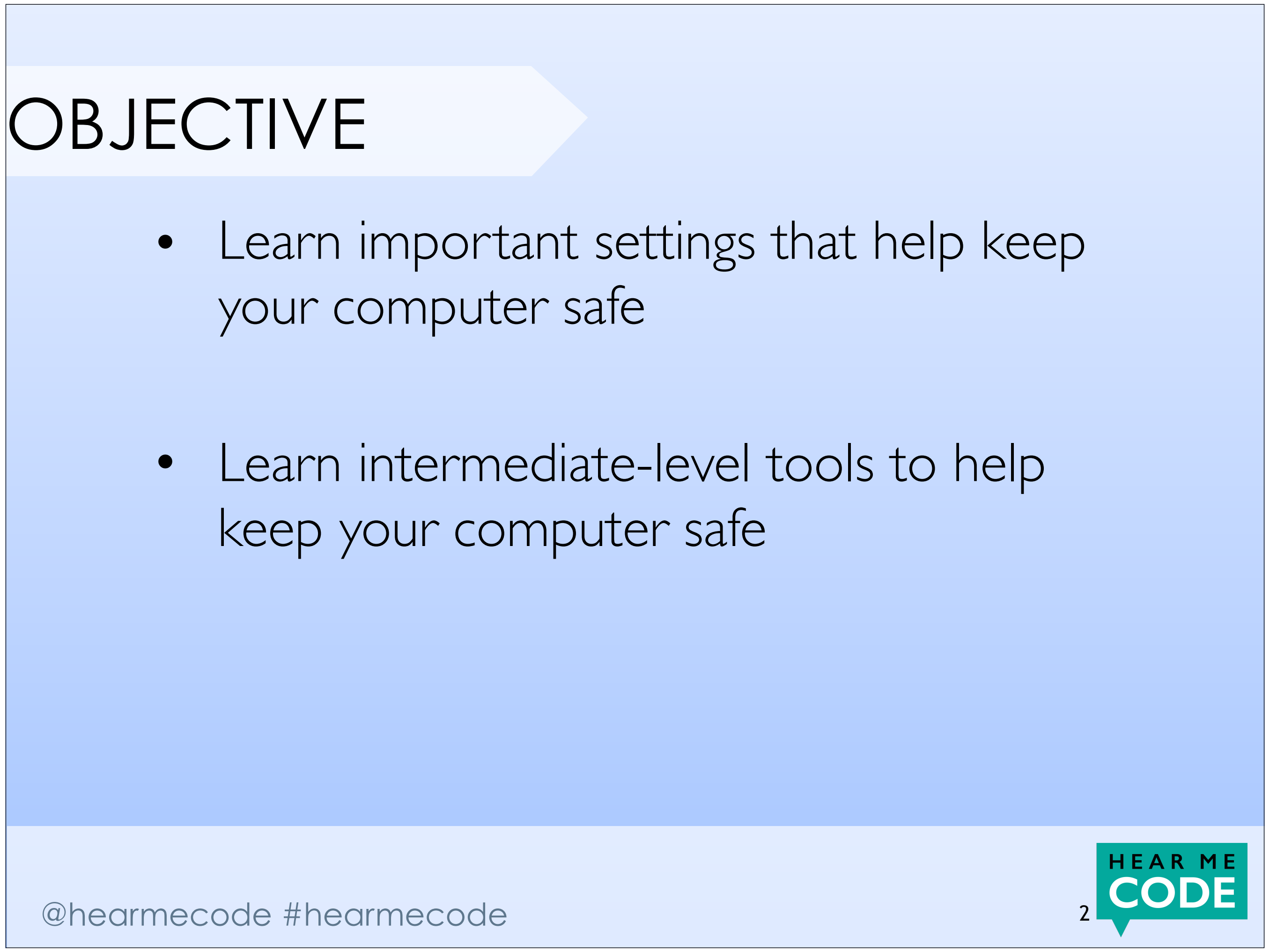
DIGITAL SECURITY IS FOR EVERYONE
PART TWO

Shannon Turner

Twitter: @svthmc



OBJECTIVE

- Learn important settings that help keep your computer safe
- Learn intermediate-level tools to help keep your computer safe

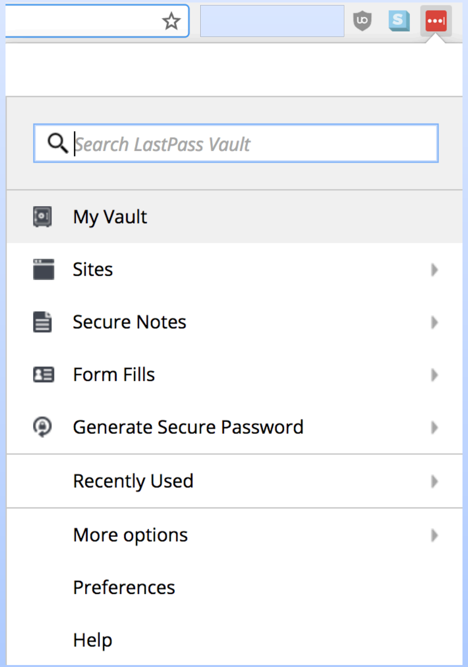
This training is a continuation of the Security is for Everyone introductory training. If you haven’t taken Part One, you should take Part One first. As a reminder, we will cover the most common threats and how you can protect yourself.

OUTLINE

1. Getting the most out of LastPass
2. Configuring your computer’s firewall
3. Encrypting your computer’s hard drive
4. Encrypting your phone’s hard drive
5. Browser extensions to keep you safer
6. Keeping safe when connecting to public WiFi
7. Using anti-virus software

GETTING THE MOST OUT OF LAST PASS

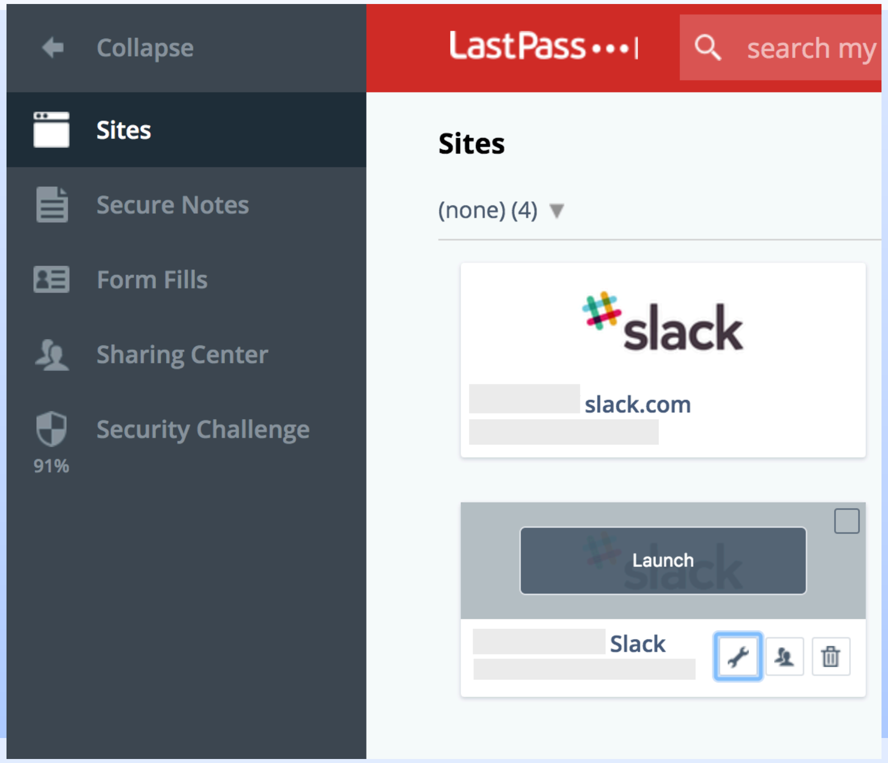
GET THE MOST FROM LAST PASS



We're going to assume you've installed the LastPass browser extension in these slides; if you have not installed LastPass or created an account yet, you'll want to review Security is for Everyone Part One before continuing.

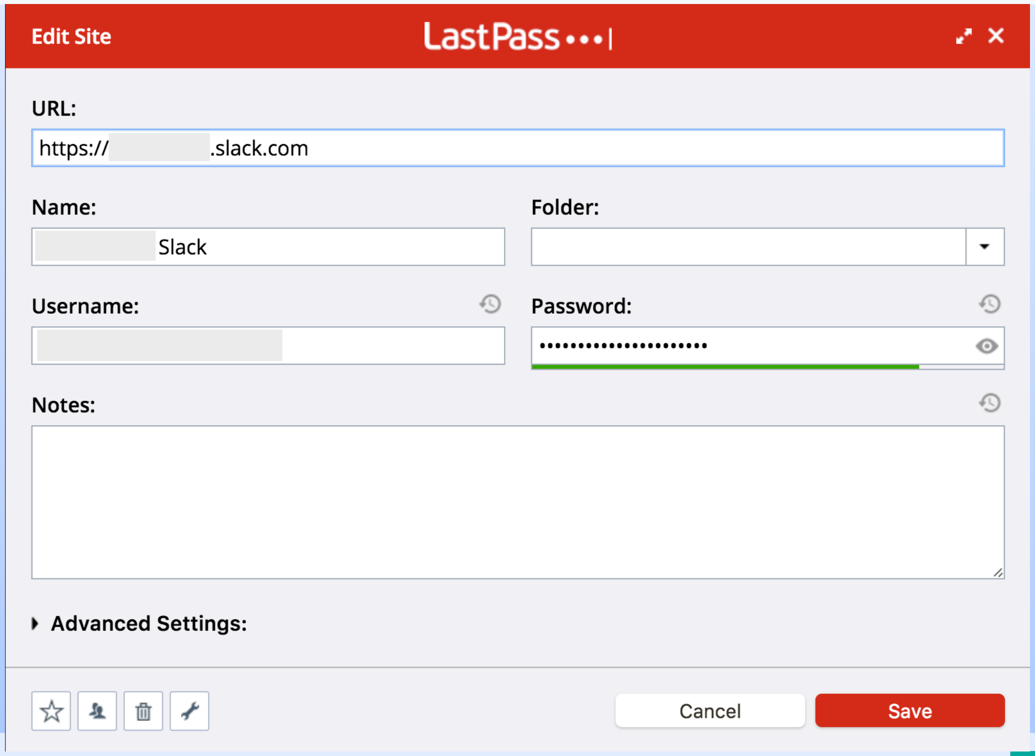
In your browser, click the LastPass logo to bring up the menu, then go to My Vault.

WEBSITE LOGINS YOU'VE SAVED



Your Vault is where all of your data is stored, including all of the sites where you've saved passwords and secure notes like two-factor authentication recovery codes. Go to sites to view all of the sites where you've saved passwords. Here, they're organized by which folder I've stored them in. Click on the wrench to see and edit that site's details.

EDITING A SAVED WEBSITE



Edit Site

LastPass •••|

URL: https://[redacted].slack.com

Name: [redacted] Slack

Folder:

Username: [redacted]

Password: ••••••••••••••••••••••

Notes:

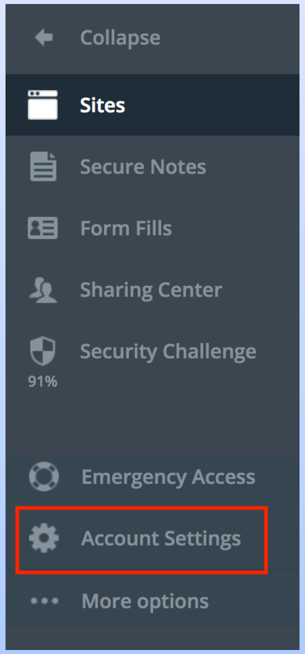
Advanced Settings:

Cancel

Save

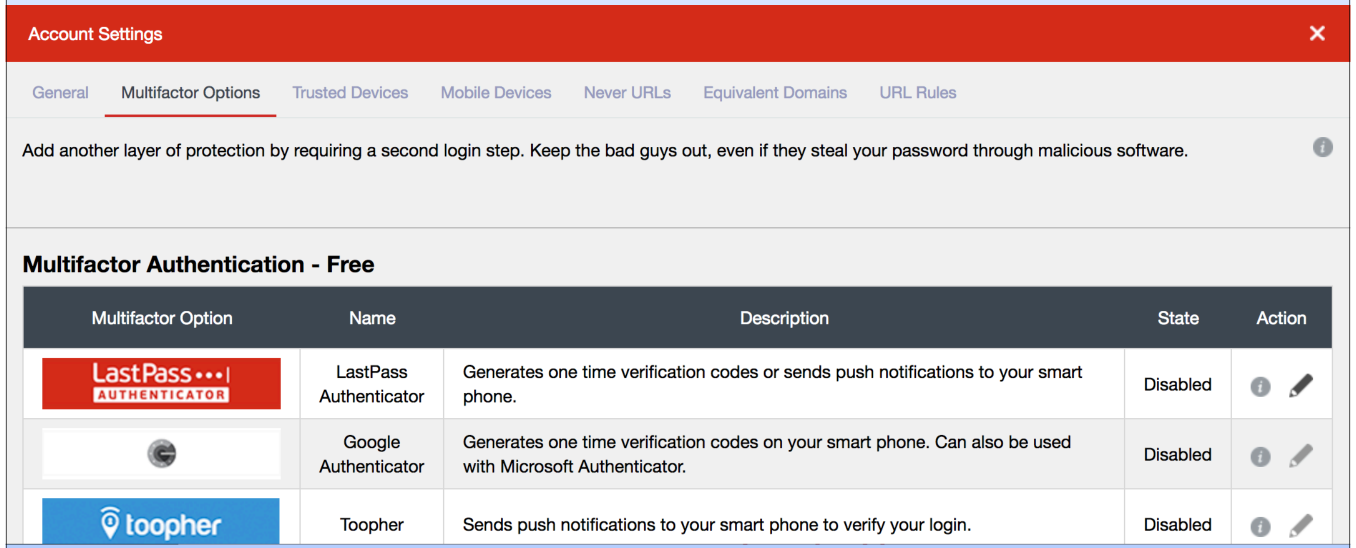
Clicking the wrench on the previous screen opens up a screen where we can edit a website that we have stored. Changing the folder a site is stored in can help you keep your passwords organized. You can also click the "eye" icon to view your password that you have saved with LastPass.

SETTING UP TWO-FACTOR AUTHENTICATION



Setting up two-factor authentication with LastPass takes a few steps. To get started, click the Account Settings from inside your Vault.

SETTING UP TWO-FACTOR AUTHENTICATION



Add another layer of protection by requiring a second login step. Keep the bad guys out, even if they steal your password through malicious software.

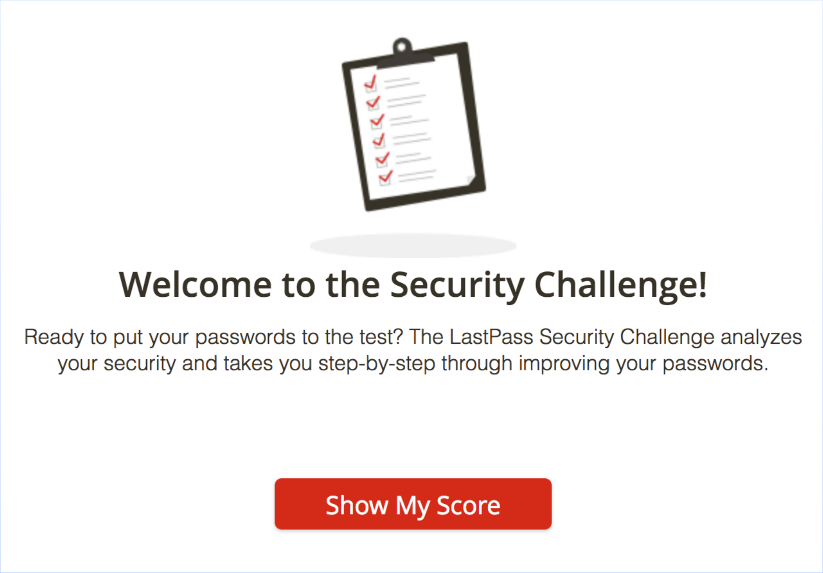
Multifactor Authentication - Free

Multifactor Option	Name	Description	State	Action
LastPass AUTHENTICATOR	LastPass Authenticator	Generates one time verification codes or sends push notifications to your smart phone.	Disabled	
	Google Authenticator	Generates one time verification codes on your smart phone. Can also be used with Microsoft Authenticator.	Disabled	
toopher	Toopher	Sends push notifications to your smart phone to verify your login.	Disabled	

From the Account Settings screen, click Multifactor Options — this is what LastPass calls Two-Factor Authentication.

You have many options, but I would recommend the LastPass Authenticator or the Google Authenticator. Click the pencil and follow the prompts to continue. I won’t show all of the steps here, but it will walk you through it.

LASTPASS SECURITY CHALLENGE

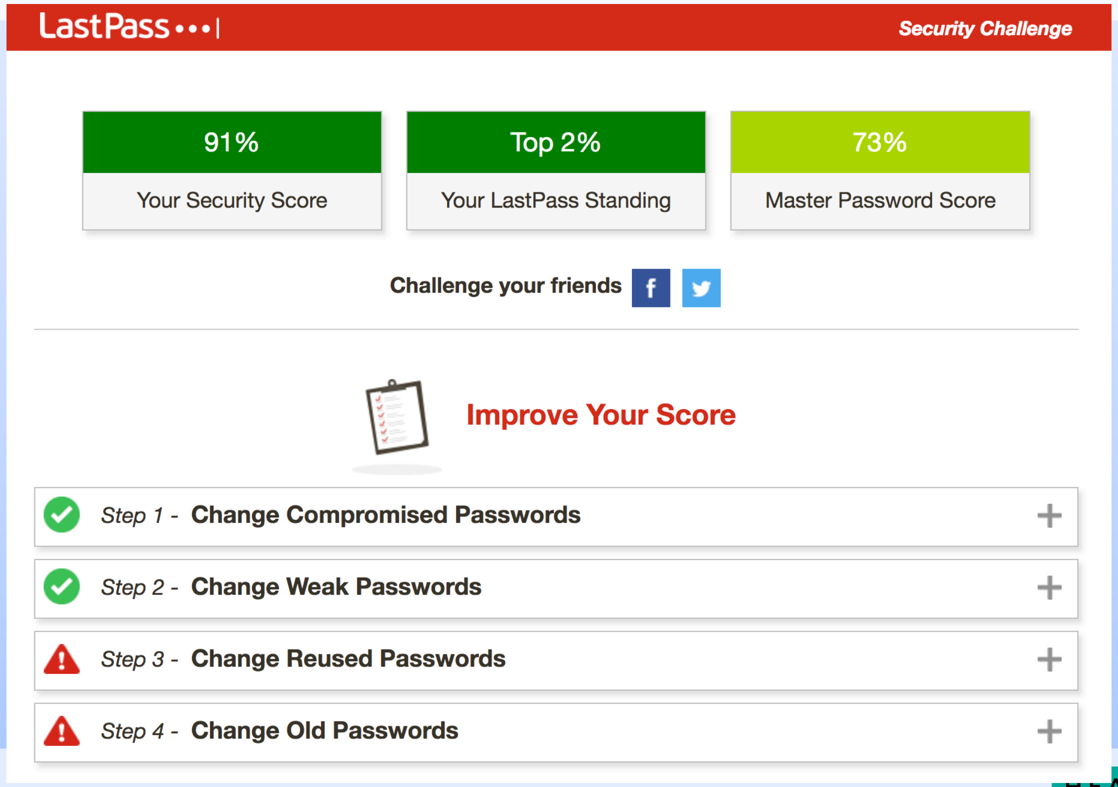


Welcome to the Security Challenge!

Ready to put your passwords to the test? The LastPass Security Challenge analyzes your security and takes you step-by-step through improving your passwords.

The LastPass security challenge will analyze how secure your passwords are and assign you a score. It will then walk you through how to improve your score and the security of your passwords. To get started, click on the Security Challenge button in the menu from your Vault.

LASTPASS SECURITY CHALLENGE



LastPass •••|

Security Challenge

91%	Top 2%	73%
Your Security Score	Your LastPass Standing	Master Password Score

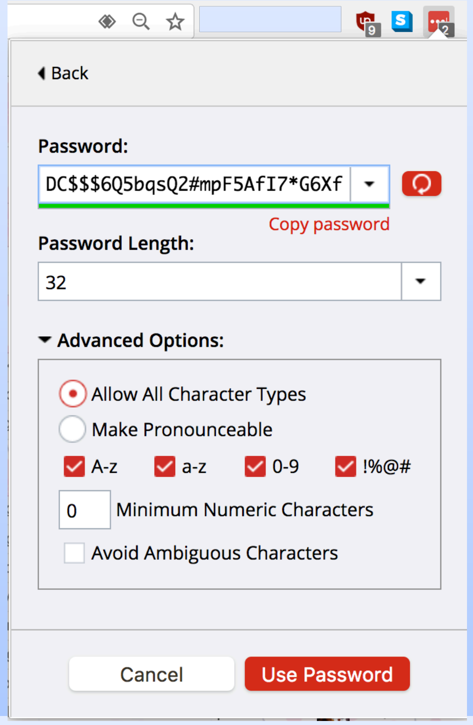
Challenge your friends f

Improve Your Score

- ✓ *Step 1 -* **Change Compromised Passwords** +
- ✓ *Step 2 -* **Change Weak Passwords** +
- ⚠ *Step 3 -* **Change Reused Passwords** +
- ⚠ *Step 4 -* **Change Old Passwords** +

Here's my security challenge - it shows my overall score and how strong my master password is, and gives me tips on what I can do to improve my score. Here, you can see that I have reused some passwords, and some of my passwords are old. If I click on Step 3 or Step 4, it will expand and give me options to improve those.

GENERATING STRONG PASSWORDS



Password: DC$$$6Q5bqsQ2#mpF5AfI7*G6Xf

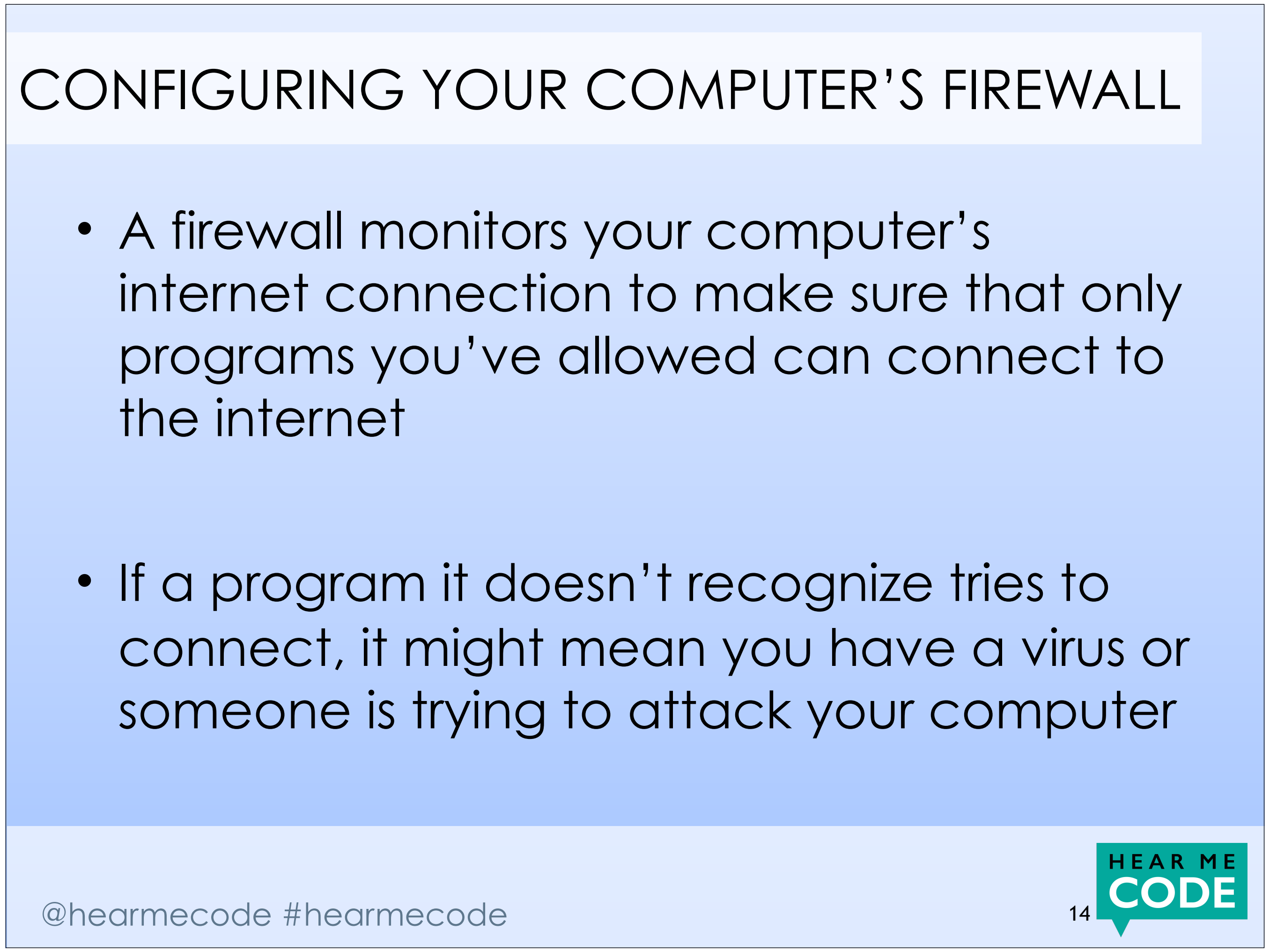
Password Length: 32

Advanced Options:

● Allow All Character Types
○ Make Pronounceable
☑ A-z ☑ a-z ☑ 0-9 ☑ !%@#
0 Minimum Numeric Characters
□ Avoid Ambiguous Characters

You can use LastPass to generate secure passwords, and customize how strong you want the passwords to be. Here, I've created a password that's 32 characters long, with upper and lowercase letters, numbers, and symbols. I wouldn't ever be able to remember this password, but that's okay because LastPass will keep it stored for me. To generate new passwords, click the lock that appears in the password field when you're creating a new account, or click the LastPass icon in your browser and go to "Generate Secure Password."

CONFIGURING YOUR COMPUTER'S FIREWALL

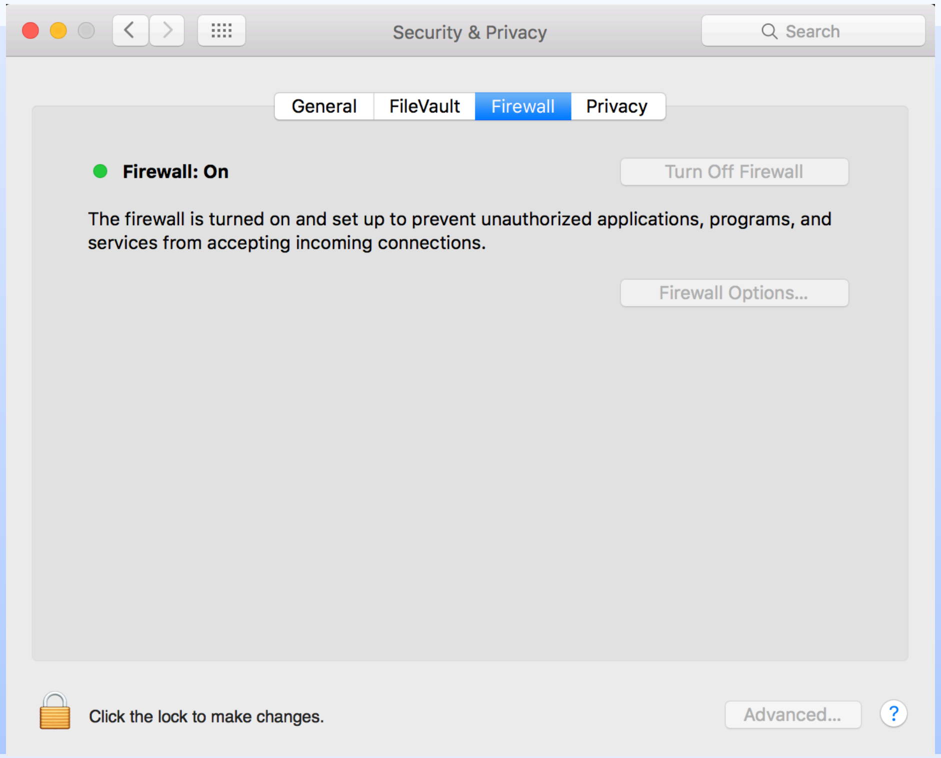


CONFIGURING YOUR COMPUTER'S FIREWALL

- A firewall monitors your computer's internet connection to make sure that only programs you've allowed can connect to the internet
- If a program it doesn't recognize tries to connect, it might mean you have a virus or someone is trying to attack your computer

In other words, a firewall makes sure that in order to connect to the internet, your computer has your permission first. It might ask you for confirmation the first time it sees a program it doesn't recognize. So for example, if I use Spotify to listen to music, the first time I run Spotify, my firewall might ask me if Spotify is allowed to connect to the internet. If I say yes, then the firewall will remember and won't ask me again about Spotify. If I said no, then the firewall will prevent Spotify from connecting to the internet. If you don't recognize the program your firewall asks about or aren't sure, you'll want to deny the request.

CONFIGURING YOUR COMPUTER’S FIREWALL



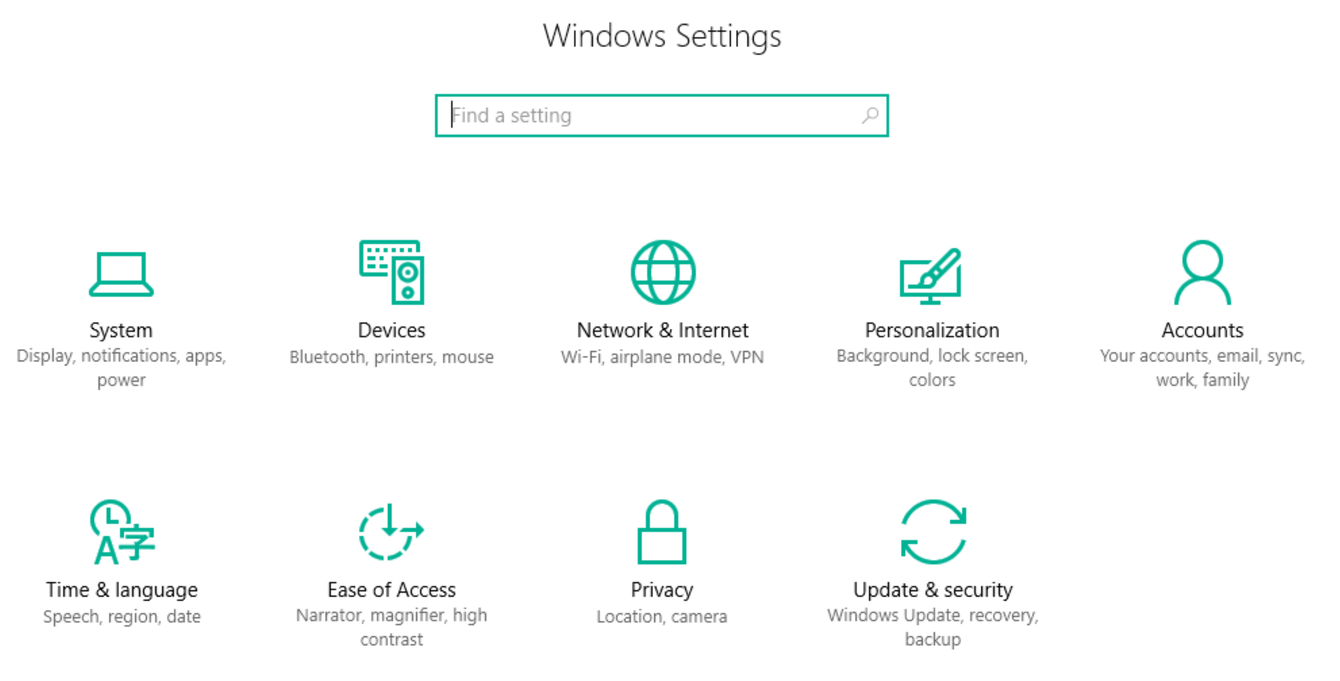
● Firewall: On

The firewall is turned on and set up to prevent unauthorized applications, programs, and services from accepting incoming connections.

Click the lock to make changes.

Here, you can see that I’ve turned on the Firewall on my Mac. To get to this screen, go to the Apple Menu > System Preferences > Security & Privacy (in the top row) and then click the Firewall tab. If your firewall is off, you’ll need to click the lock to make changes, enter your password, and click the button to turn on the firewall.

CONFIGURING YOUR COMPUTER'S FIREWALL



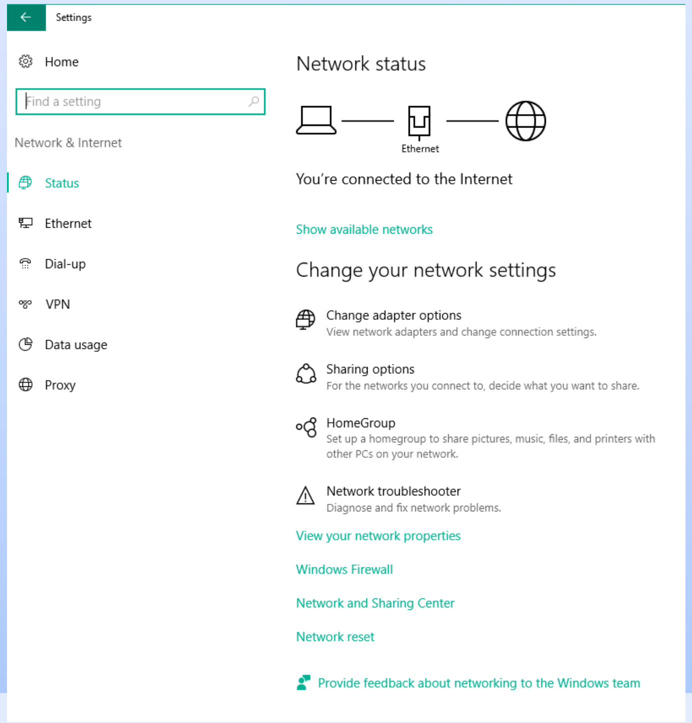
Windows Settings

Find a setting

- System — Display, notifications, apps, power
- Devices — Bluetooth, printers, mouse
- Network & Internet — Wi-Fi, airplane mode, VPN
- Personalization — Background, lock screen, colors
- Accounts — Your accounts, email, sync, work, family
- Time & language — Speech, region, date
- Ease of Access — Narrator, magnifier, high contrast
- Privacy — Location, camera
- Update & security — Windows Update, recovery, backup

On Windows, click the Windows menu, then the small gear icon. This will open the Windows settings. Next, click Network & Internet.

CONFIGURING YOUR COMPUTER'S FIREWALL



Network status

You're connected to the Internet

Show available networks

Change your network settings

Change adapter options
View network adapters and change connection settings.

Sharing options
For the networks you connect to, decide what you want to share.

HomeGroup
Set up a homegroup to share pictures, music, files, and printers with other PCs on your network.

Network troubleshooter
Diagnose and fix network problems.

View your network properties

Windows Firewall

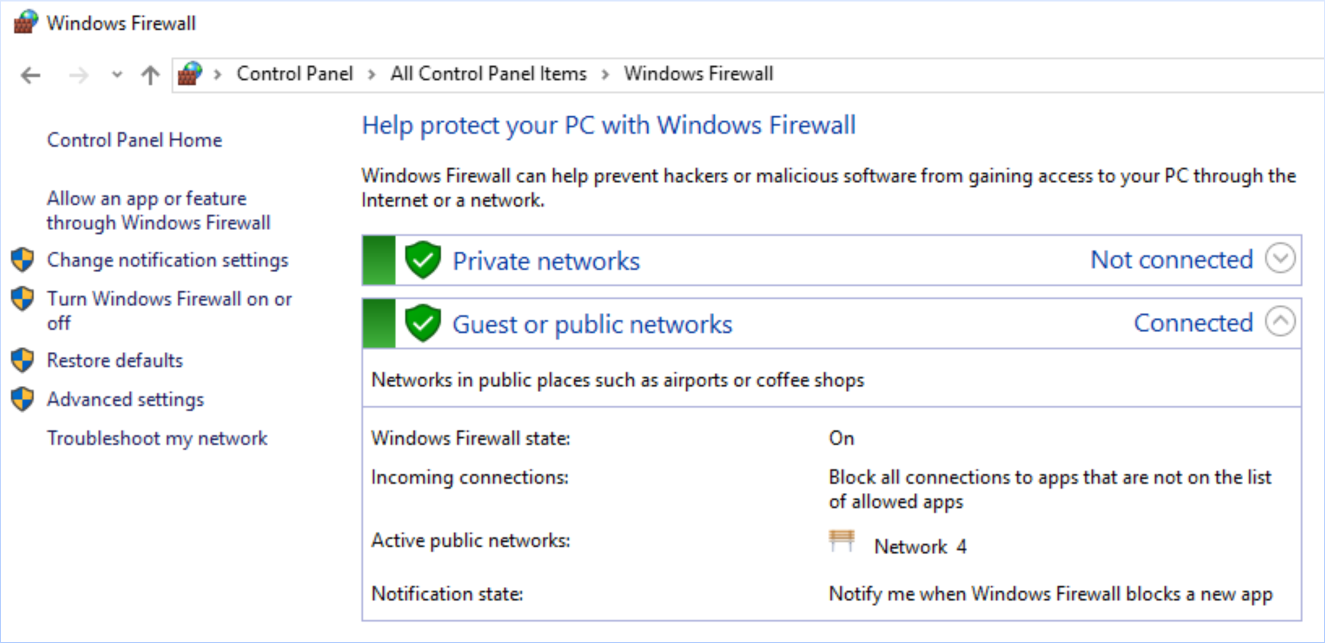
Network and Sharing Center

Network reset

Provide feedback about networking to the Windows team

Toward the bottom of the Network status screen is Windows Firewall.

CONFIGURING YOUR COMPUTER'S FIREWALL



Windows Firewall

Control Panel › All Control Panel Items › Windows Firewall

Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

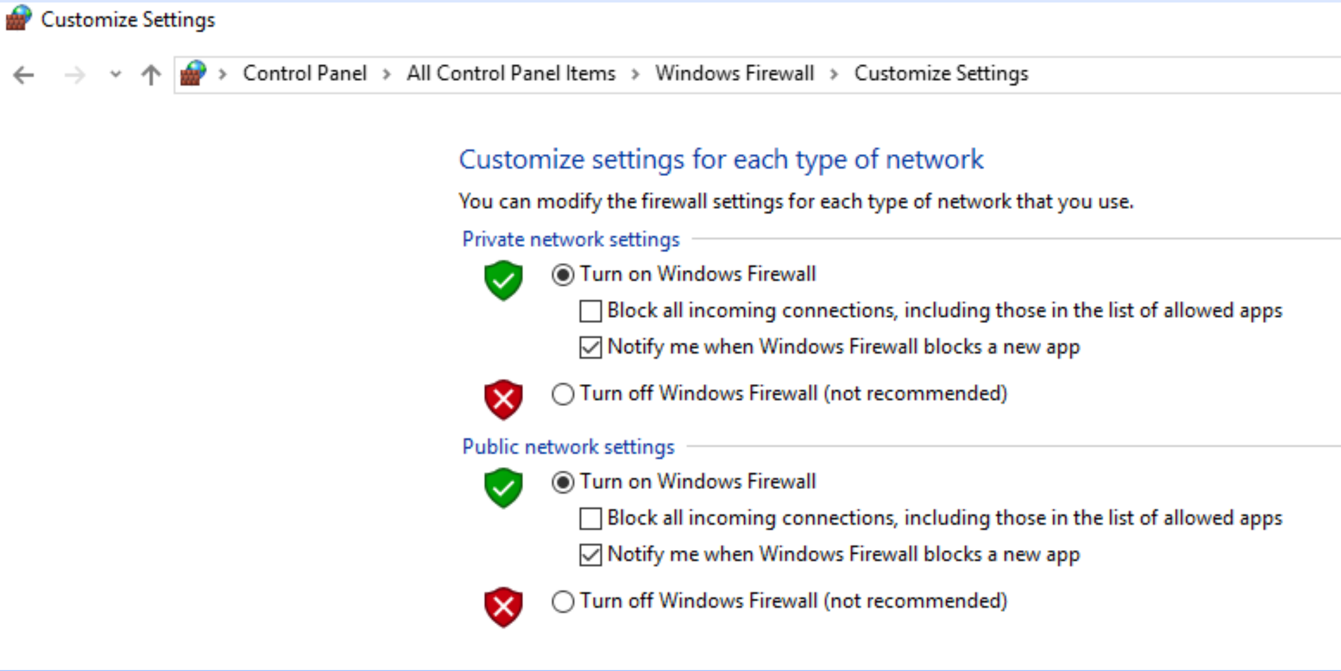
Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Network 4
Notification state:	Notify me when Windows Firewall blocks a new app

You'll want to make sure that the firewall is on. Here, my settings will block any app that I haven't allowed before, and Windows Firewall will tell me when it prevents a new app from connecting to the internet. You can customize these settings based on whether you're on your home network or connected to a public network like a coffee shop.

CONFIGURING YOUR COMPUTER'S FIREWALL



Customize Settings

Control Panel › All Control Panel Items › Windows Firewall › Customize Settings

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

○ Turn off Windows Firewall (not recommended)

Public network settings

● Turn on Windows Firewall

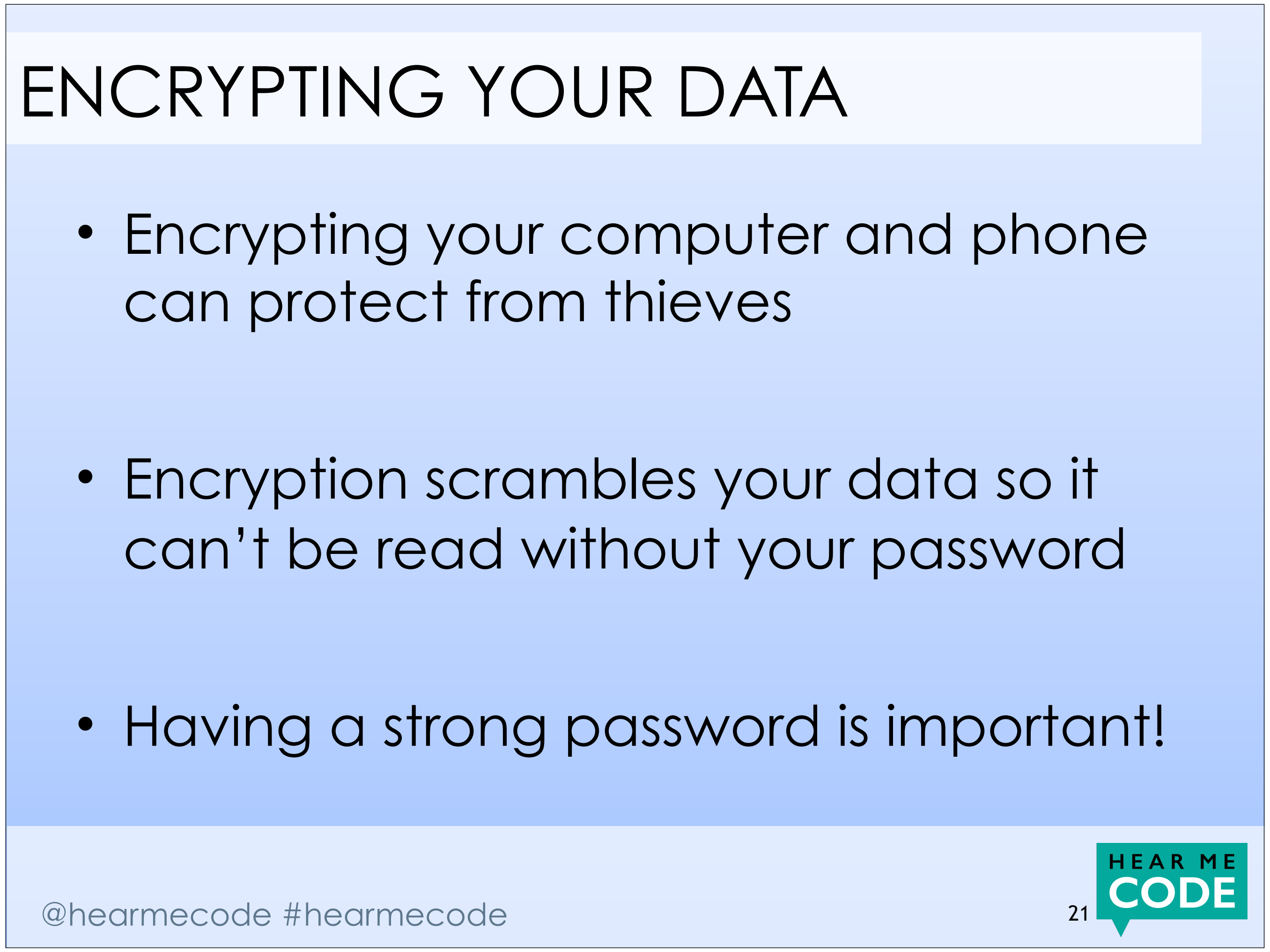
□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Firewall blocks a new app

○ Turn off Windows Firewall (not recommended)

Here's the customize settings screen, with the settings I would recommend. Private networks are like your home network where you trust all of the devices connected to it; public networks are networks like coffee shop wifi.

ENCRYPTING YOUR DATA

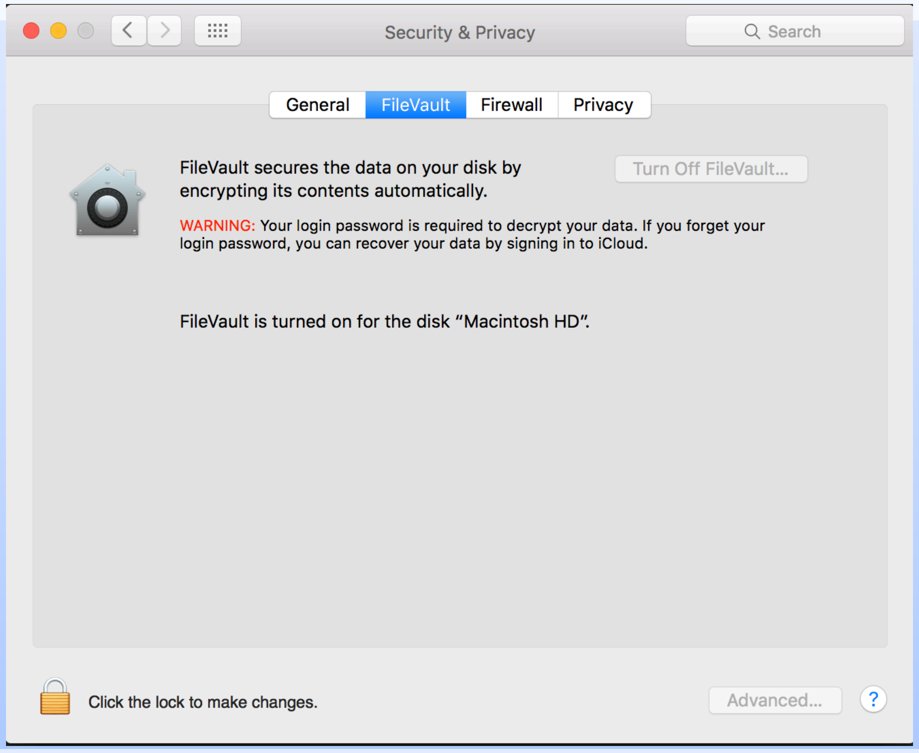


ENCRYPTING YOUR DATA

- Encrypting your computer and phone can protect from thieves
- Encryption scrambles your data so it can’t be read without your password
- Having a strong password is important!

One thing to note is that if you haven’t encrypted your device’s data yet, it’s a process that can take a little bit of time, so you’ll want to make sure that you’re at home and plugged in and won’t need to use your computer or phone for a little while.

ENCRYPTING YOUR DATA



FileVault secures the data on your disk by encrypting its contents automatically.

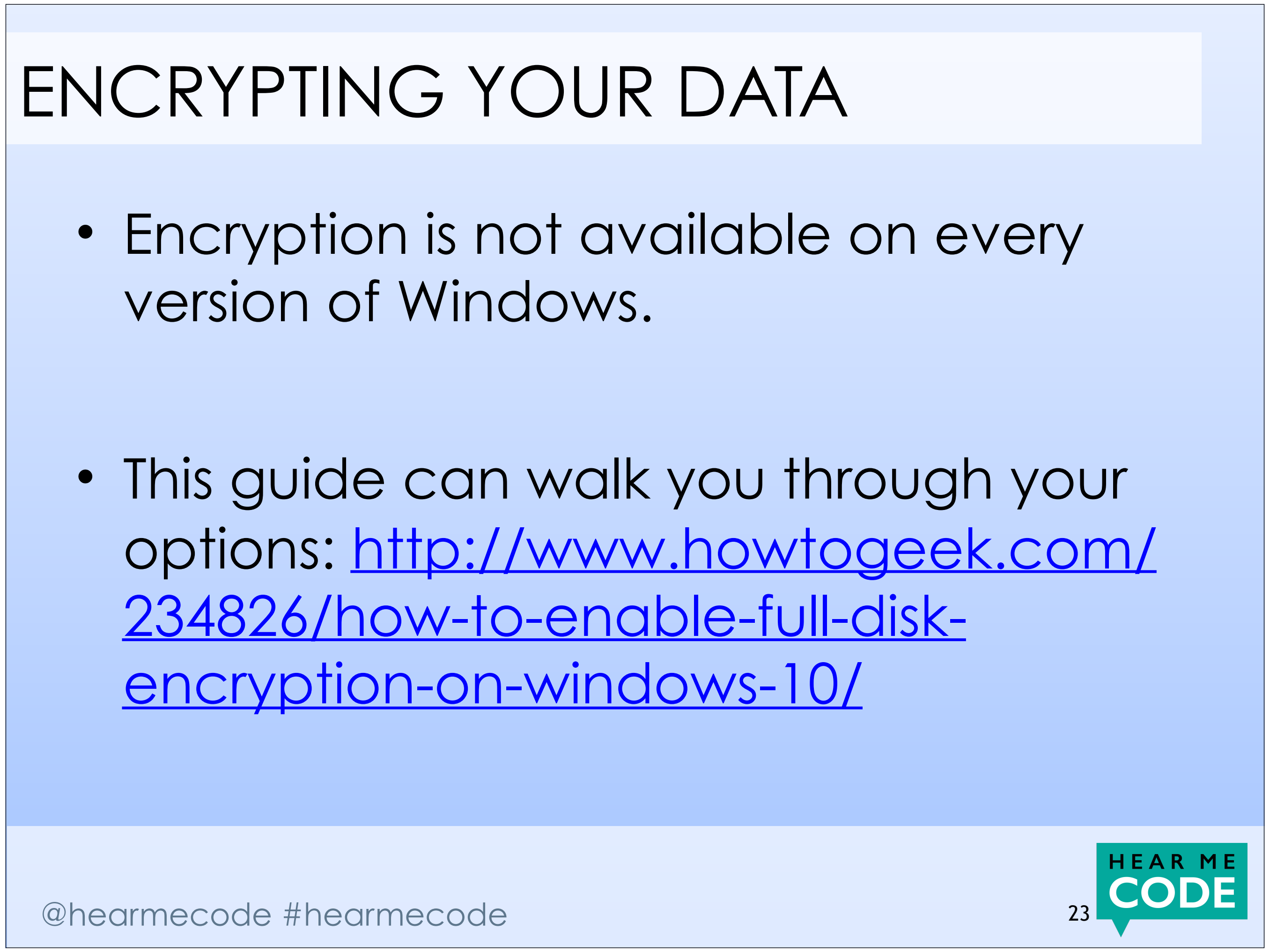
WARNING: Your login password is required to decrypt your data. If you forget your login password, you can recover your data by signing in to iCloud.

FileVault is turned on for the disk "Macintosh HD".

Click the lock to make changes.

@hearmecode #hearmecode

Apple calls disk encryption FileVault, and to turn it on, you'll go to the Apple Menu > System Preferences > Security & Privacy (in the top row) > FileVault. If you see "FileVault is turned on for the disk" and the name of your hard drive, then you already have FileVault enabled. If not, it's easy to set up. Click the lock to make changes, enter your login password, and click "Turn on FileVault." Keep in mind that encrypting your files the first time will take a little while, so you'll want to make sure that you're at home and plugged in before you get started. You may need to restart your computer to complete this process.

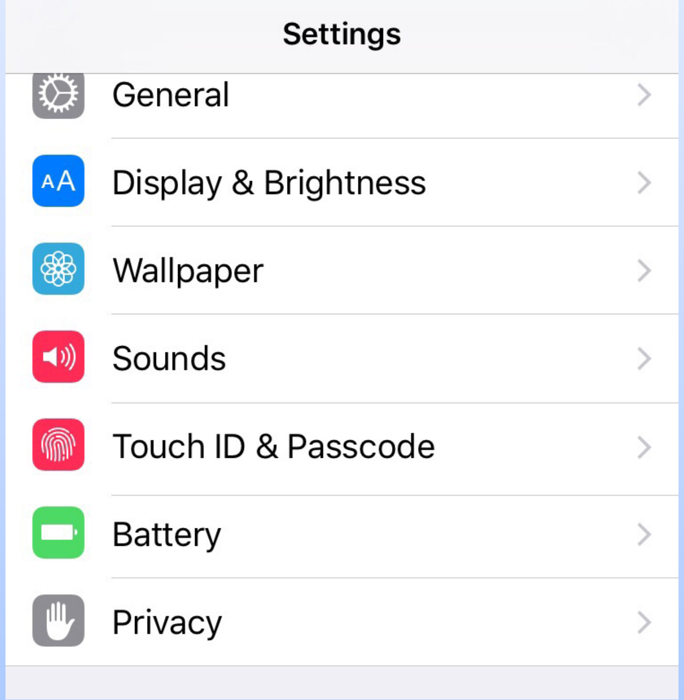


ENCRYPTING YOUR DATA

- Encryption is not available on every version of Windows.
- This guide can walk you through your options: http://www.howtogeek.com/234826/how-to-enable-full-disk-encryption-on-windows-10/

Some versions of Windows do not offer disk encryption, but the guide linked here can walk you through if it’s available and show you a free third-party option that you can use if it’s not.

ENCRYPTING YOUR PHONE

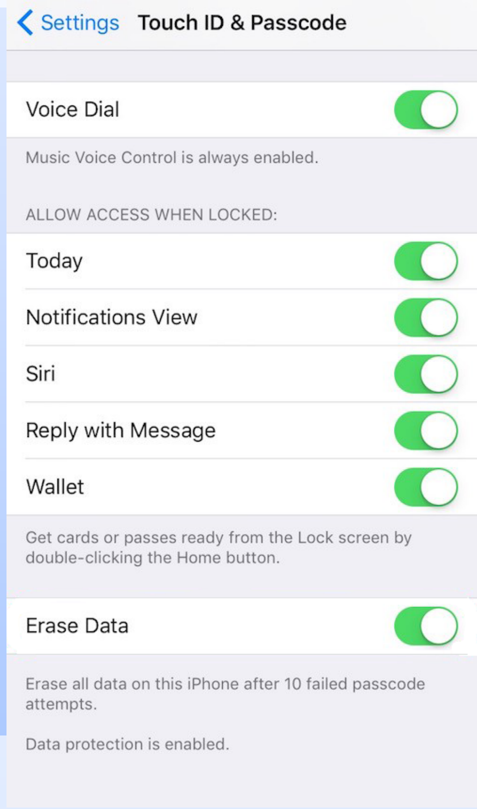


Settings

- General
- Display & Brightness
- Wallpaper
- Sounds
- Touch ID & Passcode
- Battery
- Privacy

If you have an iPhone, it’s probably encrypted already, but let’s check. Open your settings, then go to Touch ID & Passcode.

ENCRYPTING YOUR PHONE



Settings Touch ID & Passcode

Voice Dial ●

Music Voice Control is always enabled.

ALLOW ACCESS WHEN LOCKED:

Today ●

Notifications View ●

Siri ●

Reply with Message ●

Wallet ●

Get cards or passes ready from the Lock screen by double-clicking the Home button.

Erase Data ●

Erase all data on this iPhone after 10 failed passcode attempts.

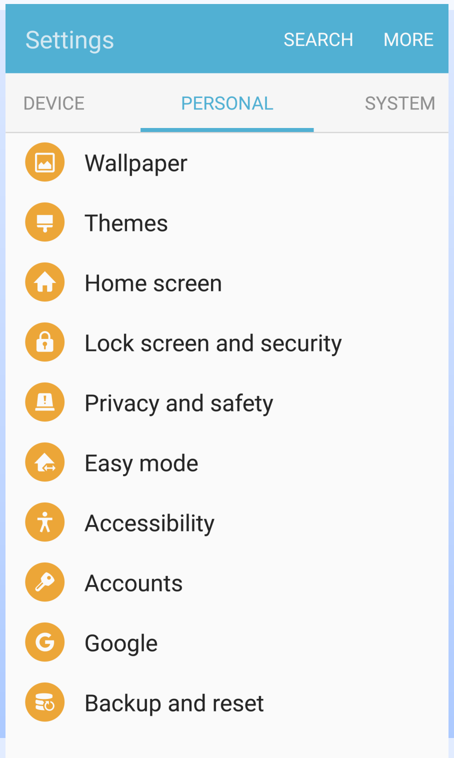
Data protection is enabled.

It'll prompt you for your password first, then scroll all the way to the bottom. If you see "Data protection is enabled," then your iPhone is encrypted. You may want to consider turning on the "Erase Data" feature that appears just above the "Data protection is enabled."

What does this do? Let's say someone steals your phone. In theory, they could try every password in the book and eventually break in. (This is another reason having a strong password is a good thing!) If you have Erase Data turned on though, they would only get 10 chances to guess your password, and after that all of the data on your phone would be erased.

If you have young children who play with your phone often, you may not want to turn on the "Erase Data" feature.

ENCRYPTING YOUR PHONE



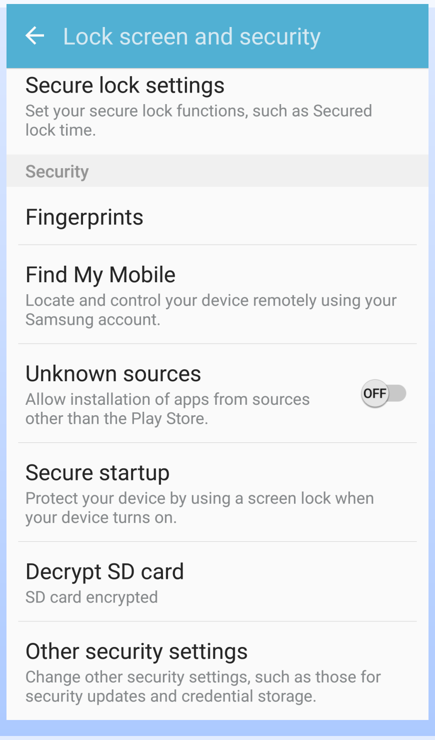
Settings SEARCH MORE

DEVICE PERSONAL SYSTEM

- Wallpaper
- Themes
- Home screen
- Lock screen and security
- Privacy and safety
- Easy mode
- Accessibility
- Accounts
- Google
- Backup and reset

To enable encryption on your Android, open your Settings, find the Personal tab, and go to Lock Screen and Security.

ENCRYPTING YOUR PHONE



Lock screen and security

Secure lock settings
Set your secure lock functions, such as Secured lock time.

Security

Fingerprints

Find My Mobile
Locate and control your device remotely using your Samsung account.

Unknown sources
Allow installation of apps from sources other than the Play Store.
OFF

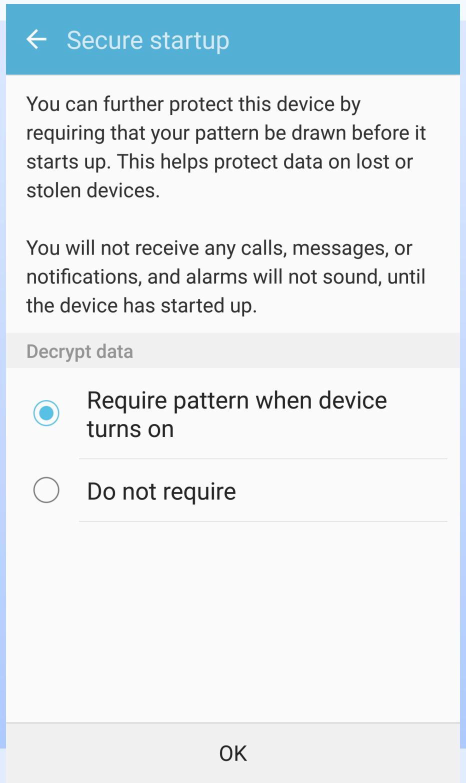
Secure startup
Protect your device by using a screen lock when your device turns on.

Decrypt SD card
SD card encrypted

Other security settings
Change other security settings, such as those for security updates and credential storage.

The Lock screen and security page has many useful settings you'll want to review but for now, click "Secure startup"

ENCRYPTING YOUR PHONE



Secure startup

You can further protect this device by requiring that your pattern be drawn before it starts up. This helps protect data on lost or stolen devices.

You will not receive any calls, messages, or notifications, and alarms will not sound, until the device has started up.

Decrypt data

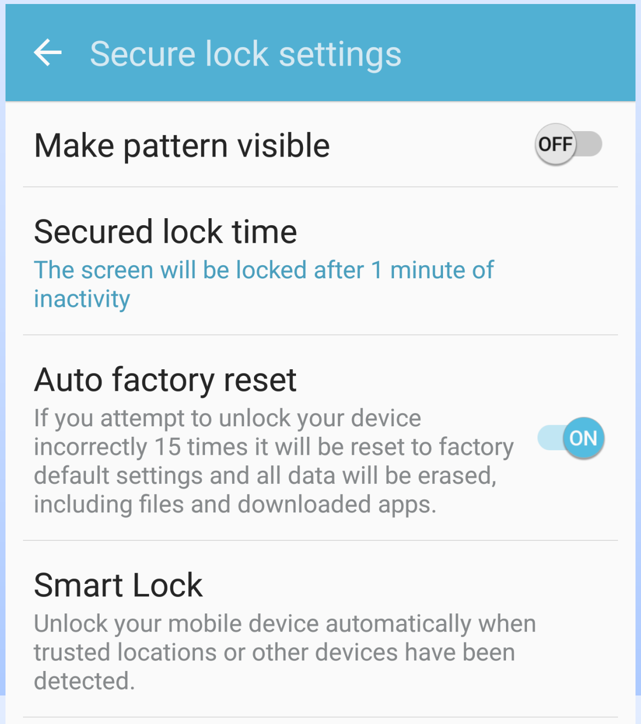
● Require pattern when device turns on

○ Do not require

Secure startup is what Android calls disk encryption, and you'll want to require your pattern or password when the device turns on. If you're turning this on for the first time, keep in mind it can take a little while to enable, and that you'll want to make sure that you're plugged in before you get started.

An important note: if you have an SD card, you will need to encrypt that separately from your phone's main hard drive.

ENCRYPTING YOUR PHONE



Make pattern visible — OFF

Secured lock time

The screen will be locked after 1 minute of inactivity

Auto factory reset — ON

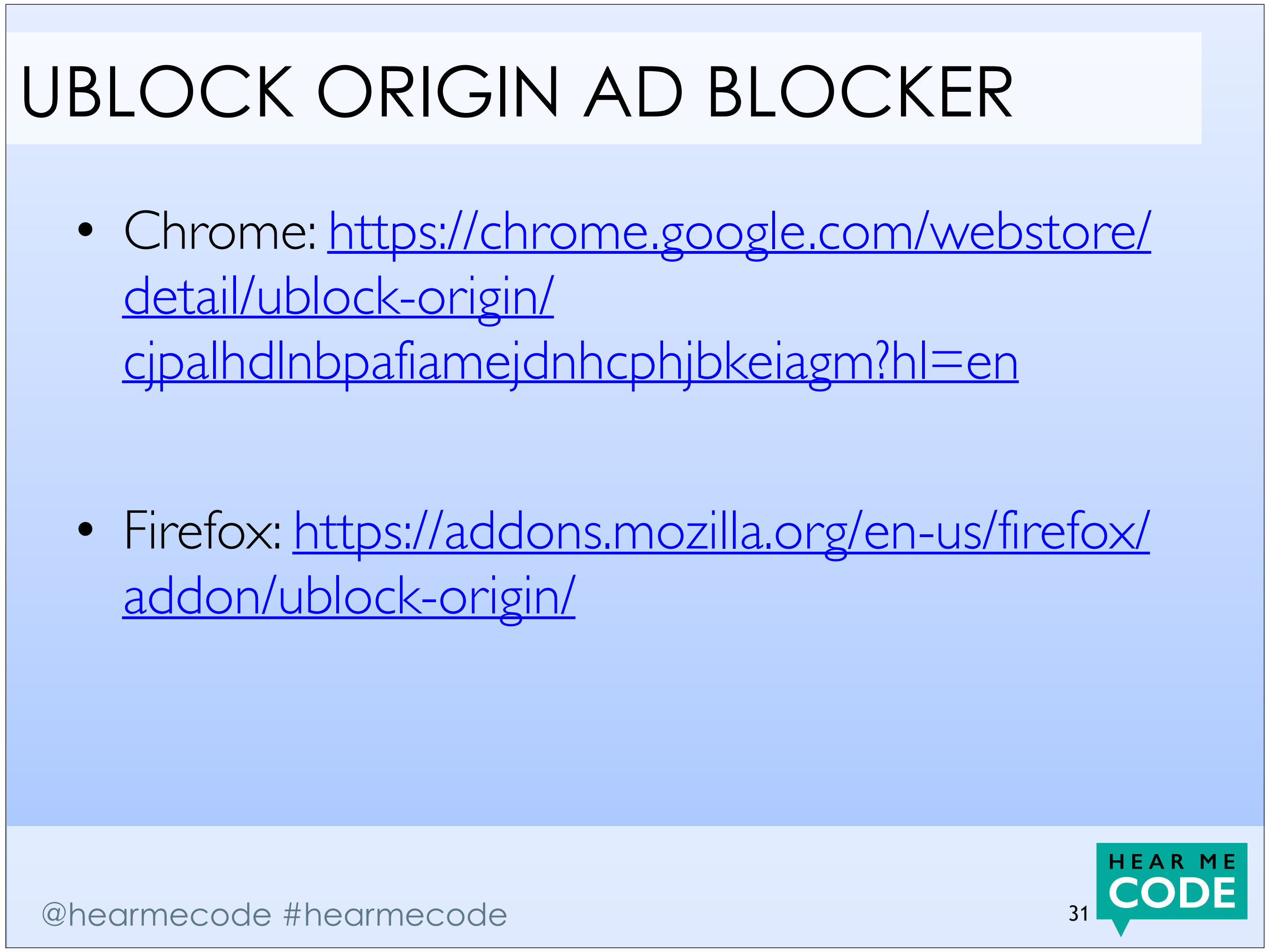
If you attempt to unlock your device incorrectly 15 times it will be reset to factory default settings and all data will be erased, including files and downloaded apps.

Smart Lock

Unlock your mobile device automatically when trusted locations or other devices have been detected.

While we’re in the Lock Screen & Security page, let’s take a look at the Secure lock settings. Here, I have my phone set to lock after 1 minute of inactivity, and just like the iPhone “Erase data” feature, I have the “Auto factory reset” feature enabled so that someone can’t try every password in the book.

BROWSER EXTENSIONS TO KEEP YOU SAFER

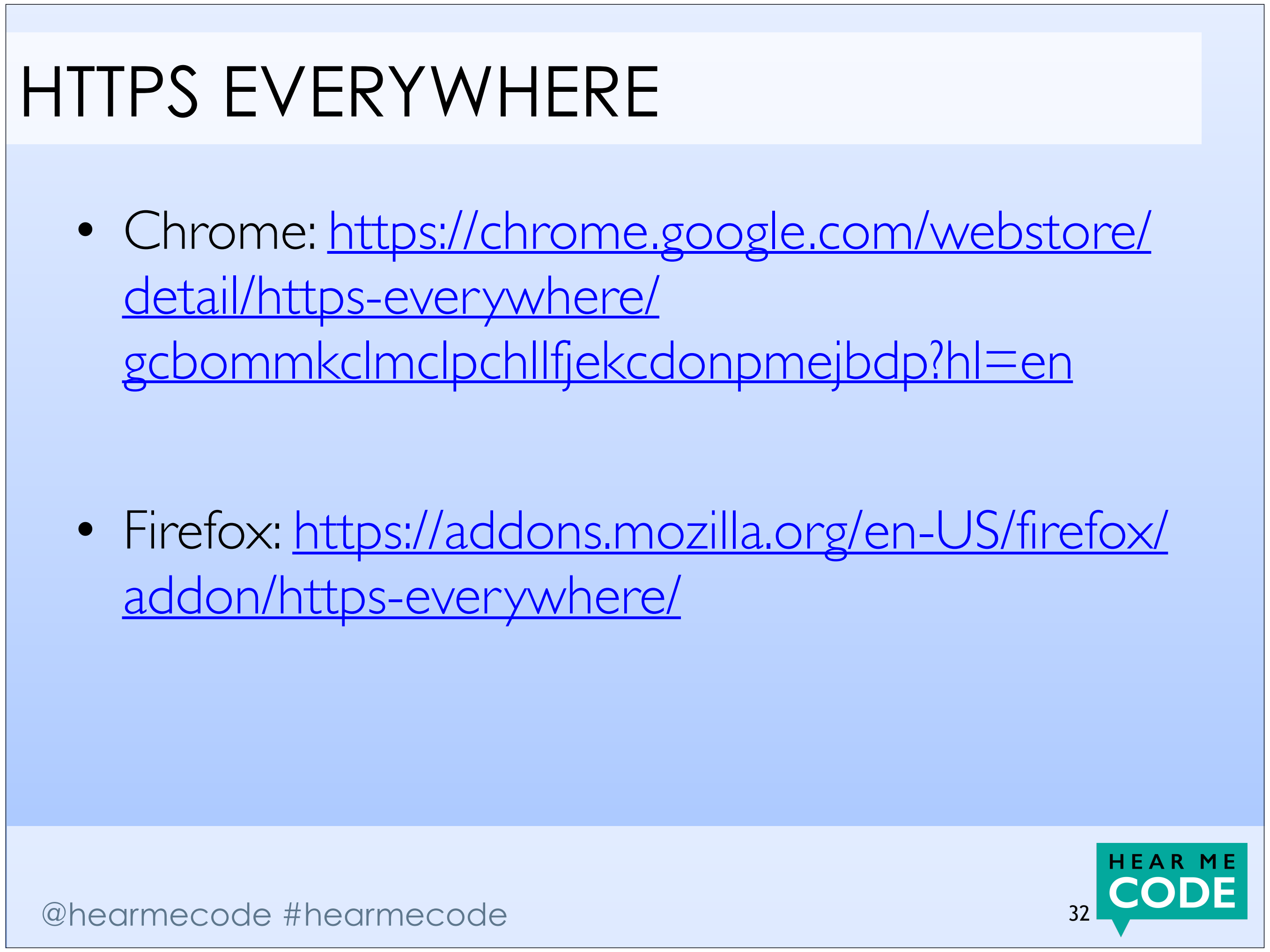


UBLOCK ORIGIN AD BLOCKER

- Chrome: https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=en
- Firefox: https://addons.mozilla.org/en-us/firefox/addon/ublock-origin/

Ads can track which websites you’ve visited and are not merely intrusive from a privacy perspective; they can also be a security risk. Malicious ads can infect your computer with a virus, so blocking them with a trusted ad blocker can keep you safe. You may notice that UBlock blocks things like social media buttons in addition to advertisements. You can also turn it off on a per-site basis if you like.

These are links that will let you download a browser extension for either Chrome or Firefox.



HTTPS EVERYWHERE

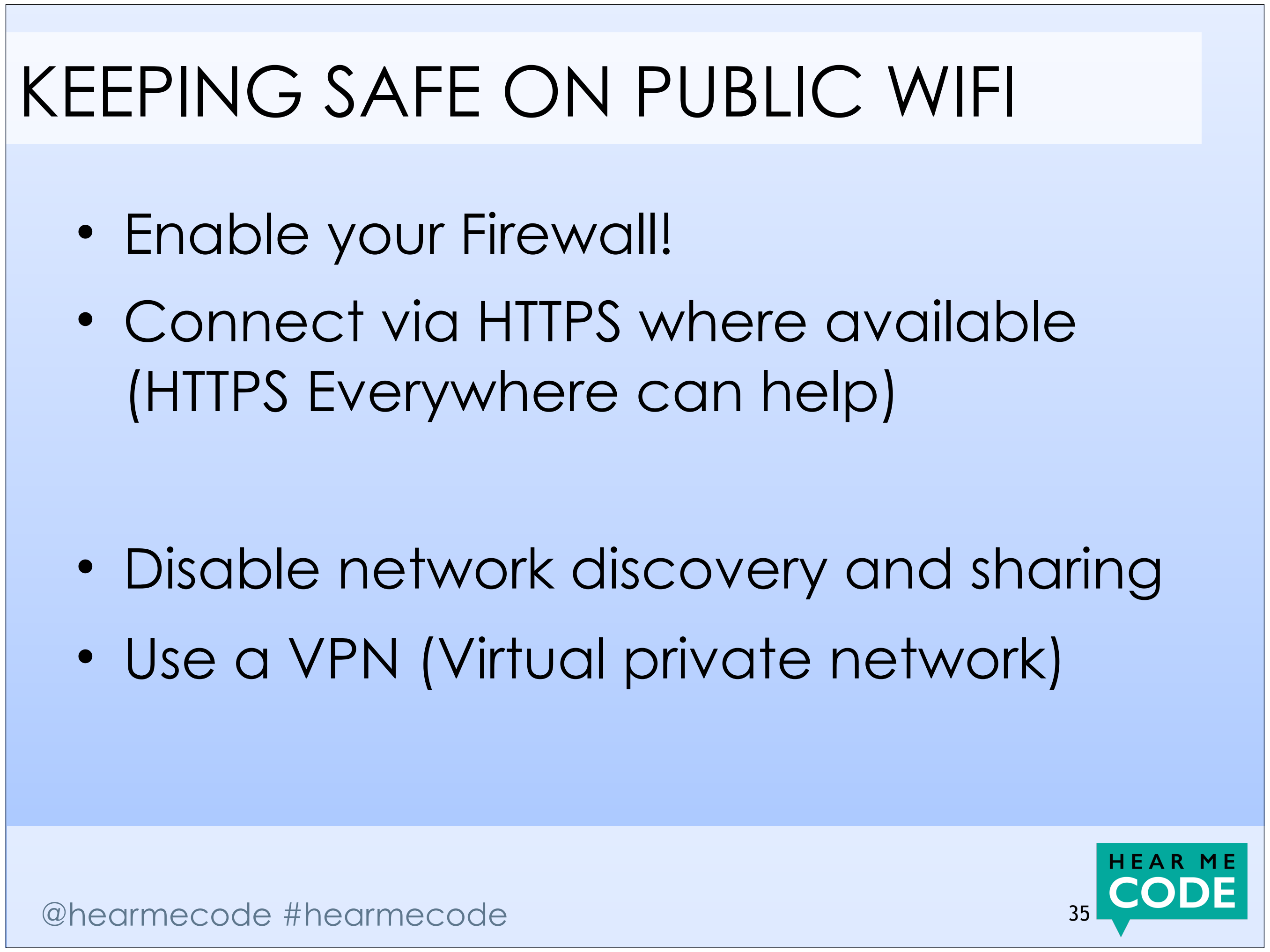
- Chrome: https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp?hl=en
- Firefox: https://addons.mozilla.org/en-US/firefox/addon/https-everywhere/

HTTPS Everywhere is a browser extension that can change some insecure HTTP requests into secure HTTPS requests. It’s not perfect and if a website isn’t configured to use HTTPS at all, it *will not* make that connection between your website and the computer secure.

KEEPING SAFE ON PUBLIC WIFI

WHAT COULD GO WRONG?

- Hackers could be on the public network too
- Whoever is on the network can see everyone else who is connected and could monitor non-secure internet traffic
- Attackers could create a “lookalike” network, then monitor the traffic of everyone who connects



KEEPING SAFE ON PUBLIC WIFI

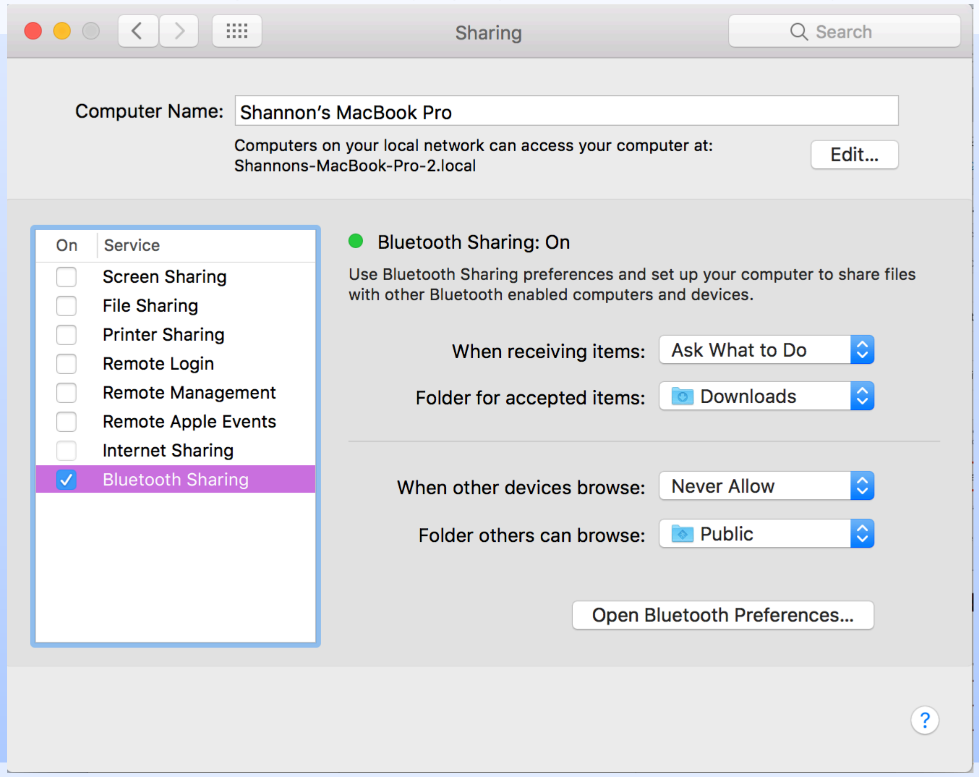
- Enable your Firewall!
- Connect via HTTPS where available (HTTPS Everywhere can help)

- Disable network discovery and sharing
- Use a VPN (Virtual private network)

If you've been following along with this training start to finish, you have already completed the first two steps: enabling your computer's firewall and installing the HTTPS Everywhere browser extension. There's two more things we should do to protect ourselves when connecting to public wifi, and in the next few slides we'll show how to do those.

If you're on a public Wifi and not connecting via HTTPS, it's possible for someone to intercept your internet traffic.

DISABLE NETWORK DISCOVERY AND SHARING



Sharing

Computer Name: Shannon’s MacBook Pro

Computers on your local network can access your computer at:
Shannons-MacBook-Pro-2.local

On	Service
☐	Screen Sharing
☐	File Sharing
☐	Printer Sharing
☐	Remote Login
☐	Remote Management
☐	Remote Apple Events
☐	Internet Sharing
☑	Bluetooth Sharing

● Bluetooth Sharing: On

Use Bluetooth Sharing preferences and set up your computer to share files with other Bluetooth enabled computers and devices.

When receiving items: Ask What to Do

Folder for accepted items: Downloads

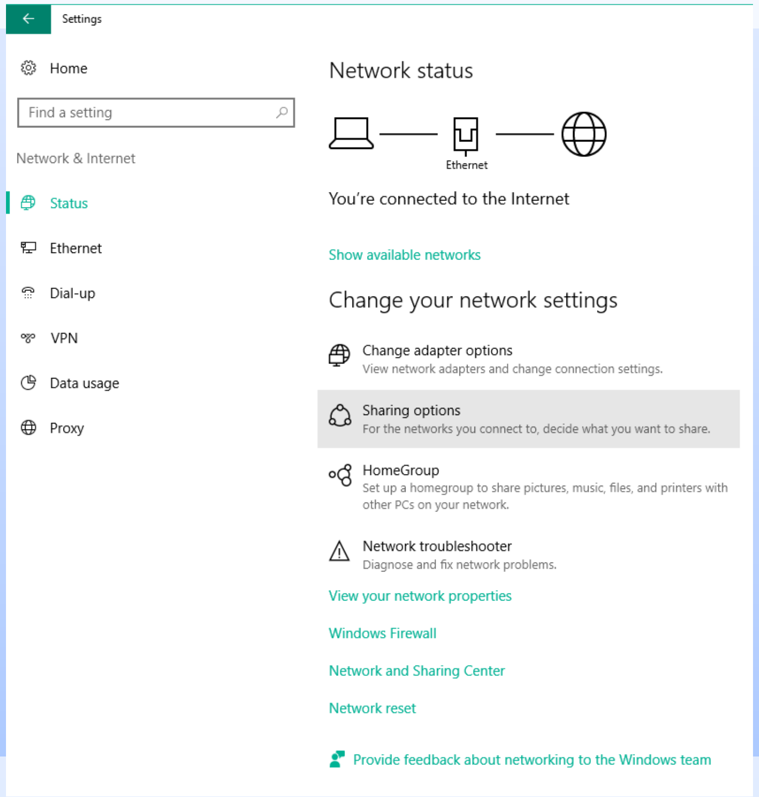
When other devices browse: Never Allow

Folder others can browse: Public

Usually, the sharing settings are off by default — that’s a good thing! While sharing can be a useful feature in some situations, it can also leave your computer vulnerable if the settings are too permissive. Check your computer’s settings by going to the Apple Menu > System Preferences > Sharing (in the third row). Each type of sharing (Screen Sharing, File Sharing, Printer Sharing, Remote Login, and so on) has its own set of permissions to configure. Here, I have all of them turned off except for Bluetooth Sharing, which I was using when creating this slideshow to send pictures from my phone to my computer. If all of the checkboxes are unchecked, that’s good — it means you’re not using these features.

If you do decide to use these features, make sure you configure them carefully, understand what you’re doing, and turn them off if you no longer need them. This is a good idea not just for keeping yourself safe on public wifi, but generally.

DISABLE NETWORK DISCOVERY AND SHARING



Settings

Home

Find a setting

Network & Internet

- Status
- Ethernet
- Dial-up
- VPN
- Data usage
- Proxy

Network status

You're connected to the Internet

Show available networks

Change your network settings

Change adapter options
View network adapters and change connection settings.

Sharing options
For the networks you connect to, decide what you want to share.

HomeGroup
Set up a homegroup to share pictures, music, files, and printers with other PCs on your network.

Network troubleshooter
Diagnose and fix network problems.

View your network properties

Windows Firewall

Network and Sharing Center

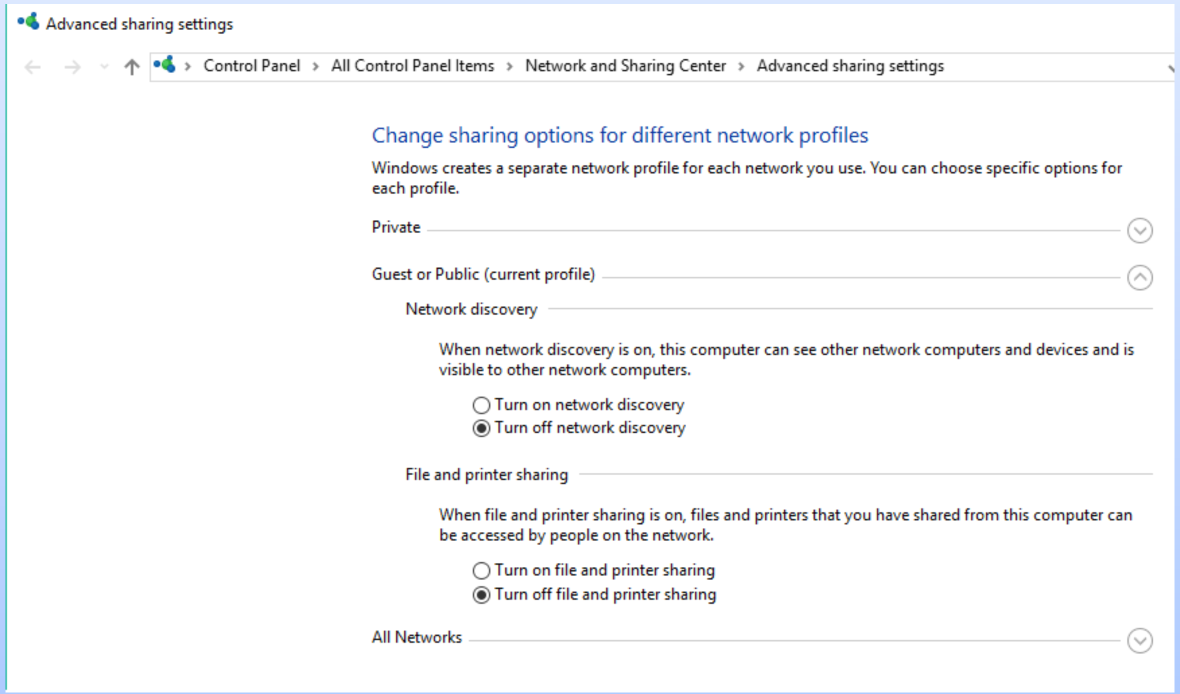
Network reset

Provide feedback about networking to the Windows team

@hearmecode #hearmecode

On Windows, open the settings as seen earlier, and go to the Network status window. This time, go to the Sharing options as seen in the highlighted screenshot.

DISABLE NETWORK DISCOVERY AND SHARING



Advanced sharing settings

Control Panel › All Control Panel Items › Network and Sharing Center › Advanced sharing settings

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private

Guest or Public (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

○ Turn on network discovery
● Turn off network discovery

File and printer sharing

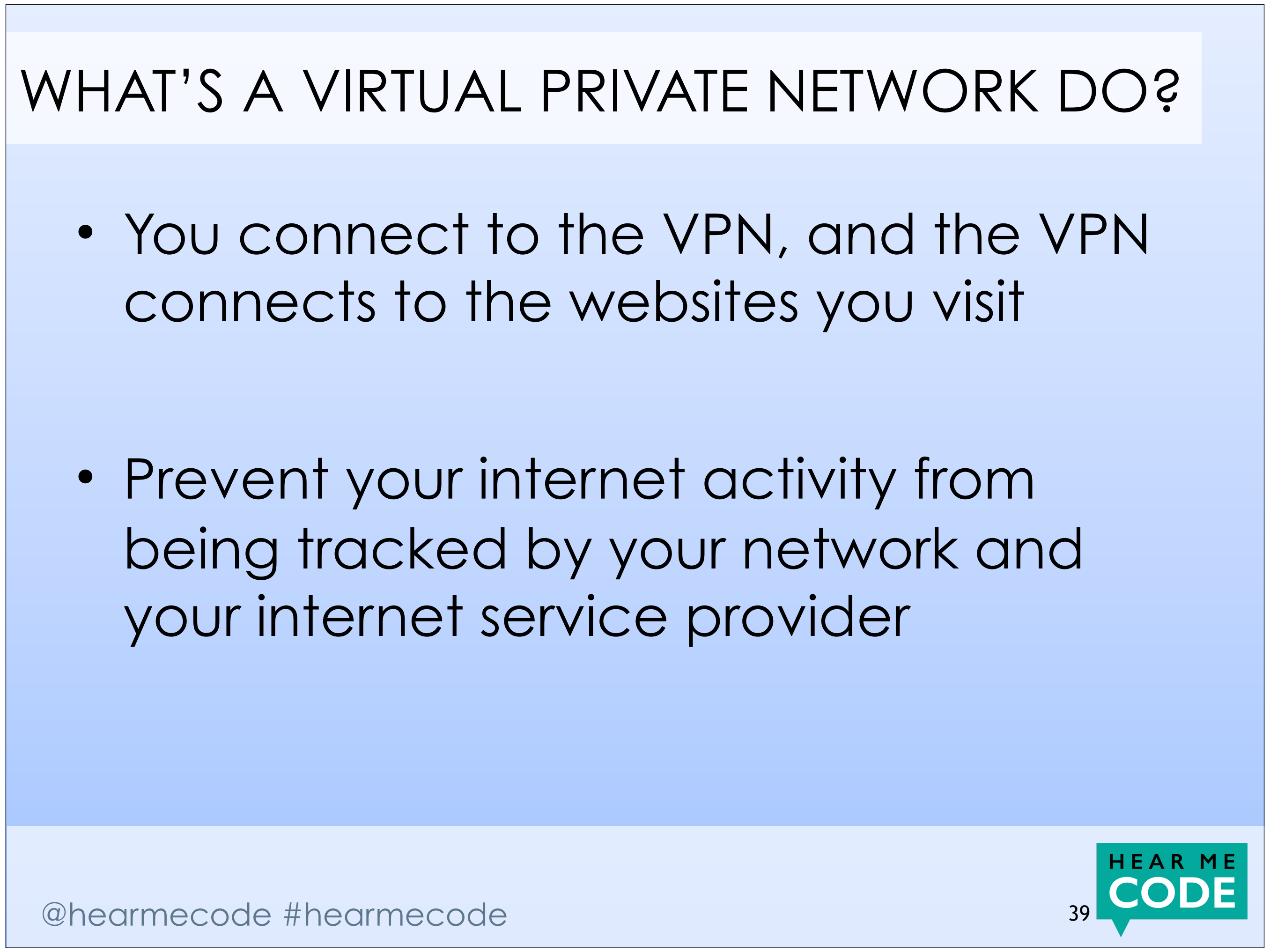
When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

○ Turn on file and printer sharing
● Turn off file and printer sharing

All Networks

In this window you will be able to configure your network settings based on which type of network you're connected to. You might want a different set of permissions if you're on your home network versus if you're at a coffeeshop. In this screenshot, I'm configuring the settings for a public network like that you would use at a coffeeshop. I've chosen to turn off network discovery and turn off file and printer sharing.

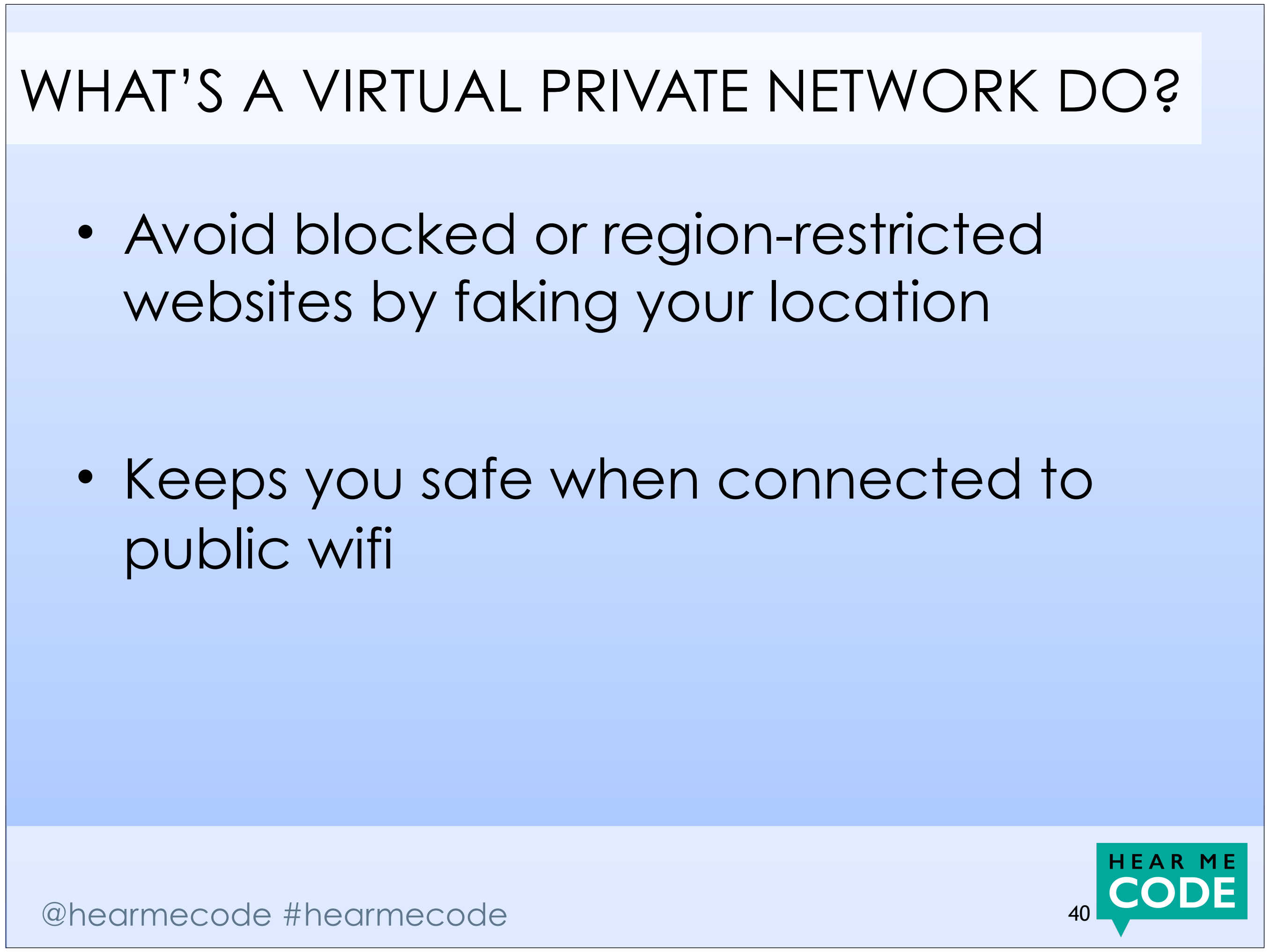
What that means is that my computer won't be visible to other computers on this network, and that any files I've put in a share folder won't be accessible to computers on this network.



WHAT'S A VIRTUAL PRIVATE NETWORK DO?

- You connect to the VPN, and the VPN connects to the websites you visit
- Prevent your internet activity from being tracked by your network and your internet service provider

Your internet service provider will be able to see that you are connecting to a VPN but won't be able to tell anything beyond that.



WHAT'S A VIRTUAL PRIVATE NETWORK DO?

- Avoid blocked or region-restricted websites by faking your location
- Keeps you safe when connected to public wifi

As long as your connection to your VPN is secure, the VPN will keep your traffic from being intercepted by anyone else on the public wifi.

VIRTUAL PRIVATE NETWORKS (VPN)

- There are many services that offer VPNs
- Some options include: https://privacytoolsio.github.io/privacytools.io/#vpn
- Whatever service you use, make sure you trust them!

There are a lot of different VPNs out there - the ones linked here are just a few services. This page has a LOT of information and is aimed at advanced users, but I found it very informative so I wanted to include it. Which VPN you use is up to you and your specific needs and threat models.

ANTI-VIRUS SOFTWARE

ANTI-VIRUS SOFTWARE

- Anti-virus software can protect your computer by blocking viruses and other kinds of malicious programs (malware)

- Yes, even Macs can get viruses.

ANTI-VIRUS SOFTWARE

- Visiting malicious websites and downloading counterfeit software are common ways you can get a virus

- Ad blockers can help but for an added layer of protection, you'll want to get anti-virus software

ANTI-VIRUS SOFTWARE

- Many anti-virus providers have a free service, but some are paid.

- I use https://www.avast.com/

- Most importantly: keep your software up to date!

CONTINUE LEARNING

Resources and additional trainings will be added here periodically.