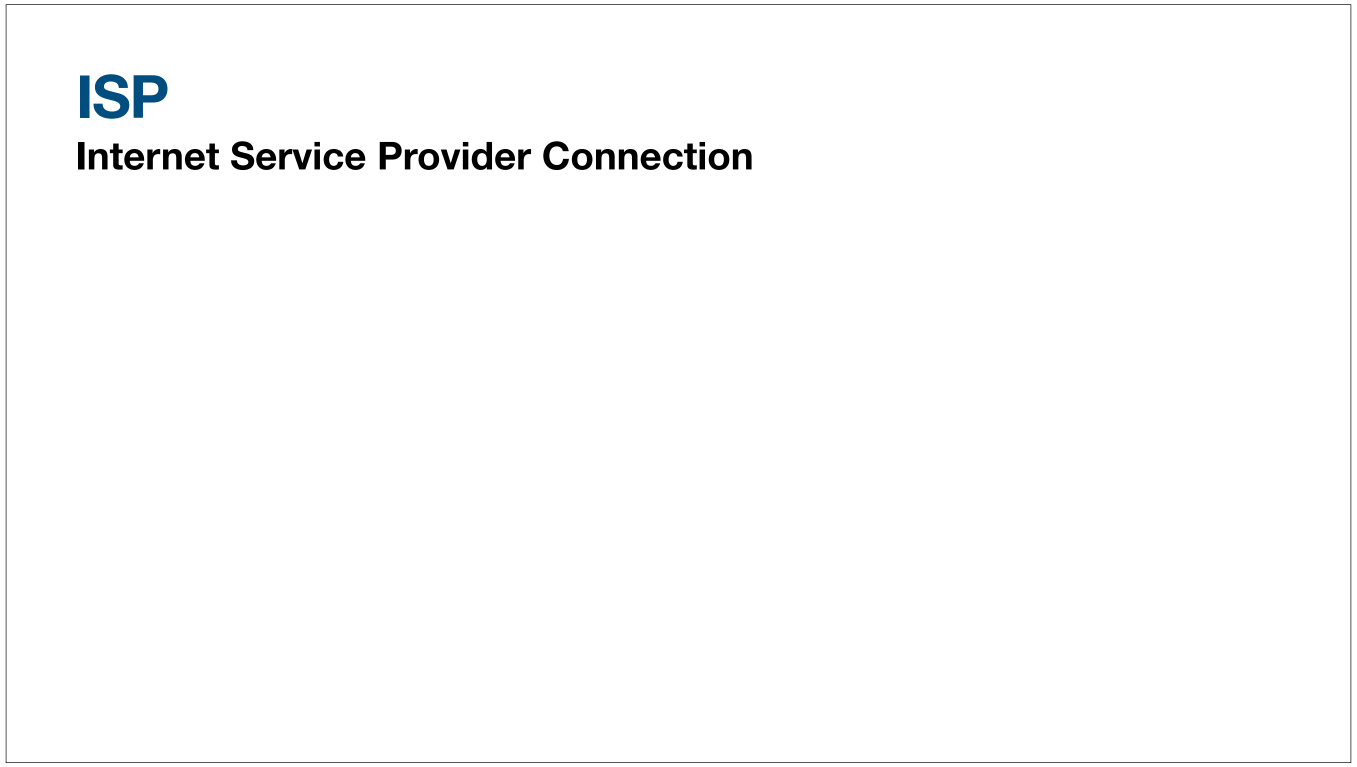
But it doesn’t necessarily protect your privacy.

Your ISP has visibility of every URL you go to, encrypted or not. They know if you go to google, they know what you searched for.

YouTube: You can’t tell from the URL, but if you go to that URL you’ll see that I’ve watched a video of the 1929 Detroit Tigers playing the Philadelphia Athletics.

And My ISP knows it too.

Since 2017, in the US, ISPs have been allowed to mine and sell data derived from your browsing history. If you want to further protect your privacy, a Virtual Private Network or VPN is your answer.



ISP

Internet Service Provider Connection

Your internet traffic travels from your device, over the network to your ISP, which is usually close to you. Even for large ISPs like Comcast, they have what are called Points of Presence or POPs all over the country.

Connecting to a close-by POP makes your internet faster than if you had to make a connection Half-way across the country.

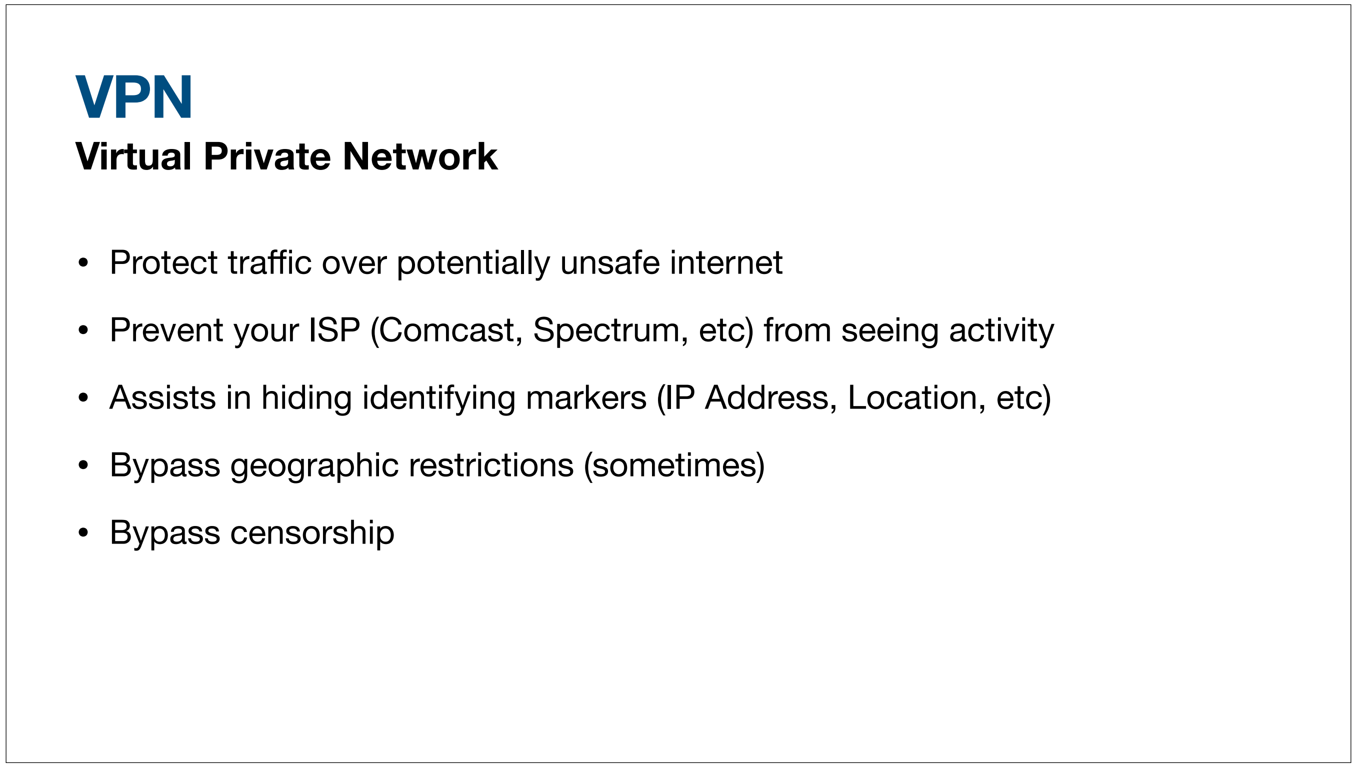
VPN

Virtual Private Network

Using a VPN, you device will now connect to a server owned by the VPN company.

But it will create a connection within that connection…a tunnel, which hides all of your traffic from your ISP.

Now your traffic is invisible to your ISP (but potentially visible to the VPN provider, who, depending on who you use, might be selling all of your data). Your VPN provider matters.



VPN

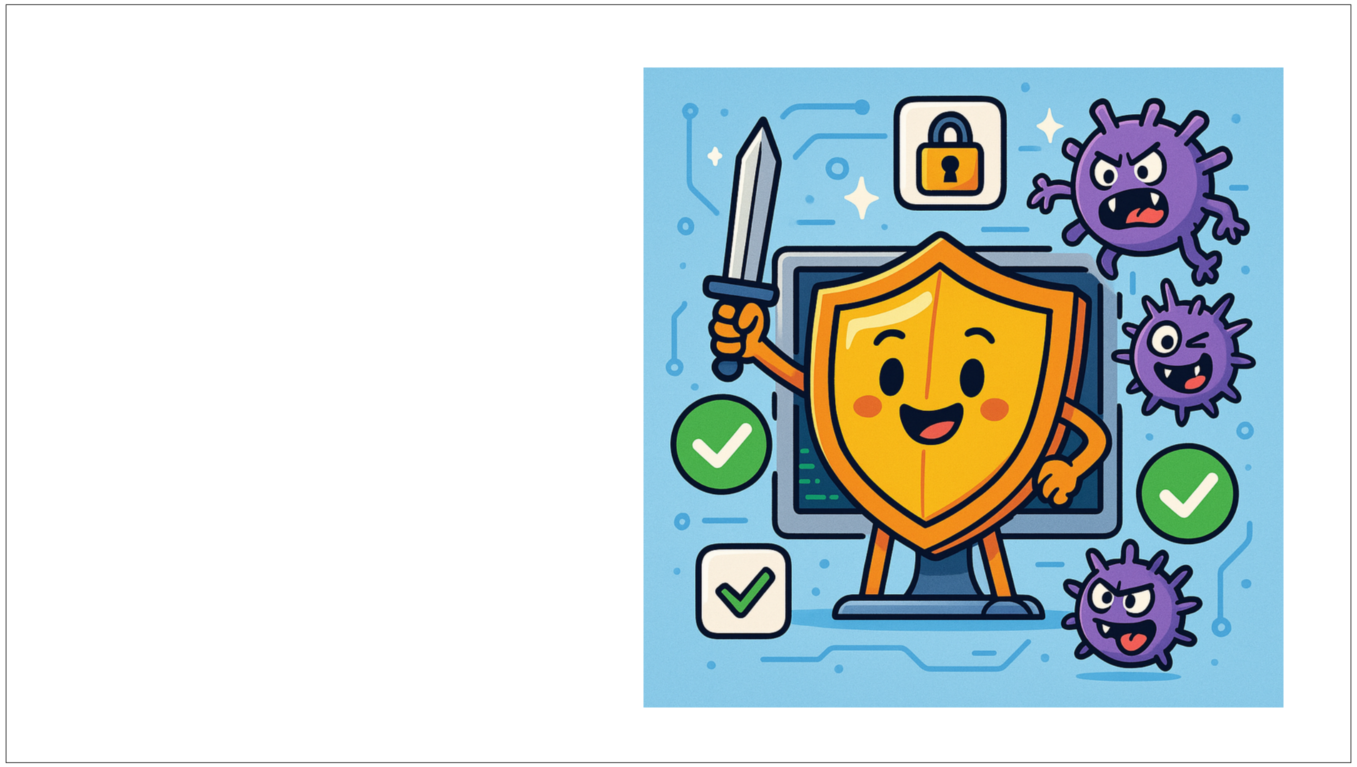
Virtual Private Network

- Protect traffic over potentially unsafe internet
- Prevent your ISP (Comcast, Spectrum, etc) from seeing activity
- Assists in hiding identifying markers (IP Address, Location, etc)
- Bypass geographic restrictions (sometimes)
- Bypass censorship

So why would you use a VPN?

For most people, they are too much hassle.
 - VPN connection might go down and you might not realize it
 - Can be very slow
 - More configuration, compatibility challenges, passwords, and cost (although some are free…why?)

The main reason to use a VPN is if you are connected to an unsafe WiFi network. And in that case, your best option is to use your mobile phones hotspot capability and connect to your phone instead.



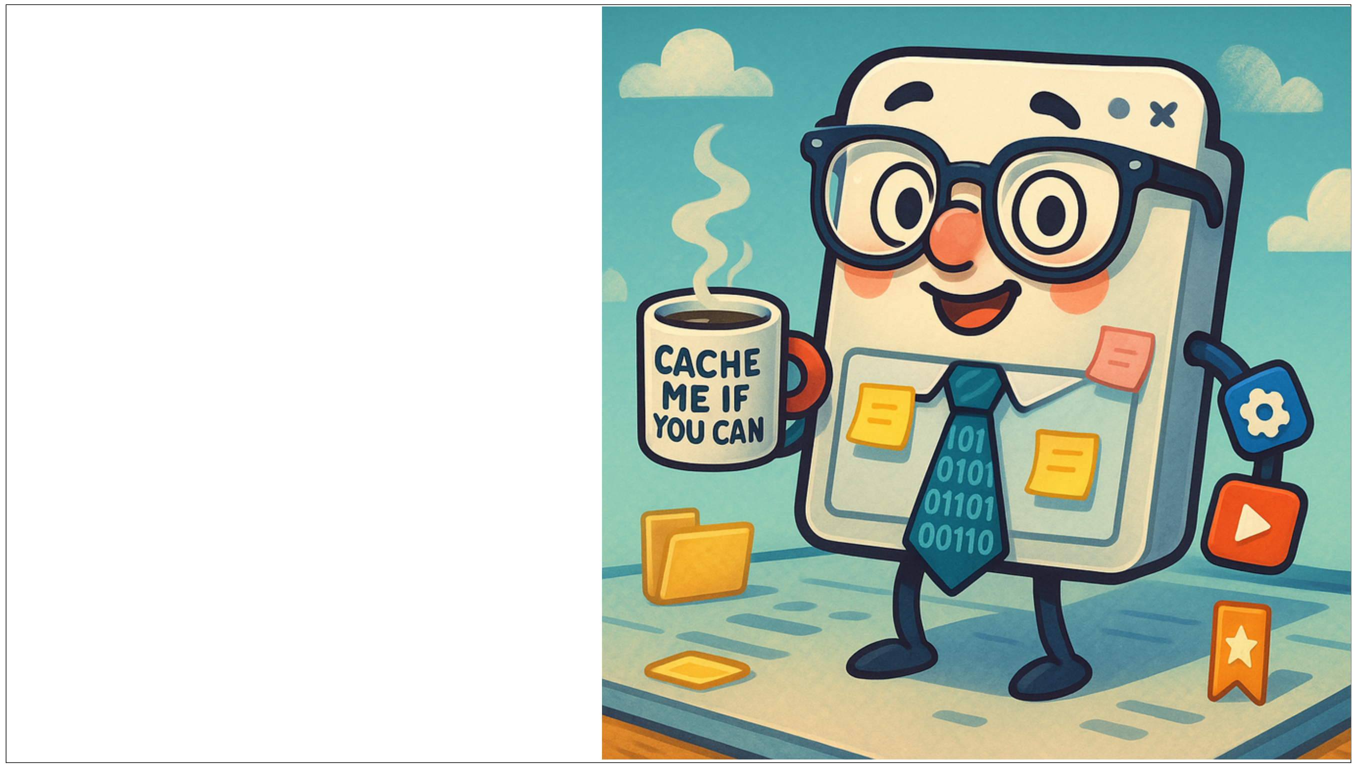
Viruses exist
Malware exists

Anti-Virus software can detect viruses and malware, remove it, and keep your data safe

For Mac and Windows computers, for the most part, you do not need additional software.
The built-in safeguards will protect you, it helps to keep your operating system up to date.

But you can really only make that assumption if you take reasonable precautions.
1) Don’t install any software except from the App Store
2) Stay away from shady websites
3) Don’t download anything that you can’t absolutely verify and trust

The ultimate solution is to make sure your backups are current. If you were to ever get a virus on your computer, you can erase your computer, restore from backup, and you’re good to go.

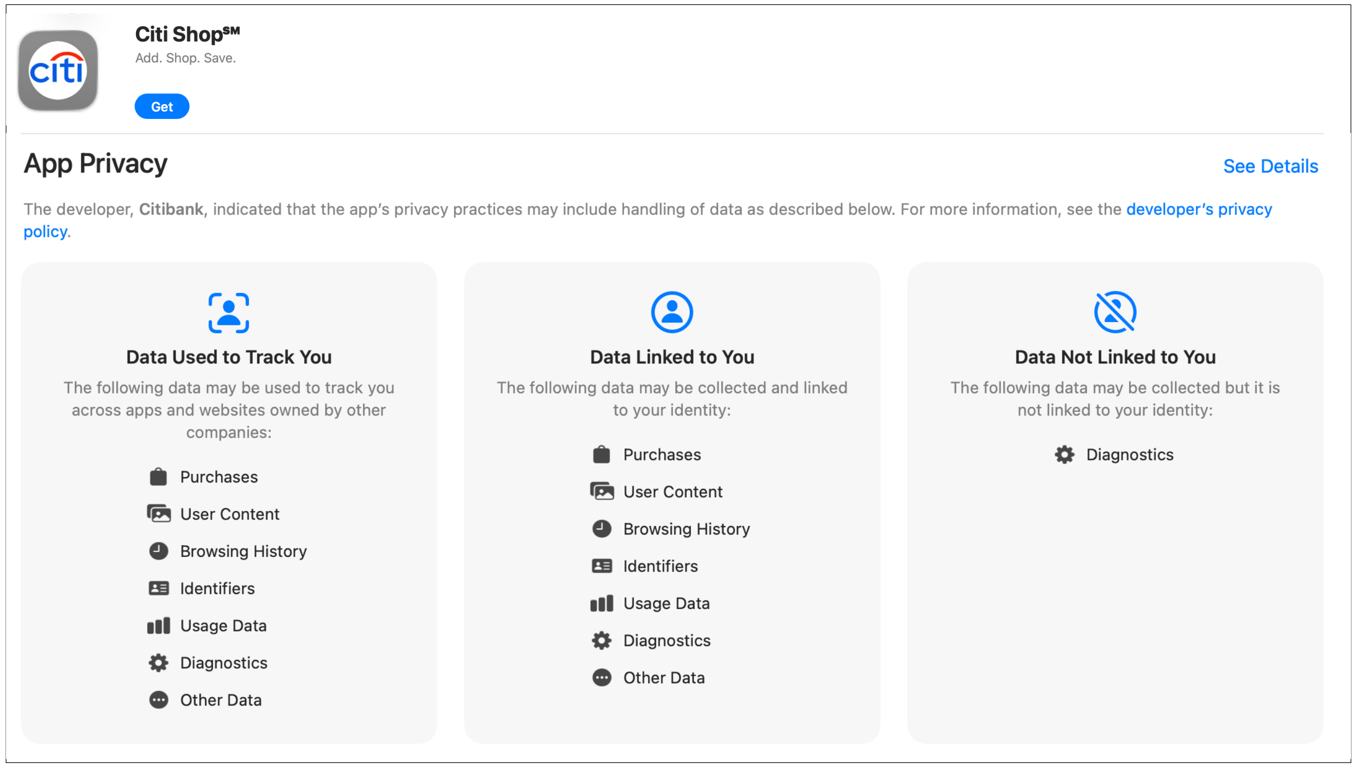


Examples
- Shopping assistants to find the best price
- Ad Blockers
- Grammar checkers
- Accessibility assistants

A lot of software sounds convenient, few make it so
We don’t need these typically - often we install them and never use them

They are privacy bandits!
- when you install a browser extension, it basically has access to everything that’s in your browser window
- they might be legitimate extensions when you install them, then get popular, someone buys the company and changes the terms and conditions so that they have greater access to your data

Don’t complicate your life…keep things simple
Best advice is to remove these from your browser, unless you have a very specific browser extension need.



Citi Shop℠
Add. Shop. Save.
Get

App Privacy
See Details

The developer, **Citibank**, indicated that the app's privacy practices may include handling of data as described below. For more information, see the developer's privacy policy.

Data Used to Track You

The following data may be used to track you across apps and websites owned by other companies:

- Purchases
- User Content
- Browsing History
- Identifiers
- Usage Data
- Diagnostics
- Other Data

Data Linked to You

The following data may be collected and linked to your identity:

- Purchases
- User Content
- Browsing History
- Identifiers
- Usage Data
- Diagnostics
- Other Data

Data Not Linked to You

The following data may be collected but it is not linked to your identity:

- Diagnostics

Here's a look at the privacy practices for the #11 shopping extension in the App Store

It tracks everything.

I asked ChatGPT to analyze the detailed developer's privacy policy:

Citi collects a wide range of personal and sensitive data, including social security numbers, financial information, biometric data, geolocation, internet activity, and inferences about your behavior and preferences.

Citi may share non-sensitive personal identifiers, demographic info, commercial account and transaction data, internet activity, professional info, and behavioral inferences with third-party advertisers and partners. This could expose your information to targeted marketing, profiling, and other external uses.

The site uses cookies, web beacons, and device fingerprinting to track online behavior, potentially creating very detailed profiles about you. These tracking tools may persist across devices and be shared with third parties, raising risks of cross-site tracking and profiling.

Your personal information may be stored and processed in countries with different (and potentially weaker) data protection laws. Foreign government authorities may legally access your data.

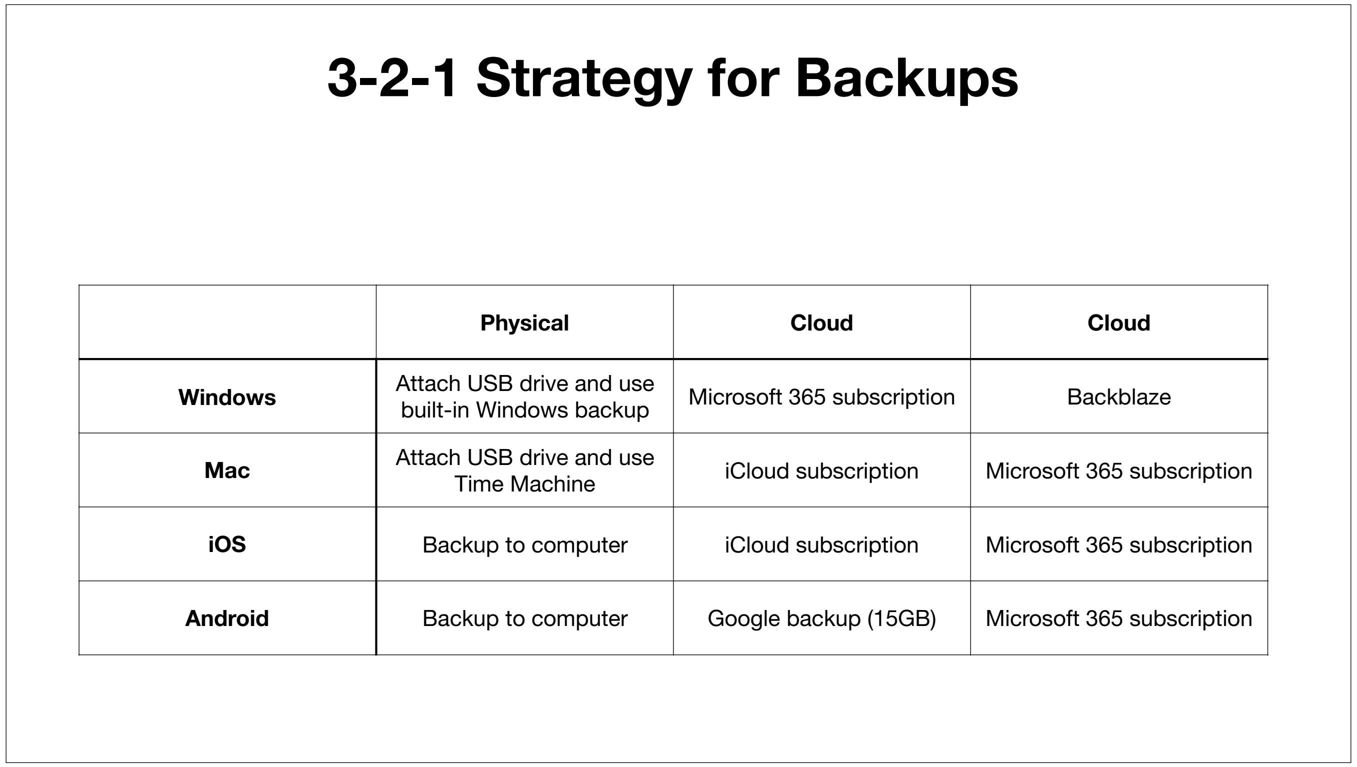
Interest-Based Advertising: Citi can use your data to deliver targeted ads on its own and third-party platforms, tie your personal information to lifestyle attributes, and associate multiple devices to you.

Potential Gaps in Security: While Citi implements security measures, they acknowledge that no online system is 100% secure, meaning your personal information can still be vulnerable to breaches.

This is a complicated subject.

How many people backup their computer? How do you do it?

A robust backup strategy is the 3-2-1 rule



3-2-1 Strategy for Backups

	Physical	Cloud	Cloud
Windows	Attach USB drive and use built-in Windows backup	Microsoft 365 subscription	Backblaze
Mac	Attach USB drive and use Time Machine	iCloud subscription	Microsoft 365 subscription
iOS	Backup to computer	iCloud subscription	Microsoft 365 subscription
Android	Backup to computer	Google backup (15GB)	Microsoft 365 subscription

3 copies: Original and 2 backups
2 storage types: cloud and physical
1 offsite: not at home (cloud or family member's house)

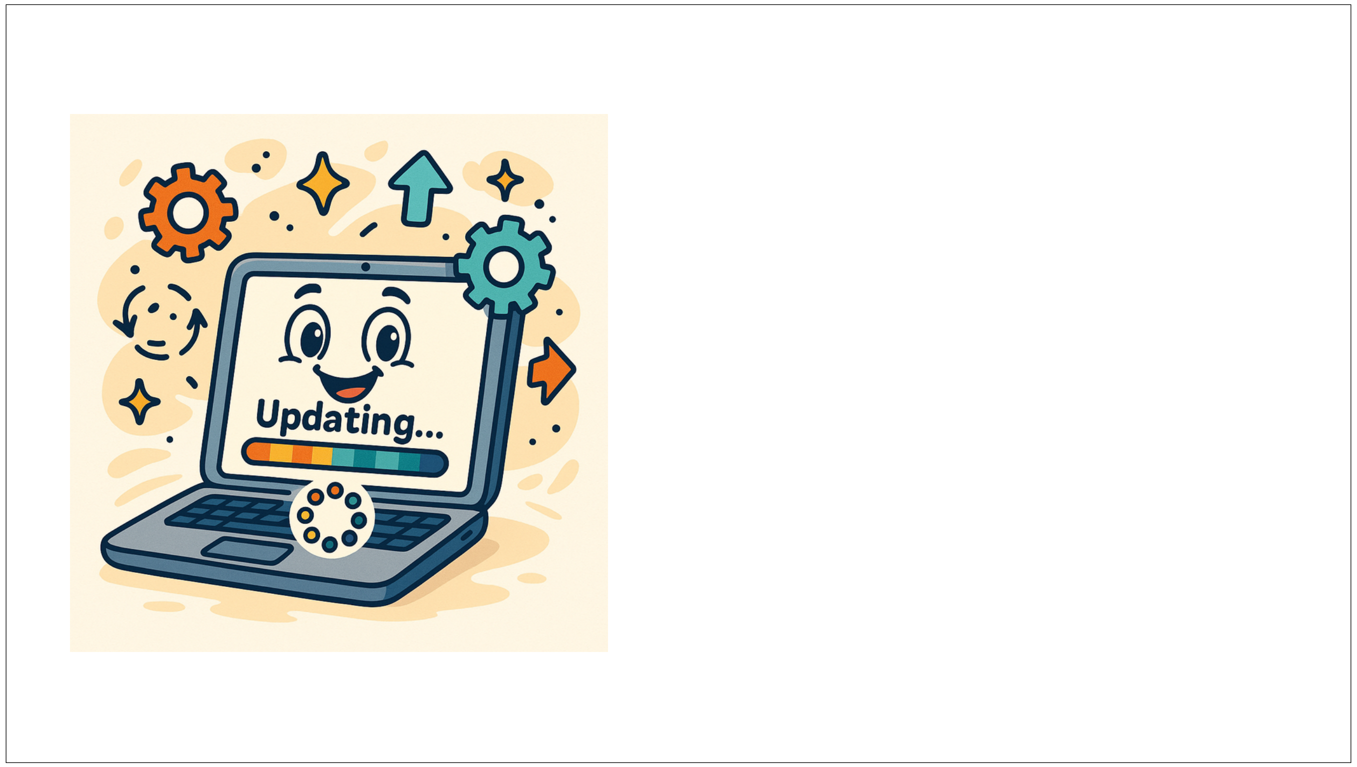
Cloud storage is typically stored in multiple locations

- it is uploaded, and then the cloud provider sends that data to multiple places around the world

You may want to consider a USB hard drive backup and create a backup schedule that meets your needs. That could be daily, weekly, monthly or longer, depending on what you store on your computer.

Cloud backups are the best for most people. They are automatic and restoring from the cloud is typically easy.

But if you switch devices from Mac to Windows, or Android to iPhone, you'll jump through some hoops to convert the backups to the new device.

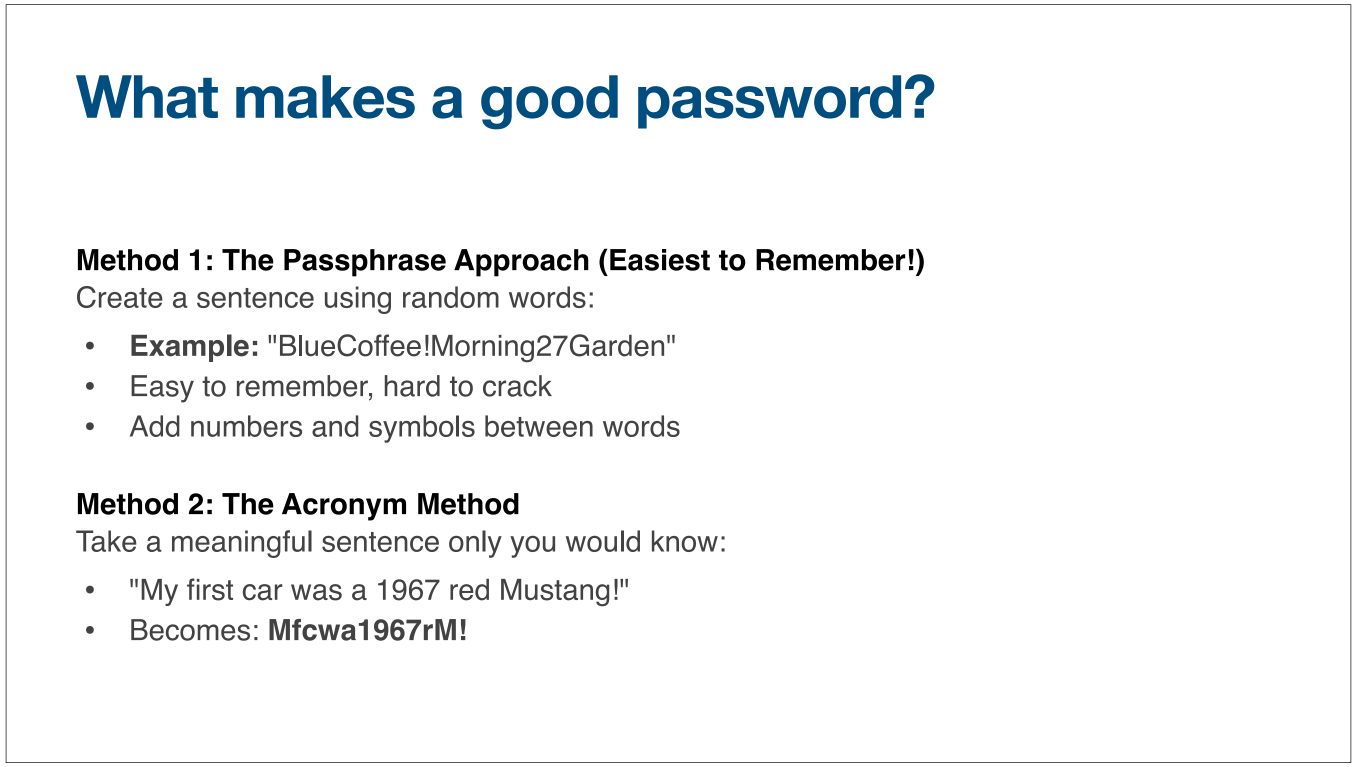


Anyone update any software over the past week?

New iOS and Mac updates were out. Windows had some updates the very end of October.

The #1 reason why computers are compromised is due to older, insecure versions of software.

Mobile
PC/Mac
IoT Devices - firmware updates
Router
TVs



What makes a good password?

Method 1: The Passphrase Approach (Easiest to Remember!)
Create a sentence using random words:

- **Example:** "BlueCoffee!Morning27Garden"
- Easy to remember, hard to crack
- Add numbers and symbols between words

Method 2: The Acronym Method
Take a meaningful sentence only you would know:

- "My first car was a 1967 red Mustang!"
- Becomes: **Mfcwa1967rM!**

Minimum 12 characters (longer is better - aim for 15-20)
Each additional character makes a password exponentially harder to crack
A long, simple passphrase often beats a short complex password
Complexity Matters

Mix of uppercase and lowercase letters
Include numbers
Add special characters (!, @, #, $, %, etc.)
BUT: Don't sacrifice length for complexity

❌ Personal information (birthdays, names, addresses)

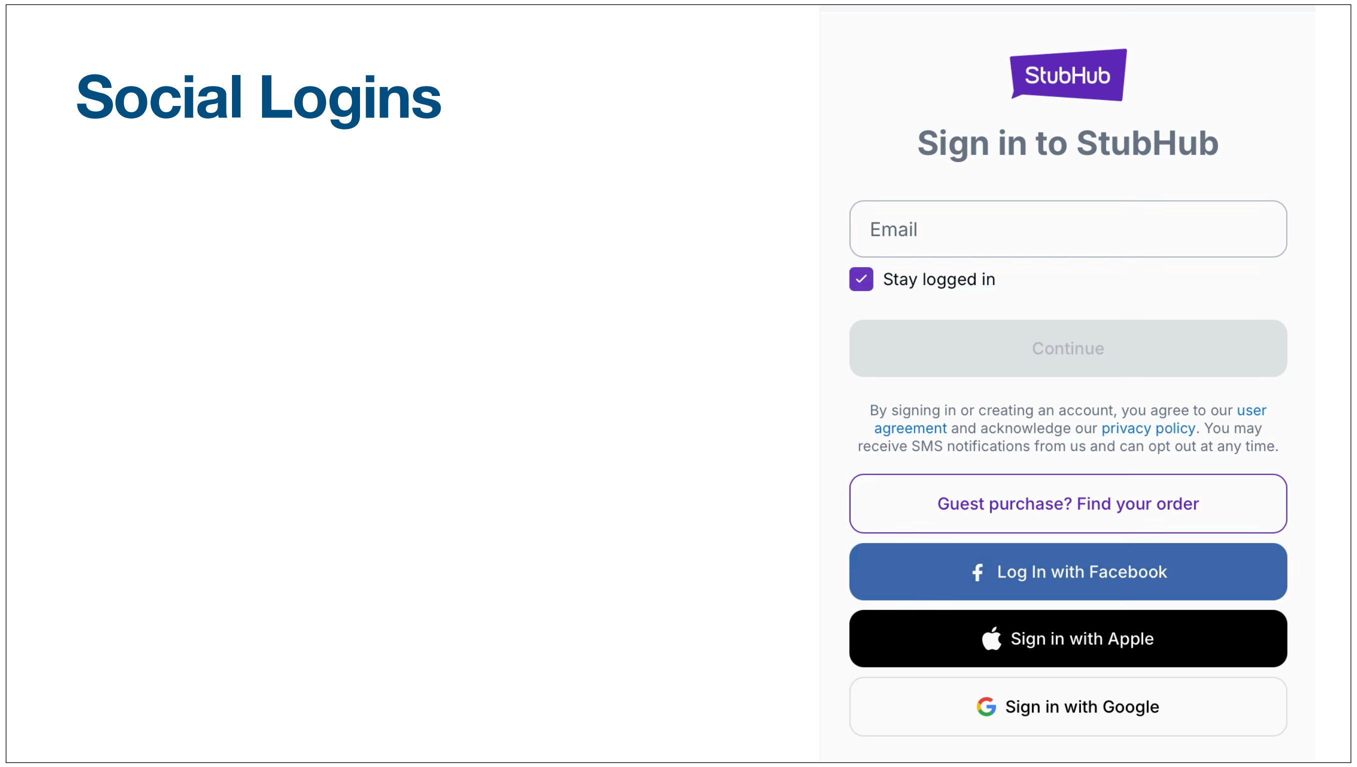
❌ Dictionary words or common phrases

❌ Sequential patterns (123456, abcdef, qwerty)

❌ The word "password" in any form

❌ Reusing passwords across multiple accounts

Social Logins



By signing in or creating an account, you agree to our user agreement and acknowledge our privacy policy. You may receive SMS notifications from us and can opt out at any time.

What about social logins…have you seen login pages that look like this?

What? Login with your facebook account or google account?

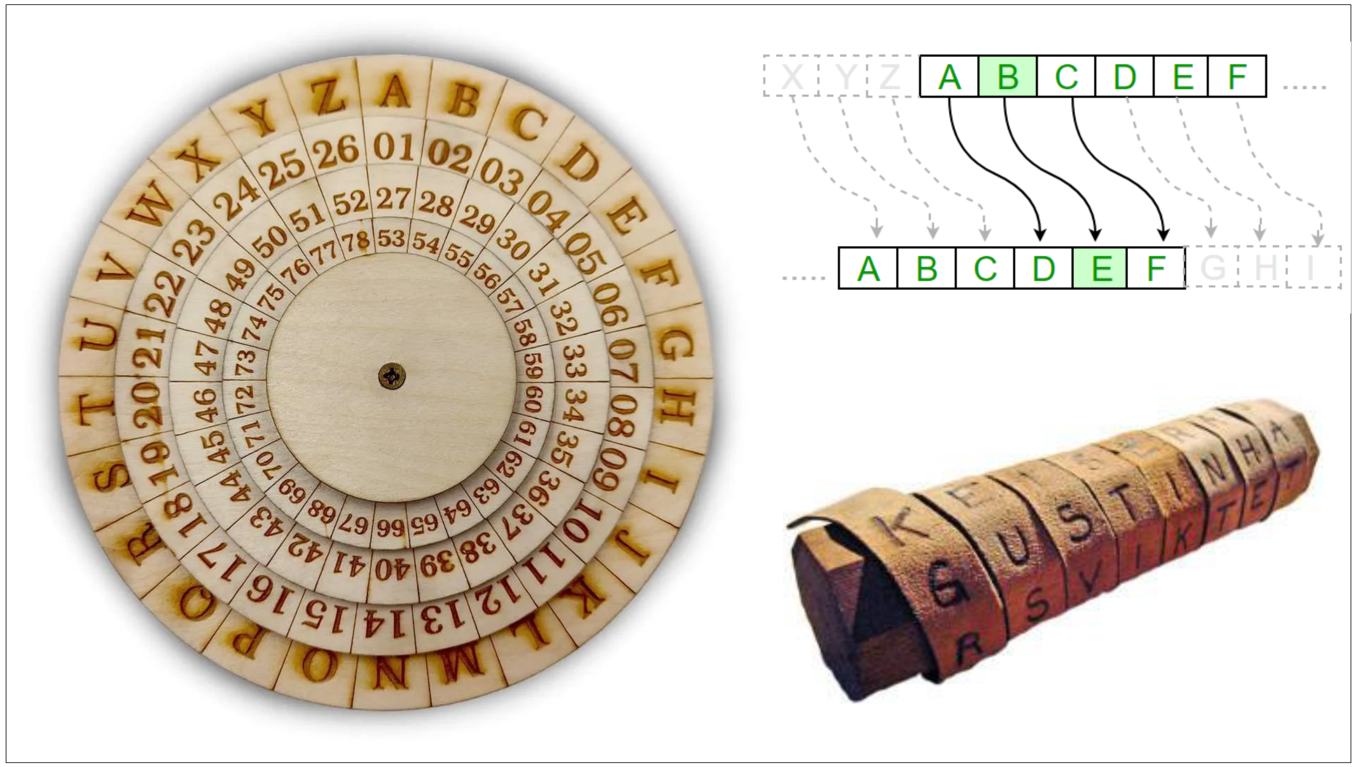
Is that safe? Yes

It is super convenient as well! You just click the button and if you're already logged into your social media account, it will log you in to this site as well.

If you are not logged in to your social media account, you will be prompted to do so.

It does introduce some risk, however. If someone steals your facebook account details, they they might be able to try logging into other sites…it's difficult and would be very time consuming, but possible.

To prevent that from happening, make sure you use MFA on your social logins.



Does anyone know what these are, or do?

They are ciphers…ways to encrypt a message so you can send something in secret.

They are pretty primitive, but when the average person who might intercept your message is illiterate, you don’t have to have something too sophisticated.

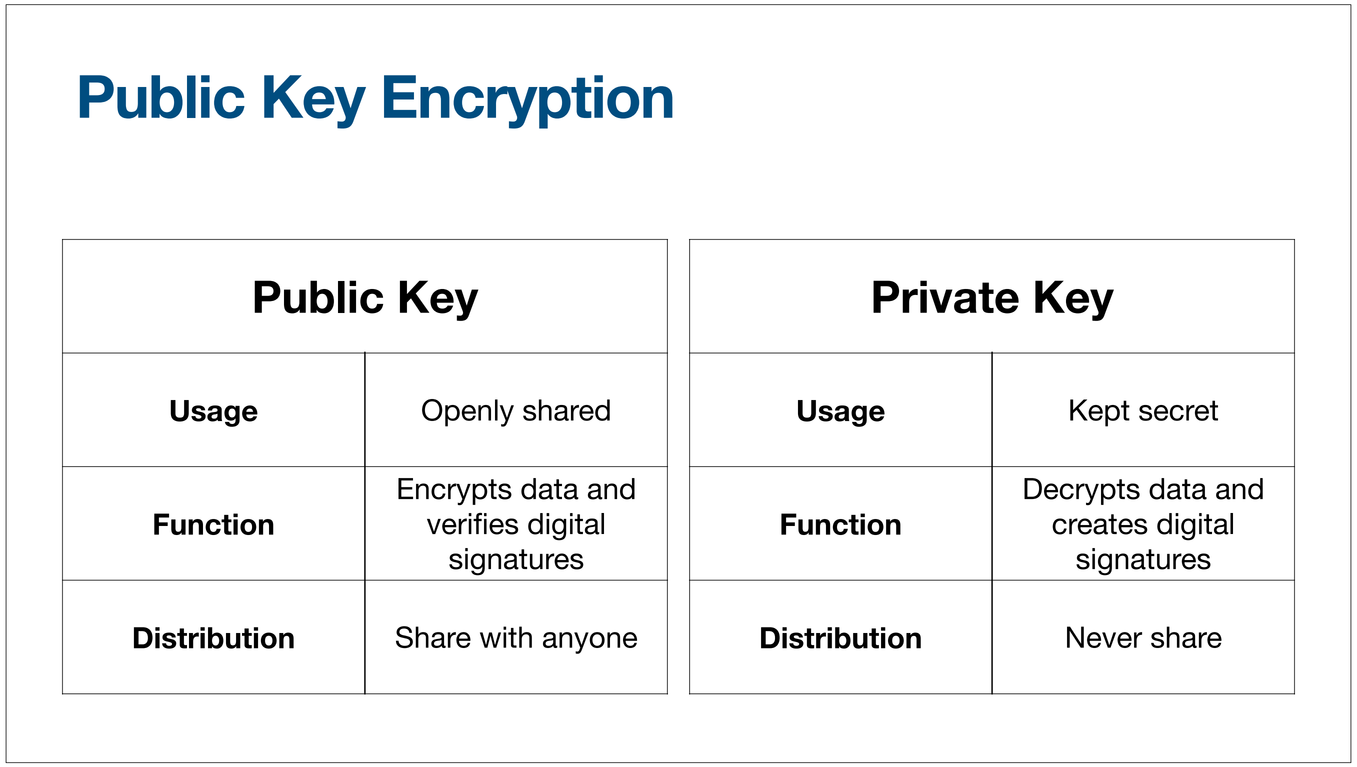
If you don’t want GenZ to read something - write it in cursive

These devices might be relatively effective, but they all have one thing in common that makes them (and many other methods) vulnerable.

Both the sender and the receiver of the message have to have the same secret code, code wheel, or other device. In order to decrypt the message, you had to use the same code as the person who encrypted it.

If someone else has that code, your encryption is now worthless.

This was a problem until about the mid-1970s.



Public Key Encryption

Public Key	
Usage	Openly shared
Function	Encrypts data and verifies digital signatures
Distribution	Share with anyone

Private Key	
Usage	Kept secret
Function	Decrypts data and creates digital signatures
Distribution	Never share

Public Key Encryption, or asymmetric cryptography, solves the problem of both parties having to have the same secret.

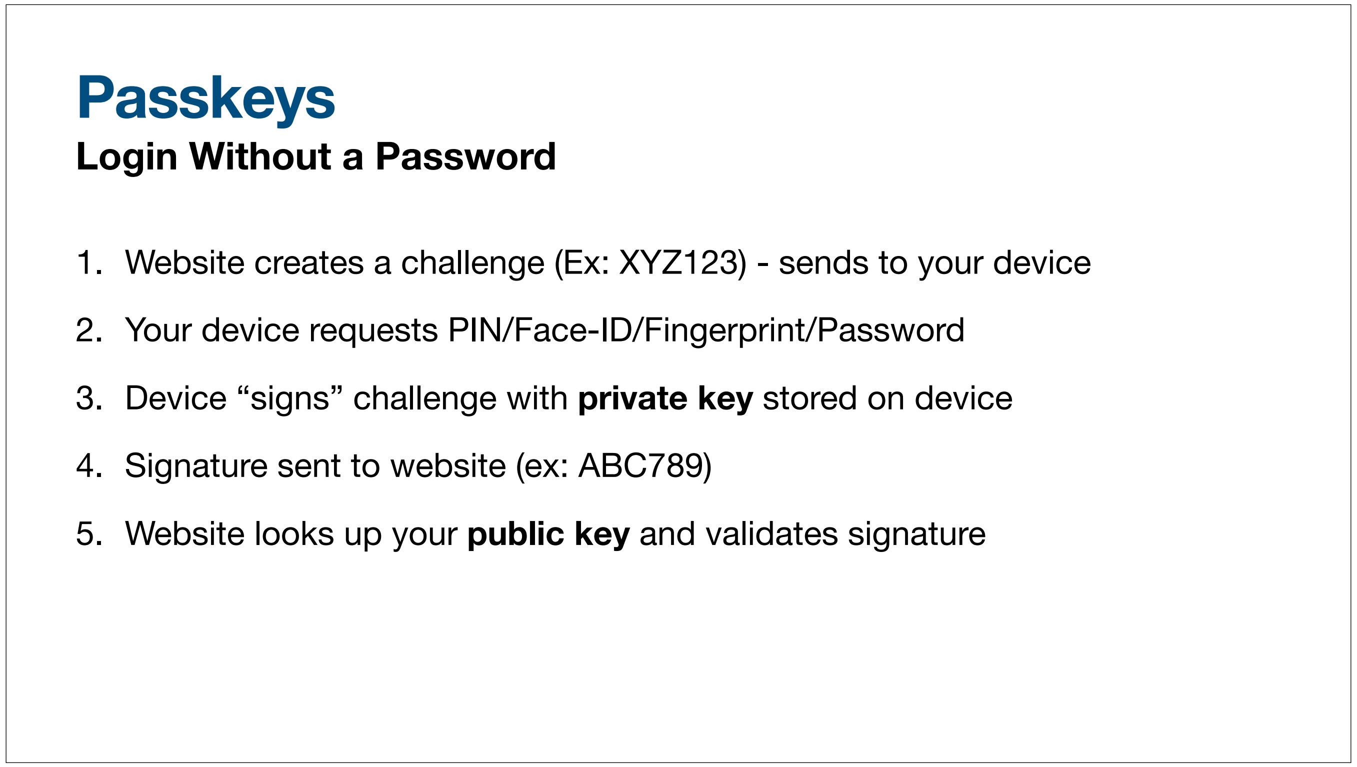
Public Key Encryption uses some heavy math that creates a public and private key pair.

You give the public key to anyone you want to send you a message. Doesn’t matter who gets there hands on it. You can share it with anyone…even broadcast it to the world.

When a message is encrypted with your public key…only you can read it, by decrypting it with your private key.

It’s important that the right public and private key pair is used, but now we have a way of encrypting and decrypting messages, without sharing the same secret.

WHY ARE WE TALKING ABOUT THIS?



Passkeys

Login Without a Password

1. Website creates a challenge (Ex: XYZ123) - sends to your device
2. Your device requests PIN/Face-ID/Fingerprint/Password
3. Device “signs” challenge with **private key** stored on device
4. Signature sent to website (ex: ABC789)
5. Website looks up your **public key** and validates signature

Passkeys use this system in order to allow you to login without a password

When you create a Passkey for a website, which is created on your device, you store the private key on your device and send the website your public key.

Now when you go to that website, the website and your device talk to each other, and validate that you are who you say you are.

If someone steals your public key, they don’t have access to anything. It’s useless to them.

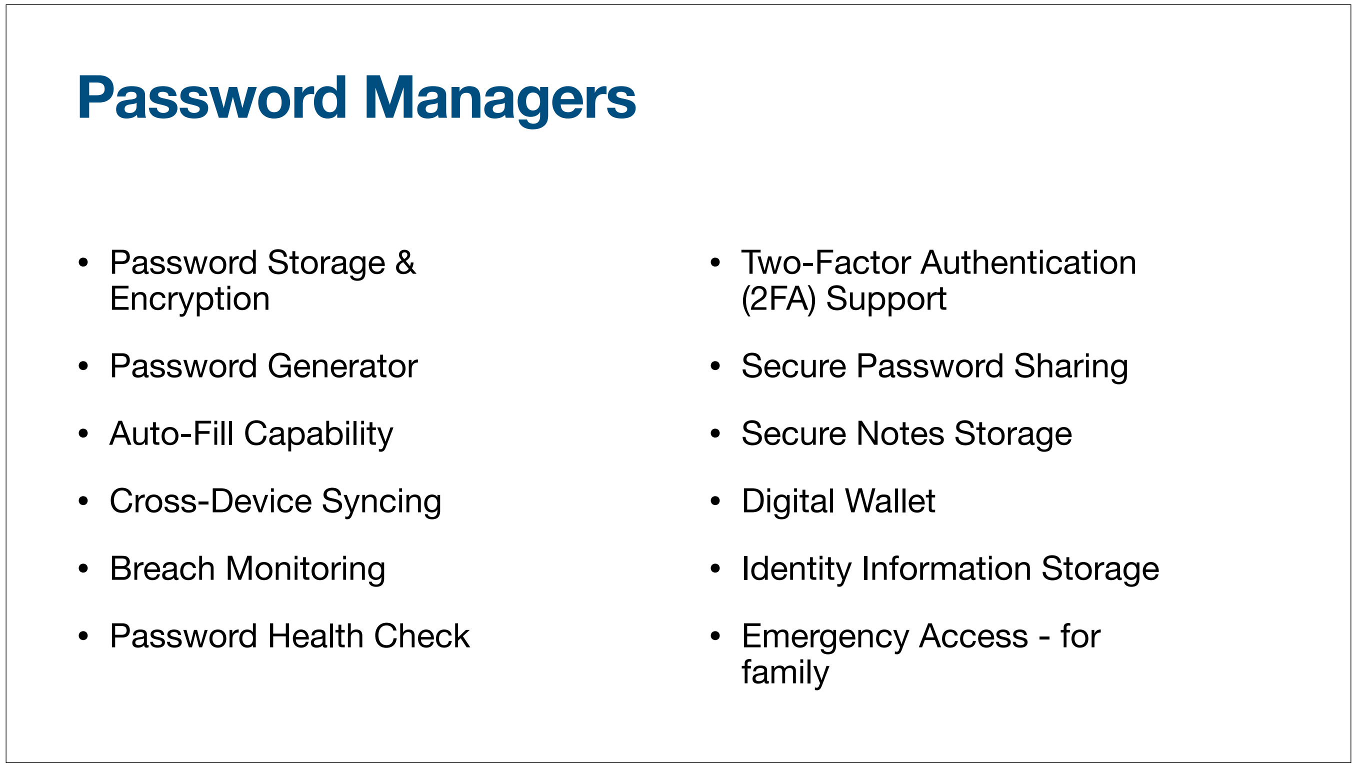
Passkeys can make it super simple to login securely to websites without typing your user name and password. And…it makes everything more secure because the website no longer needs your password.

Cover this more in the Windows and Mac sessions.

How many people use a password manager?

What do you use?

How religious are you about using it?



Password Managers

- Password Storage & Encryption
- Password Generator
- Auto-Fill Capability
- Cross-Device Syncing
- Breach Monitoring
- Password Health Check
- Two-Factor Authentication (2FA) Support
- Secure Password Sharing
- Secure Notes Storage
- Digital Wallet
- Identity Information Storage
- Emergency Access - for family

Built-in to Safari, Chrome, Edge browsers

Passwords app on iOS and Mac

The password manager built-in to the browser work well, as long as you just login to websites. If you use apps as well, they do not work there. That requires a stand-along password manager.

We will cover this more in the upcoming sessions, as this is a critical piece to configuring your devices.

Go through all of your accounts
Add them to your password managers
Change passwords to unique passwords, managed by password manager

Make sure MFA is enabled on your email

Show flow of entering passwords into manager to ensure data is captured

If you have multi-platforms, you need 1Password

We're at the finish line for the information part of the course.

The next sessions are about making sure you can put it to use.

This is new ground. Not sure how this will pan-out, but if we can make sure:
- Settings and config
- Using password management

We'll be in a pretty good place.

How many are coming to each day?

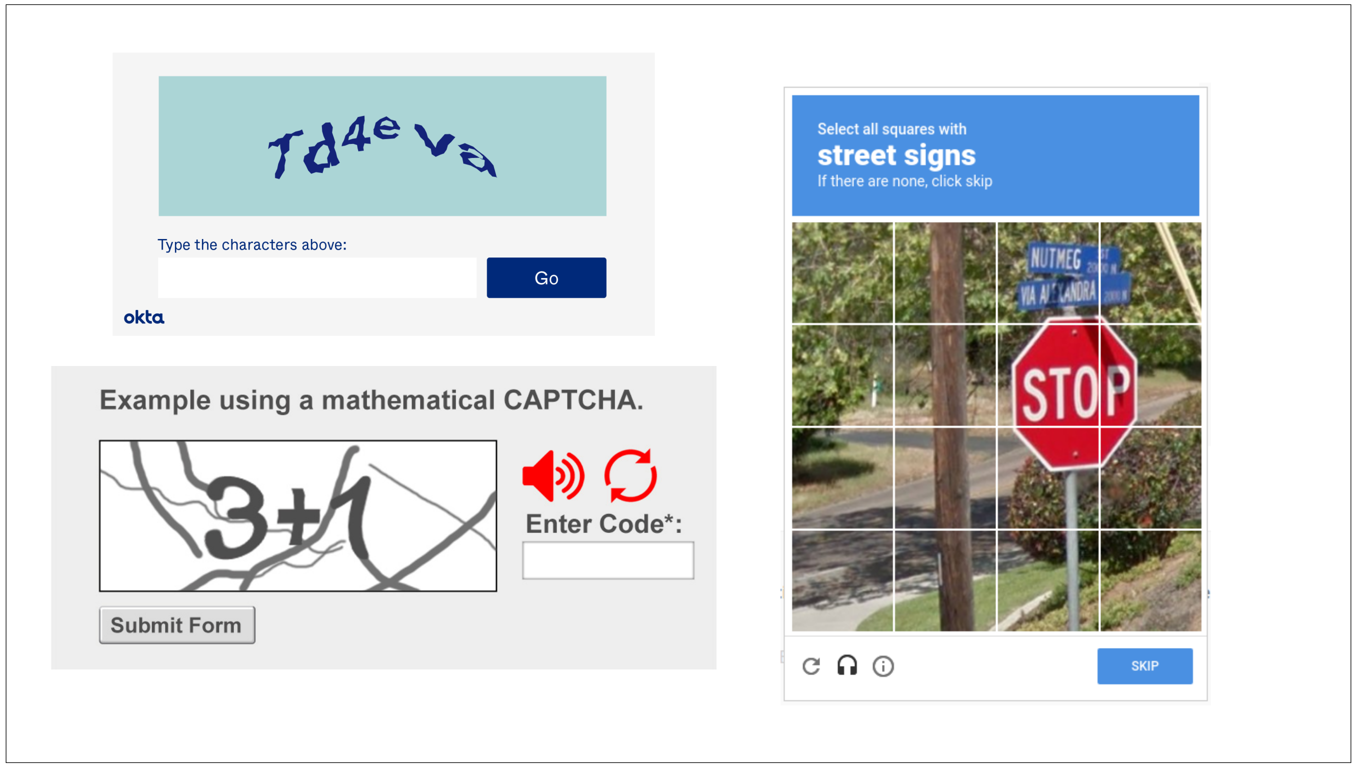
What devices will you bring?

How do you know if you your accounts have been compromised.

You might not.

But this site can provide some level of confirmation, and details where your account information has surfaced.

Let’s take a look.



Type the characters above:

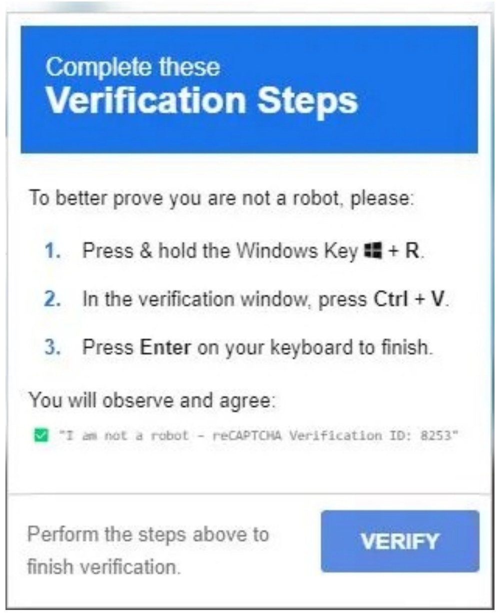
Example using a mathematical CAPTCHA.

Enter Code*:

Select all squares with **street signs**

If there are none, click skip

Why do captchas exist?
Why do we need to prove we are human?



Complete these

Verification Steps

To better prove you are not a robot, please:

1. Press & hold the Windows Key ⊞ + R.
2. In the verification window, press **Ctrl** + **V**.
3. Press **Enter** on your keyboard to finish.

You will observe and agree:

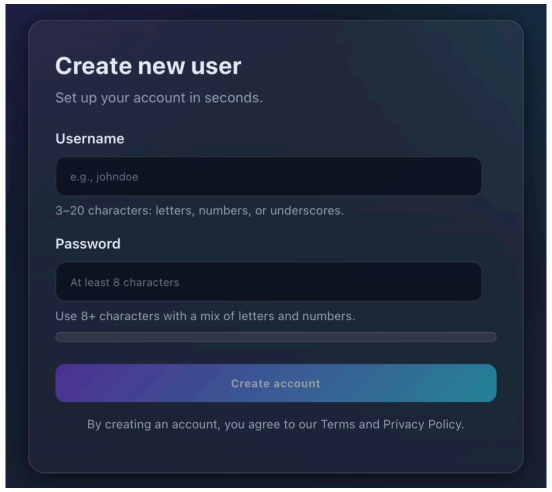
☑ "I am not a robot - reCAPTCHA Verification ID: 8253"

Perform the steps above to finish verification.

What if we get this as a CAPTCHA?

What does Windows+R do?
What does Ctrl+V do?

What happens when you create an account?



Create new user

Set up your account in seconds.

Username

3–20 characters: letters, numbers, or underscores.

Password

Use 8+ characters with a mix of letters and numbers.

By creating an account, you agree to our Terms and Privacy Policy.

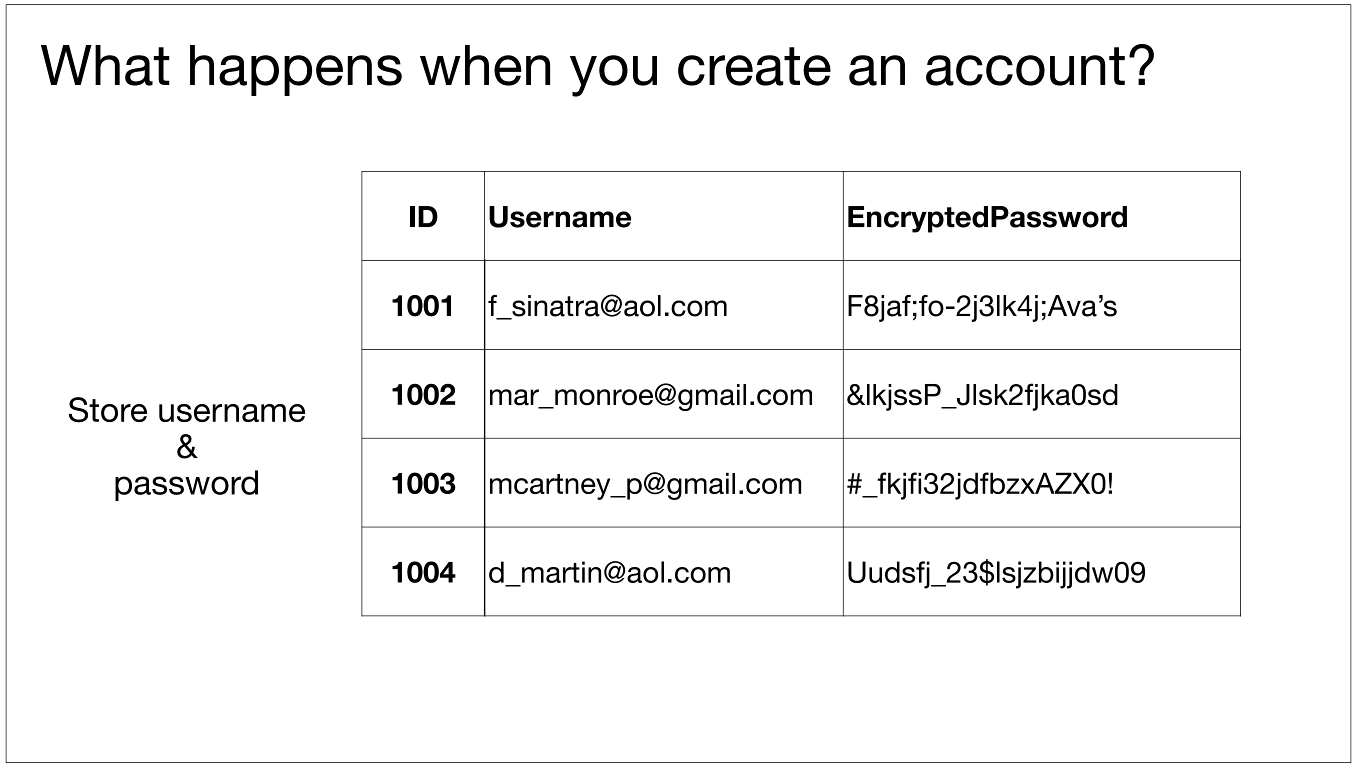
Check Rules

Store username
&
password

What happens when you create an account?

Store username
&
password

ID	Username	Password
1001	f_sinatra@aol.com	OldBlueEyes
1002	mar_monroe@gmail.com	SomeLikeItHot
1003	mcartney_p@gmail.com	BeatleMania!
1004	d_martin@aol.com	ThatsAmore6000

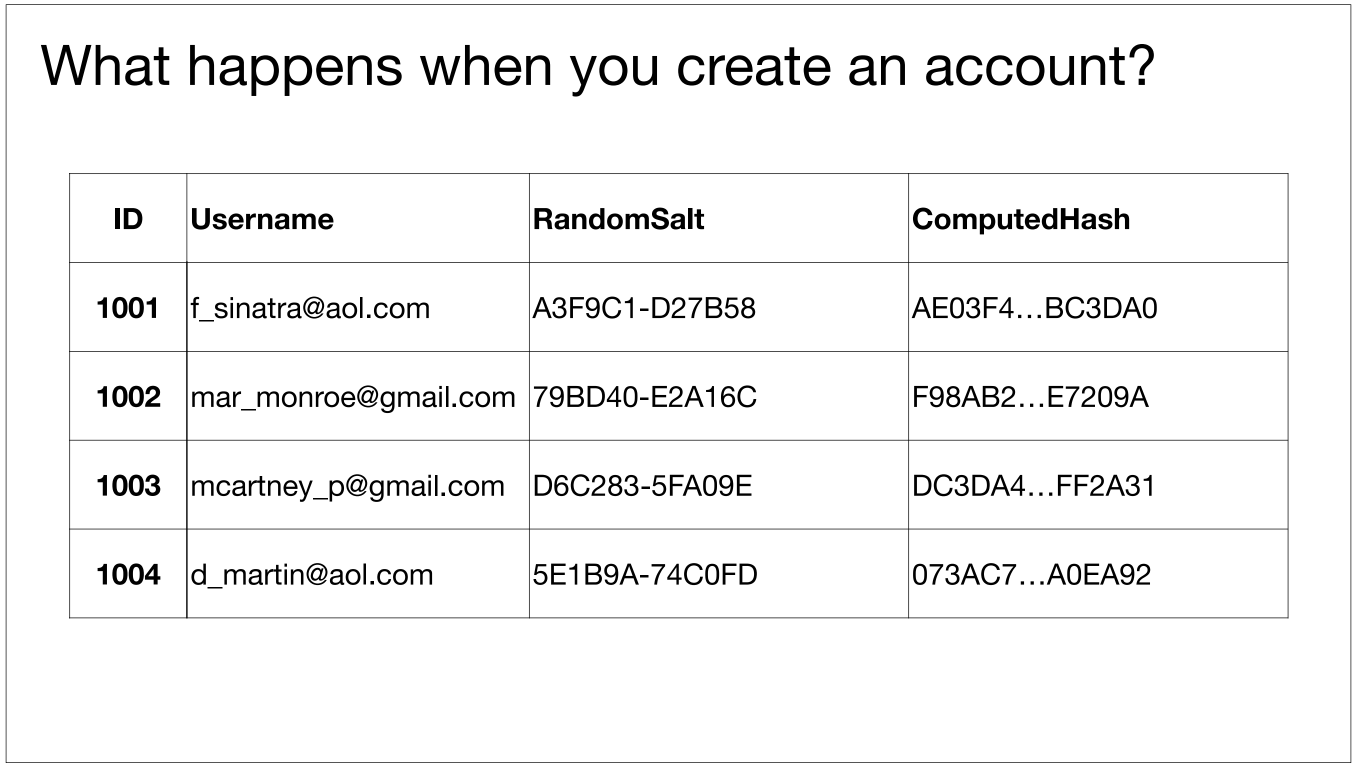


What happens when you create an account?

Store username
&
password

ID	Username	EncryptedPassword
1001	f_sinatra@aol.com	F8jaf;fo-2j3lk4j;Ava’s
1002	mar_monroe@gmail.com	&lkjssP_Jlsk2fjka0sd
1003	mcartney_p@gmail.com	#_fkjfi32jdfbzxAZX0!
1004	d_martin@aol.com	Uudsfj_23$lsjzbijjdw09

But encryption can be reversed
If the encryption key is found out, the entire password list could be vulnerable

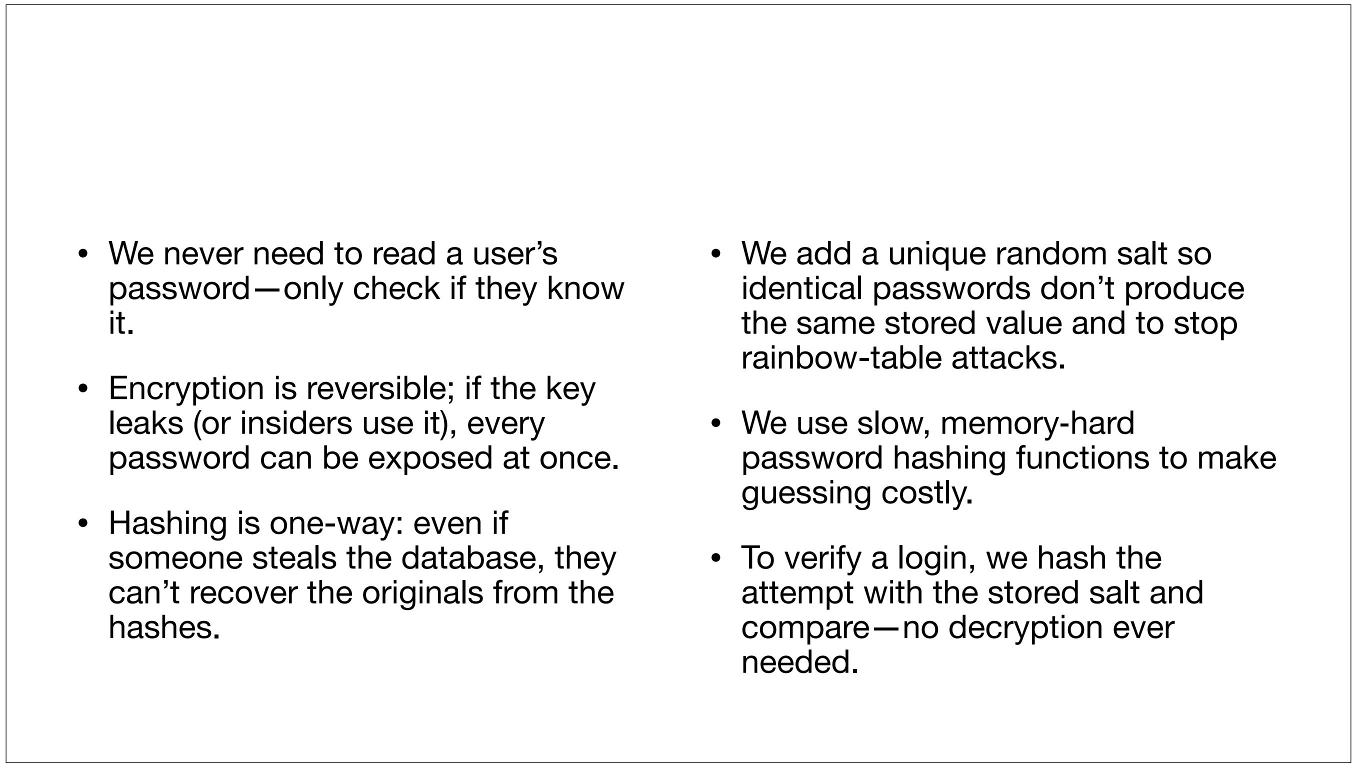


What happens when you create an account?

ID	Username	RandomSalt	ComputedHash
1001	f_sinatra@aol.com	A3F9C1-D27B58	AE03F4…BC3DA0
1002	mar_monroe@gmail.com	79BD40-E2A16C	F98AB2…E7209A
1003	mcartney_p@gmail.com	D6C283-5FA09E	DC3DA4…FF2A31
1004	d_martin@aol.com	5E1B9A-74C0FD	073AC7…A0EA92

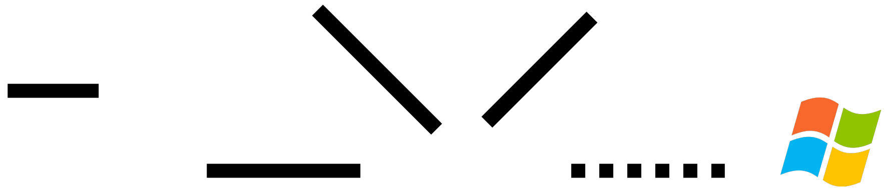
Hashing

- **Deterministic**
  - Same data in will result in same hash…always!
- **Quick**
- **Irreversible**
  - Designed to make it impossible to reverse and recreate the original input.



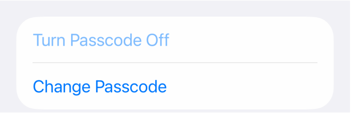
- We never need to read a user’s password—only check if they know it.
- Encryption is reversible; if the key leaks (or insiders use it), every password can be exposed at once.
- Hashing is one-way: even if someone steals the database, they can’t recover the originals from the hashes.
- We add a unique random salt so identical passwords don’t produce the same stored value and to stop rainbow-table attacks.
- We use slow, memory-hard password hashing functions to make guessing costly.
- To verify a login, we hash the attempt with the stored salt and compare—no decryption ever needed.

Typical Home Network



Settings -> Face ID & Passcode

Set Passcode to 6 or more letters and numbers

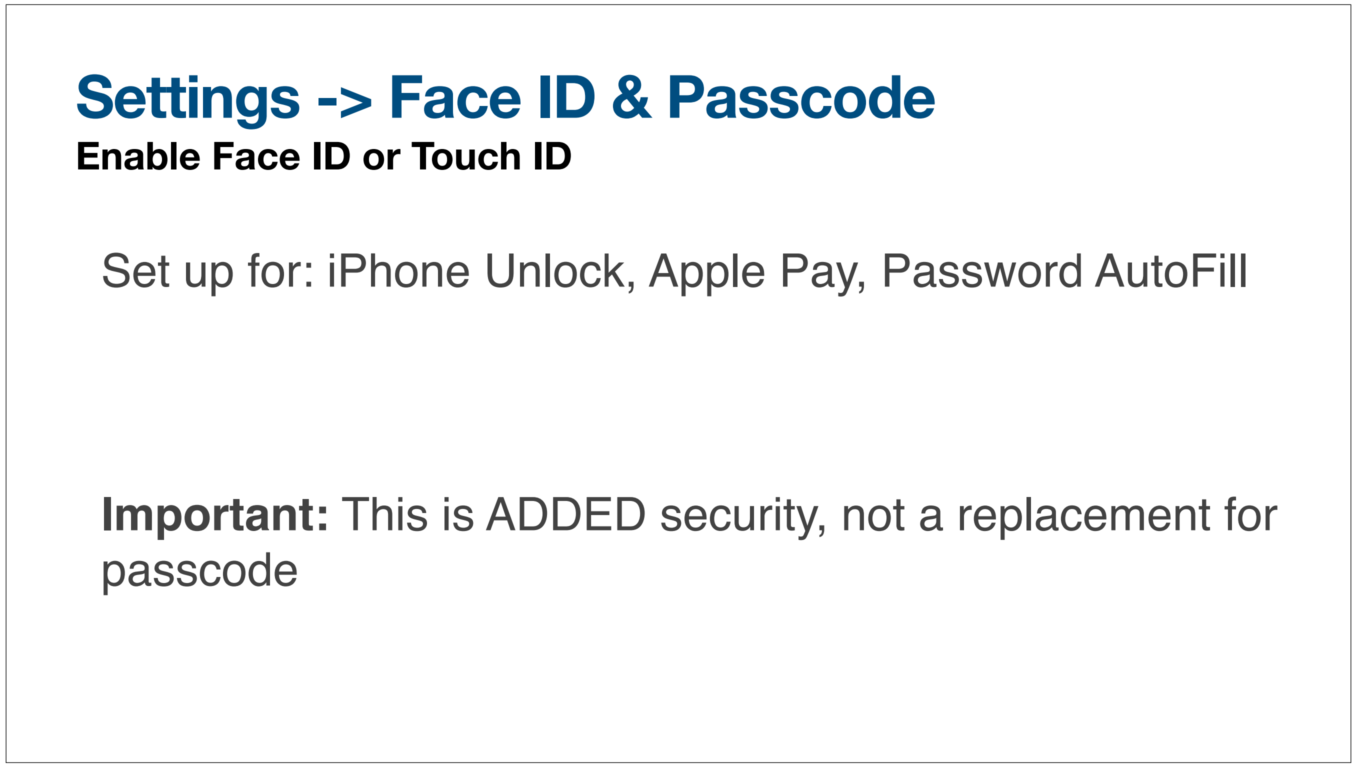


Turn Passcode Off

Change Passcode

1. **Set a Strong Passcode**
   - Tap "Change Passcode" - Tap “Passcode Options” if needed
   - Choose "Custom Alphanumeric Code" for strongest security
   - **Best Practice:** Use at least 8 characters mixing letters and numbers

Or Touch ID & Passcode if phone doesn’t use Face ID



Settings -> Face ID & Passcode

Enable Face ID or Touch ID

Set up for: iPhone Unlock, Apple Pay, Password AutoFill

Important: This is ADDED security, not a replacement for passcode

Settings -> Face ID & Passcode

Disable Lock Screen Access

Turn OFF everything?

Configure Auto-Lock

Settings -> Display & Brightness -> Auto-Lock

Set to: **2 minutes** maximum

Settings → [Your Name] → Sign-In & Security

Enable Two-Factor Authentication (2FA)

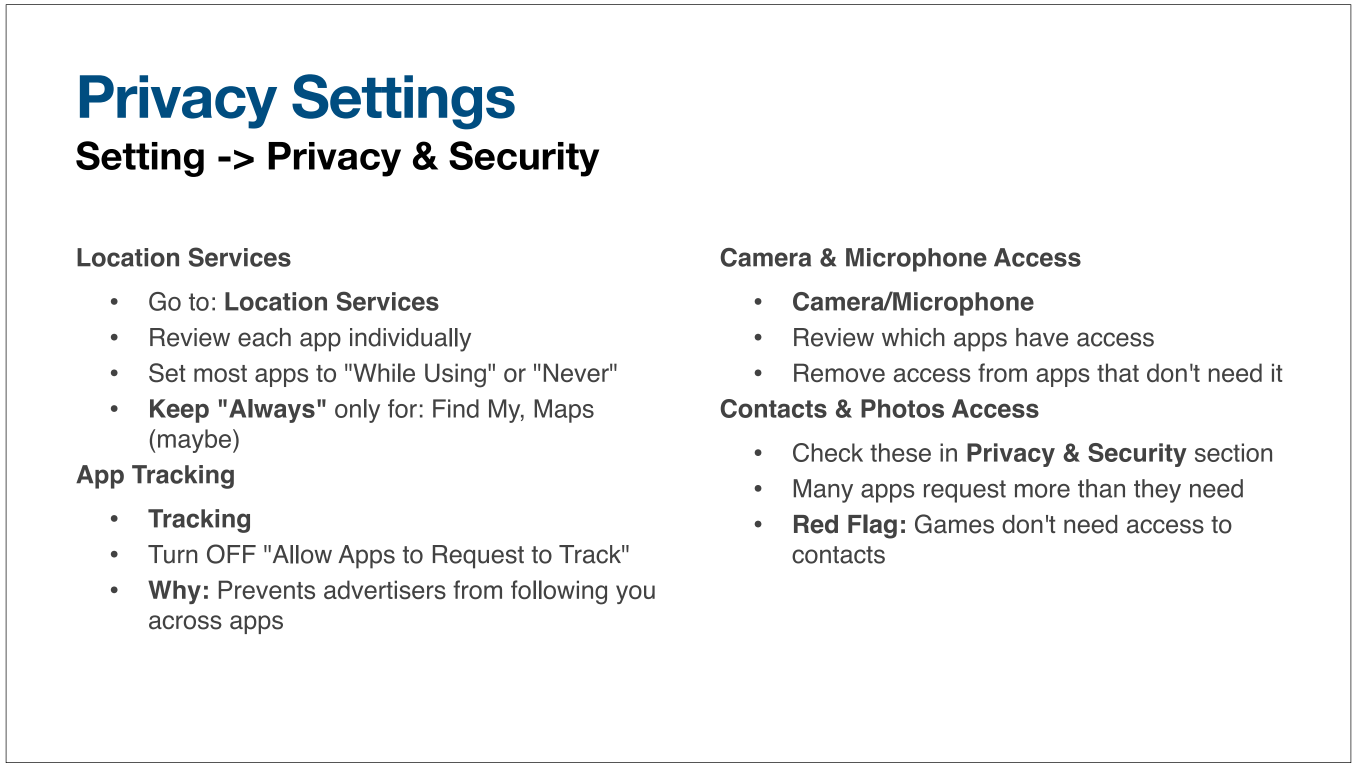
- Tap “Turn On Two-Factor Authentication”
- Add trusted phone number

Settings → [Name] → Sign-In & Security → Account Recovery

Setup Recovery Contact

- Add a trusted family member or friend

- Also consider setting up Legacy Contact



Privacy Settings

Setting -> Privacy & Security

Location Services

- Go to: **Location Services**
- Review each app individually
- Set most apps to "While Using" or "Never"
- **Keep "Always"** only for: Find My, Maps (maybe)

App Tracking

- **Tracking**
- Turn OFF "Allow Apps to Request to Track"
- **Why:** Prevents advertisers from following you across apps

Camera & Microphone Access

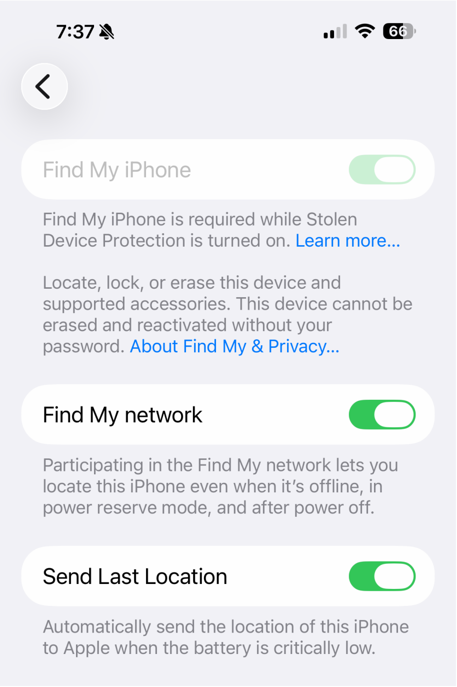
- **Camera/Microphone**
- Review which apps have access
- Remove access from apps that don't need it

Contacts & Photos Access

- Check these in **Privacy & Security** section
- Many apps request more than they need
- **Red Flag:** Games don't need access to contacts

Enable Find My iPhone

Settings -> [Name] -> Find My



7:37

Find My iPhone

Find My iPhone is required while Stolen Device Protection is turned on. Learn more...

Locate, lock, or erase this device and supported accessories. This device cannot be erased and reactivated without your password. About Find My & Privacy...

Find My network

Participating in the Find My network lets you locate this iPhone even when it's offline, in power reserve mode, and after power off.

Send Last Location

Automatically send the location of this iPhone to Apple when the battery is critically low.

Settings->General->Software Update->Auto

Enable Automatic Updates

- Turn on both download and install updates

Safari Privacy Settings

Settings->Apps->Safari

- Turn ON:
  - ✅ Prevent Cross-Site Tracking
  - ✅ Hide IP Address (choose "Trackers and Websites")
  - ✅ Fraudulent Website Warning

Mac Security

A. Account Security

1. **Require Password After Sleep**
   - **System Settings** → **Lock Screen**
   - Set "Require password after screen saver begins or display is turned off" to **Immediately**
2. **Enable FileVault Encryption**
   - **System Settings** → **Privacy & Security** → **FileVault**
   - Click "Turn On FileVault"
   - **Save recovery key somewhere safe** (write it down!)
   - **Why:** Encrypts entire hard drive; useless to thieves
3. **Firmware Password** (Intel Macs)
   - More advanced; discuss with IT helper if concerned
   - Prevents booting from external drives

B. System Security

4. **Keep macOS Updated**
   - **System Settings** → **General** → **Software Update**
   - Enable "Automatically keep my Mac up to date"
   - Check all boxes below it
5. **Firewall**
   - **System Settings** → **Network** → **Firewall**
   - Turn ON
   - Click "Options" → Block all incoming connections when needed
6. **Gatekeeper Settings**
   - **System Settings** → **Privacy & Security**
   - Under "Security," set "Allow applications downloaded from:" to **App Store and identified developers**
   - **Never** change to "Anywhere"

C. Privacy

7. **Review App Permissions**
   - **System Settings** → **Privacy & Security**
   - Check each category (Camera, Microphone, Files and Folders, etc.)
   - Remove apps that don't need access
8. **Safari Settings** (same as iOS)
   - **Safari** → **Settings** → **Privacy**
   - Enable "Prevent cross-site tracking"
   - Enable "Hide IP address"

Screen Lock

Settings -> Security -> Screen Lock

Recommended: 6-digit PIN (easier than pattern, more secure than 4-digit)

Avoid: Face unlock only, patterns (can be seen/guessed)

Write your PIN down and keep it in a safe place at home

Lock Screen Timeout

Settings -> Display -> Screen Timeout

Set to: 1-2 minutes maximum

Prevents others from accessing if you set it down

Prevents accidentally triggering an action (phone call, etc.)

Lock Screen Notifications

Settings -> Notifications -> Lock Screen

Set to: "Hide sensitive content"

Prevents others from reading your texts/emails when locked

Google Play Protect

Google Play Store -> Profile Icon -> Play Protect

Turn ON: Scan apps with Play Protect

Automatically scans for malicious apps

App Installation Security

Settings -> Security -> Install unknown apps

Verify ALL apps show "Not allowed"

Only allows apps from official Google Play Store

Anyone have an
app that is
allowed?

App Permissions Review

Settings -> Privacy -> Permission Manager

Review these permissions:

- **Location**: Only apps that NEED it (Maps, Weather)
- **Camera**: Only camera and video apps
- **Microphone**: Only calling and recording apps
- **Contacts**: Only communication apps

Set others to "Don't allow" or "Ask every time"

Two-Factor Authentication

Settings -> Google -> Manage your Google Account -> Security

Turn ON: 2-Step Verification

Use your phone number for backup codes

Even if someone has your password, they can't get in to your account

Recovery Information

Settings -> Google -> Manage your Google Account -> Security

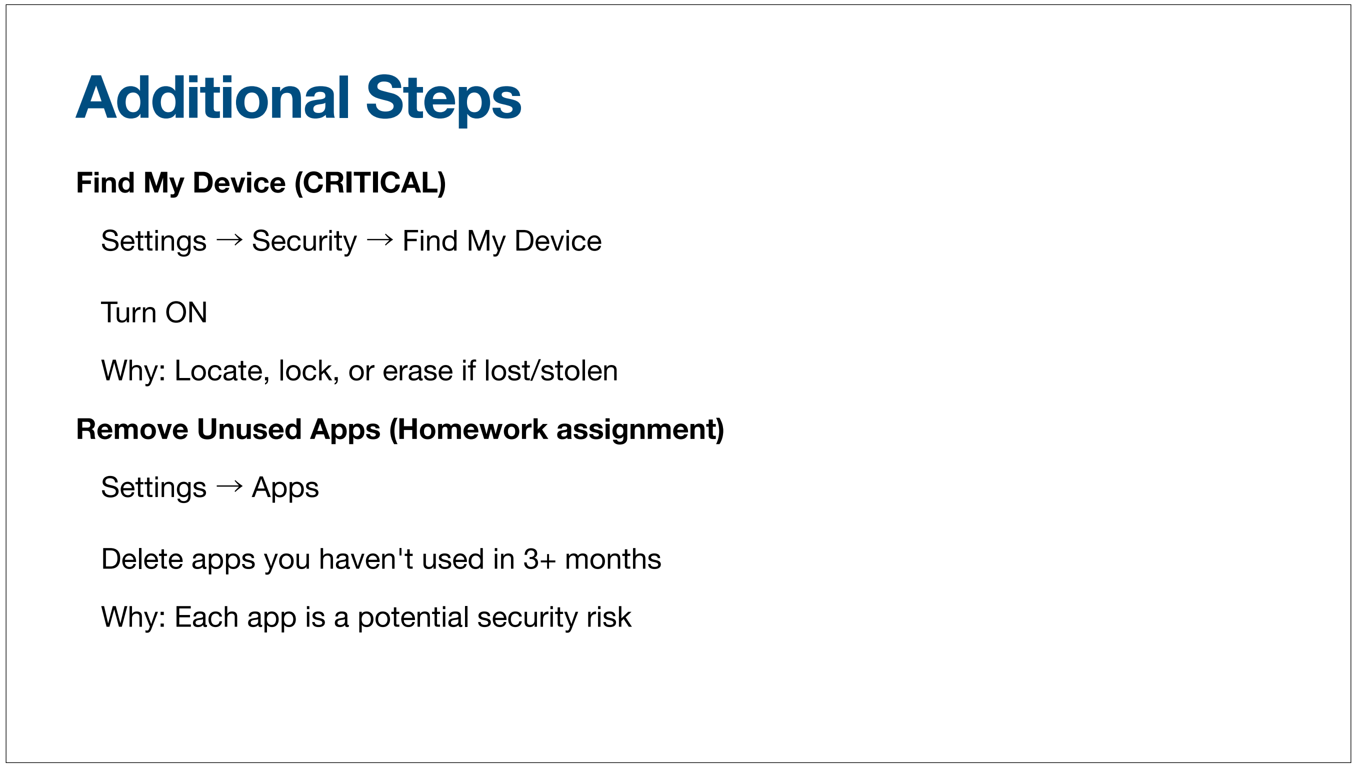
Add: Recovery phone number AND recovery email

Critical if you're locked out

Security Checkup

Google Account -> Security -> Security Checkup

Complete all recommended actions



Additional Steps

Find My Device (CRITICAL)

Settings → Security → Find My Device

Turn ON

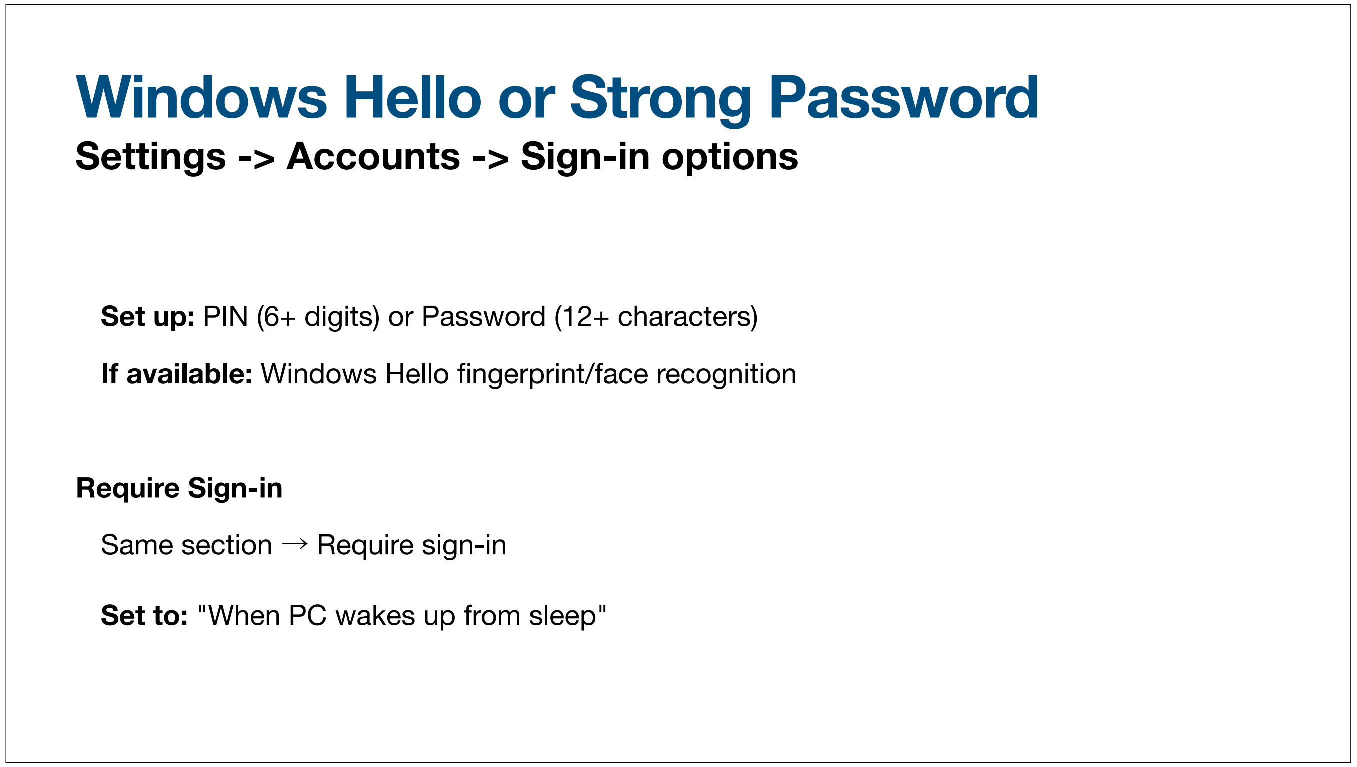
Why: Locate, lock, or erase if lost/stolen

Remove Unused Apps (Homework assignment)

Settings → Apps

Delete apps you haven't used in 3+ months

Why: Each app is a potential security risk



Windows Hello or Strong Password

Settings -> Accounts -> Sign-in options

Set up: PIN (6+ digits) or Password (12+ characters)

If available: Windows Hello fingerprint/face recognition

Require Sign-in

Same section → Require sign-in

Set to: "When PC wakes up from sleep"

Account Type Verification

Settings -> Accounts -> Your Info

Verify: Using Microsoft Account (not local)

Enables cloud backup and recovery

Windows Security Check

Search for “Windows Security” -> Open

Check all areas show green checkmarks:

Virus & threat protection: ON

Firewall & network protection: ON

App & browser control: ON

Real-time Protection

Windows Security -> Virus & threat protection

Verify: Real-time protection is ON

Turn ON: Cloud-delivered protection

Firewall Verification

Windows Security -> Firewall & network protection

All networks should show: "Firewall is on"

SmartScreen

Windows Security -> App & browser control

Set all to: Warn or Block

Automatic Updates

Settings -> Windows Update

Turn ON: Get the latest updates as soon as they're available

Uninstall Unnecessary Software

Settings -> Apps -> Installed apps

Remove: Trial software, games you don't play, toolbars

Don't remove anything from Microsoft or your PC manufacturer

Microsoft Account Security

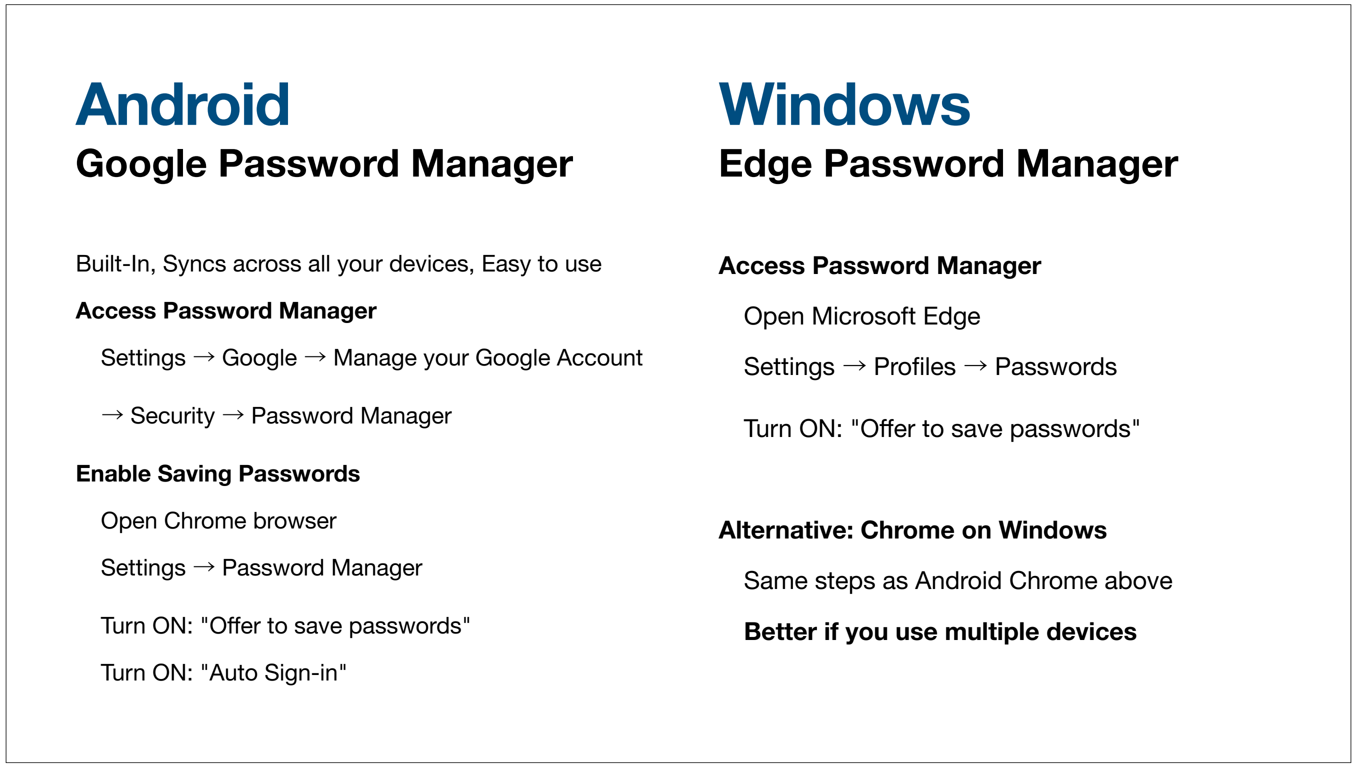
Navigate to account.microsoft.com -> Security

Click: Manage how I sign in

Turn ON: Two-step verification

Add recovery information

Passwordless
account?



Android

Google Password Manager

Built-In, Syncs across all your devices, Easy to use

Access Password Manager

Settings → Google → Manage your Google Account

→ Security → Password Manager

Enable Saving Passwords

Open Chrome browser

Settings → Password Manager

Turn ON: "Offer to save passwords"

Turn ON: "Auto Sign-in"

Windows

Edge Password Manager

Access Password Manager

Open Microsoft Edge

Settings → Profiles → Passwords

Turn ON: "Offer to save passwords"

Alternative: Chrome on Windows

Same steps as Android Chrome above

Better if you use multiple devices

Add your First Password

Go to a website you use (e.g., your bank)

Log in with your current password

When prompted "Save password?" → **Click YES**

Password is now saved!

Viewing Your Passwords

Android:

Go to passwords.google.com

Verify your identity (fingerprint/PIN)

See all saved passwords

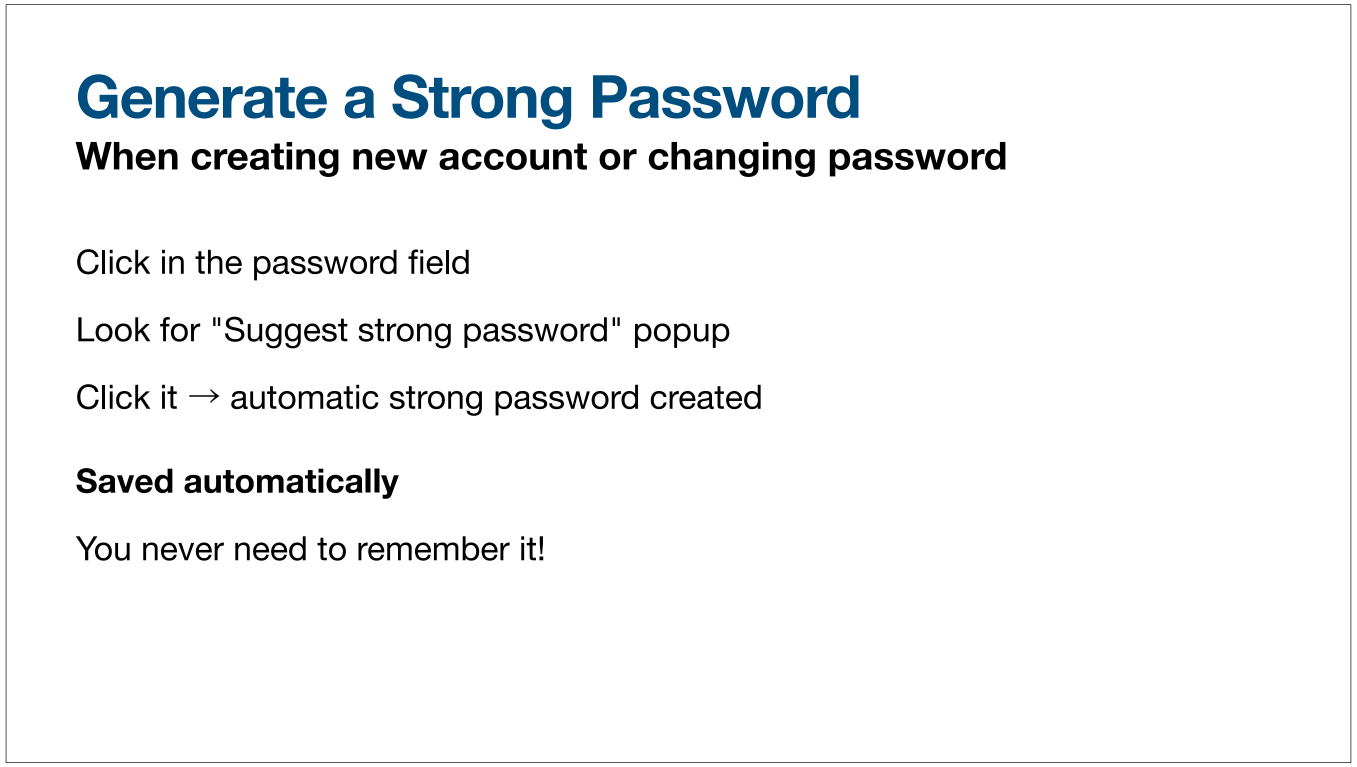
Click any password → Eye icon to view

Windows/Edge:

Edge → Settings → Profiles → Passwords

See all saved passwords

Click eye icon to reveal



Generate a Strong Password

When creating new account or changing password

Click in the password field

Look for "Suggest strong password" popup

Click it → automatic strong password created

Saved automatically

You never need to remember it!