



CYBER SECURITY TIPS

End User & System Protection

Eric Adams, CISO, Kyriba Corp.



PROTECTING MY COMPUTER SYSTEM

What do I need to do?

WHAT?

An aerial photograph of a city with several tall buildings. A large green rectangle is overlaid on the left side, and a white square frame is overlaid on the right side. The text is centered within the white frame.

WHY?

**ATTACKERS ON
THE INTERNET
WANT YOUR DATA**

Because it is worth
money

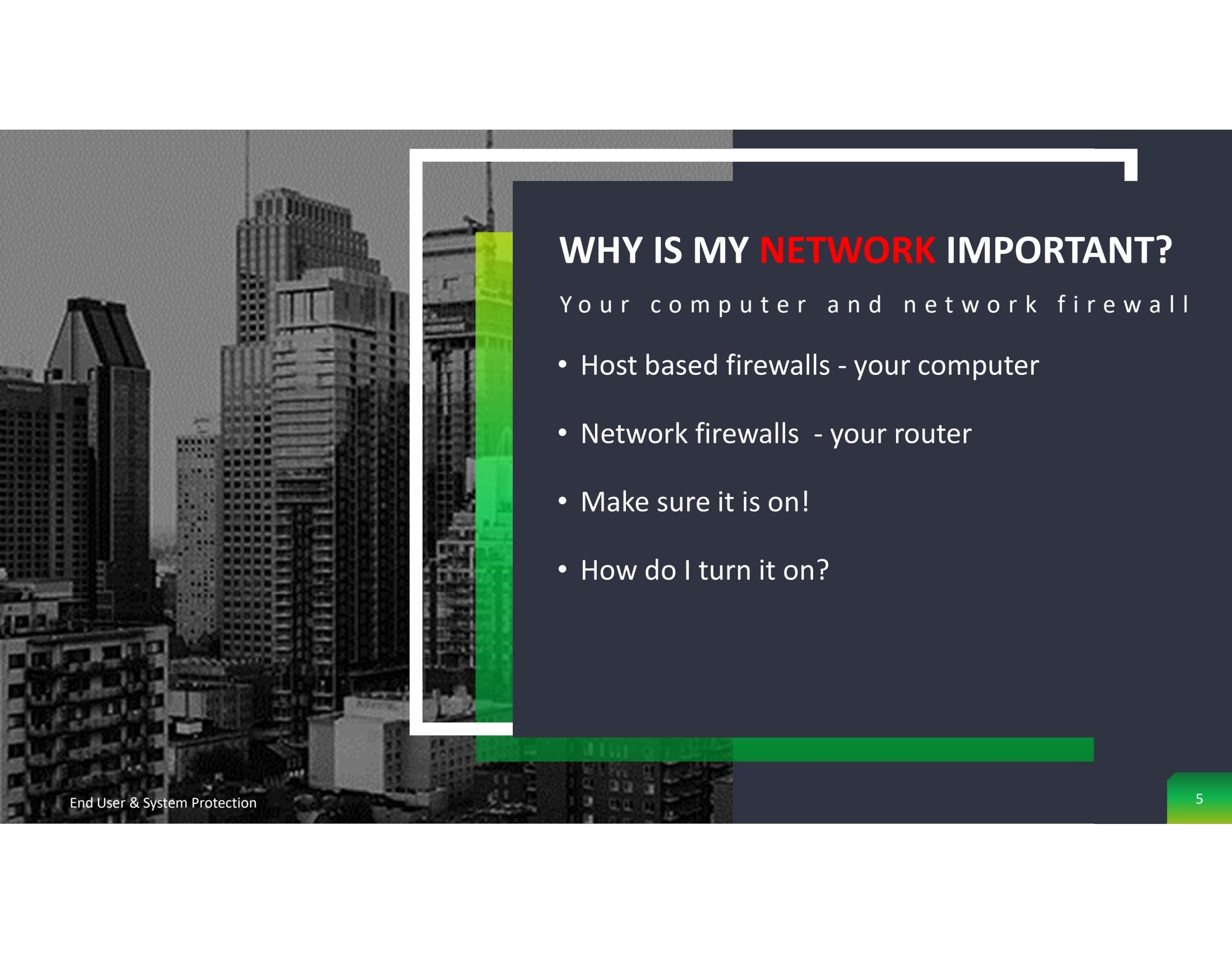
HOW DO I PROTECT MYSELF?

Protect myself and my computer system by:

- Blocking attackers on my network
- Keeping my system current and up to date
- Making sure I have backups of my system and can recover from backups
- Maintaining a way to block computer viruses and malware
- Ensuring I can identify fake emails intended to 'trick and click'



HOW?



WHY IS MY **NETWORK** IMPORTANT?

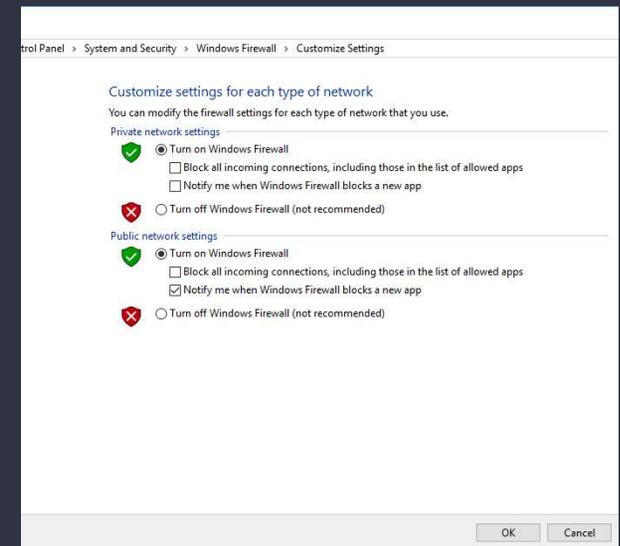
Your computer and network firewall

- Host based firewalls - your computer
- Network firewalls - your router
- Make sure it is on!
- How do I turn it on?

Just type the word 'firewall' in the search by text box in Windows.



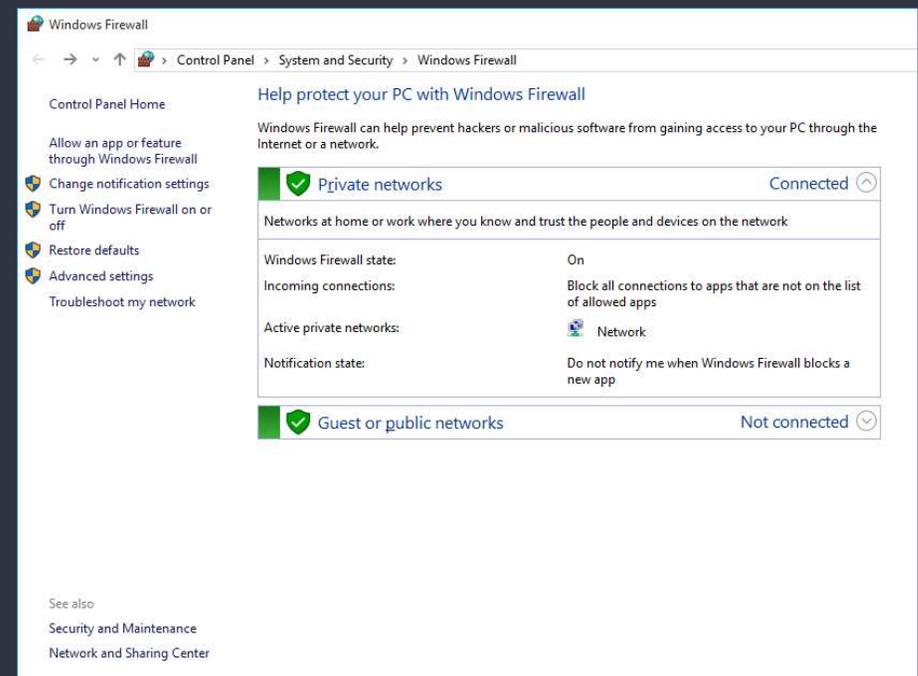
Click the circle to turn on both the private and public firewalls to on.



NOW IT IS ON

Key Points to Remember

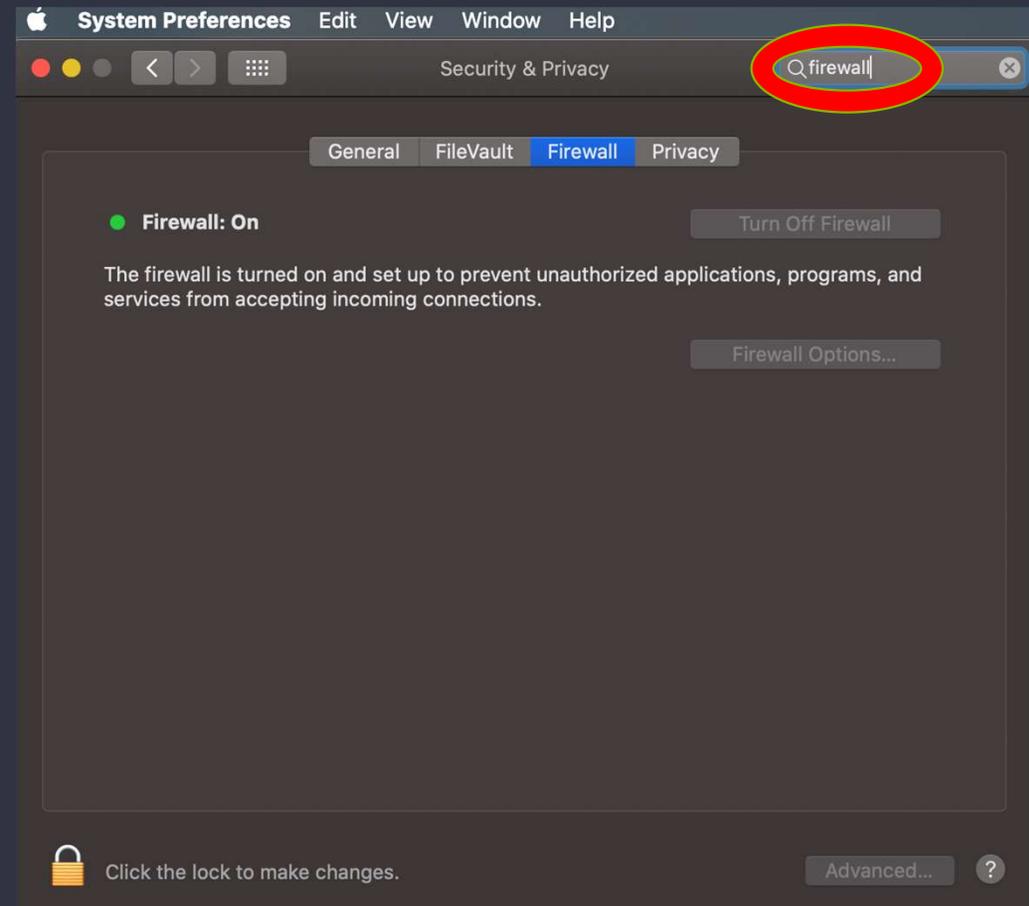
- Network Security is important to keep attackers out of your network
- Type 'Firewall' to check your firewall settings
- Laptop devices connecting remotely at public places should connect using a virtual private network (VPN) connection
- Your home router security settings should be reviewed with help from your internet service provider (ISP) customer support



APPLE MAC OS

🍏 > System Preferences

- Just type the word 'firewall' in the search by text box in Mac OS



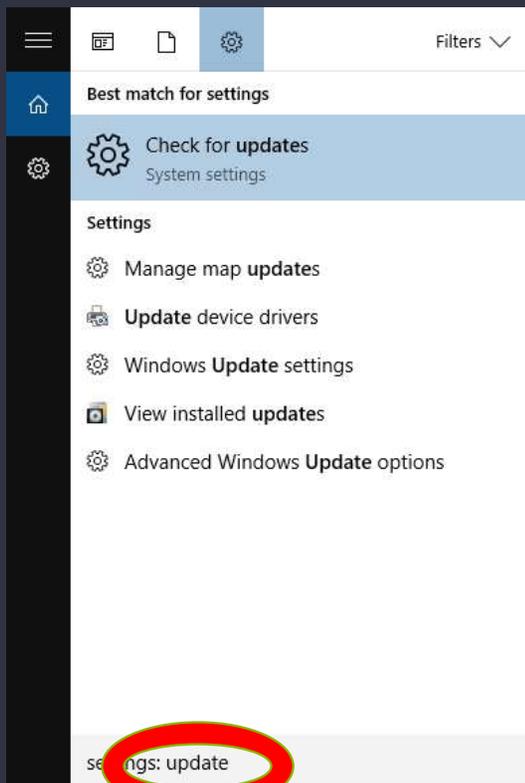


WHY ARE **UPDATES** IMPORTANT?

Updating and Patching your System

- Operating System Updates
- Device Driver Updates
- Security Updates
- Automatic Patching

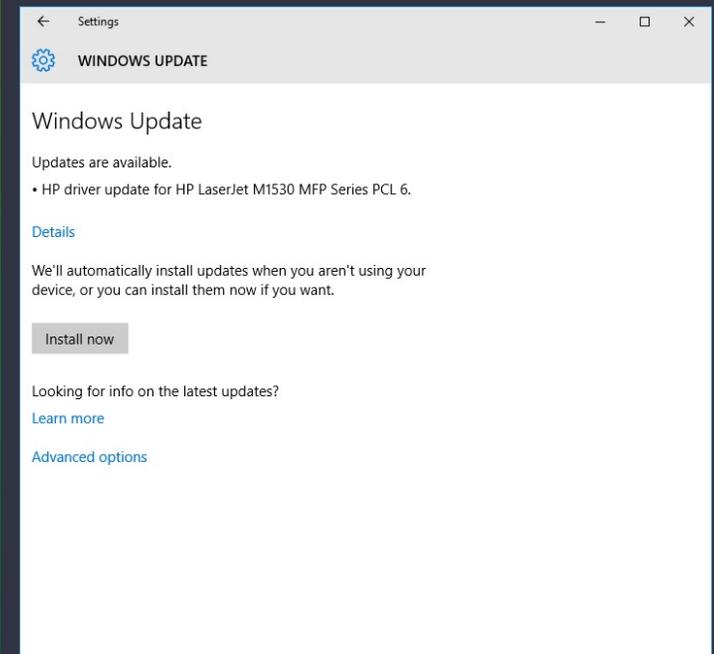
Just type the word 'update' in the search or run box in Windows.



End User & System Protection



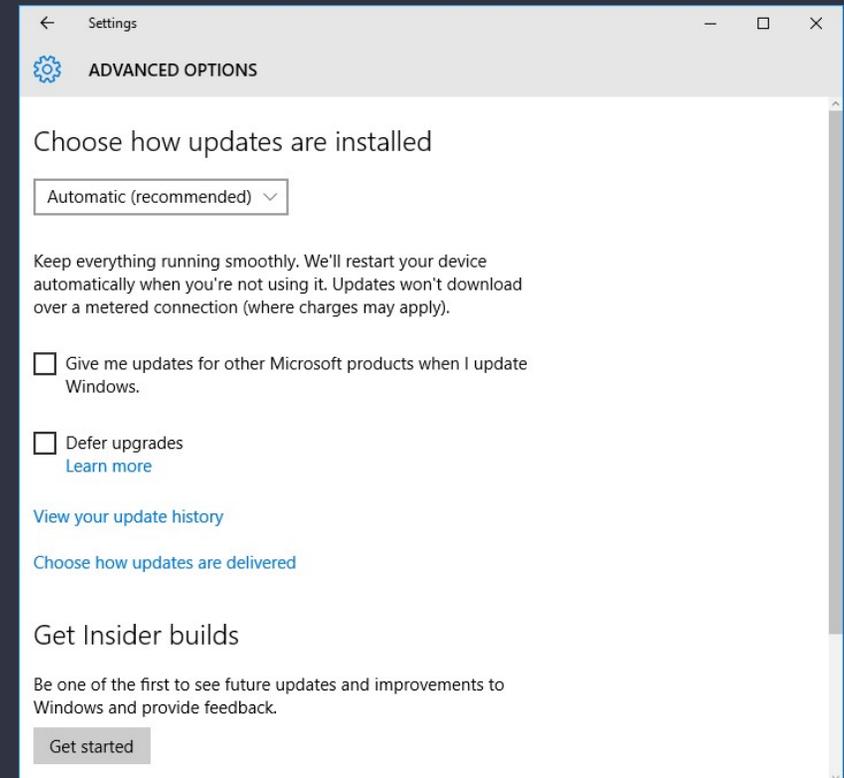
Windows found 1 item update – printer driver.



AUTOMATIC UPDATES

Key Points to Remember

- Schedule updates and patches automatically when they are released
- Be aware of notifications and displays of critical updates, some requiring a reboot to install



APPLE MAC OS

🍏 > System Preferences

- Just type the word 'update' in the search by text box in Mac OS



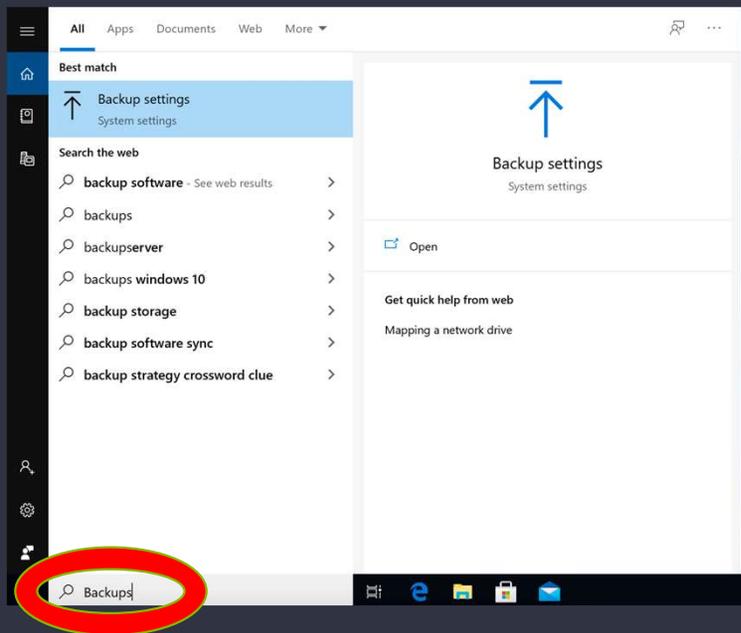


WHY IS ARE **BACKUPS** IMPORTANT?

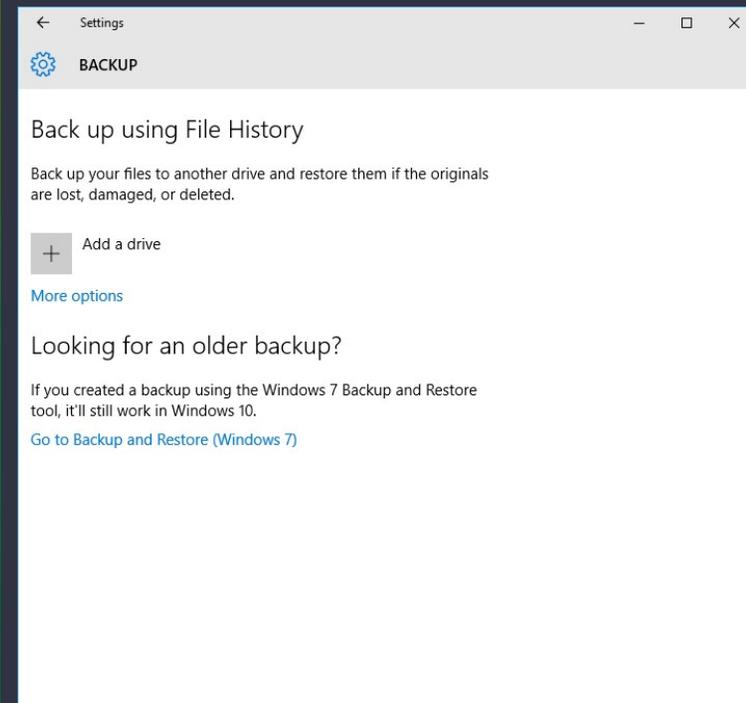
Ability to restore your files

- Goal: be able to adequately restore as soon as possible at a point as recent as possible
- This must be setup in advance – other wise there is nothing to recover
- Test backup and restore process periodically

Just type the word 'backup' in the search by text box in Windows.



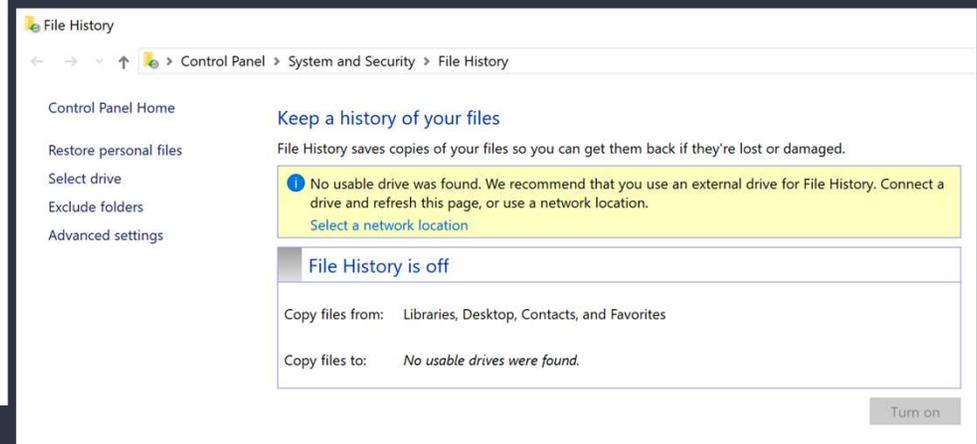
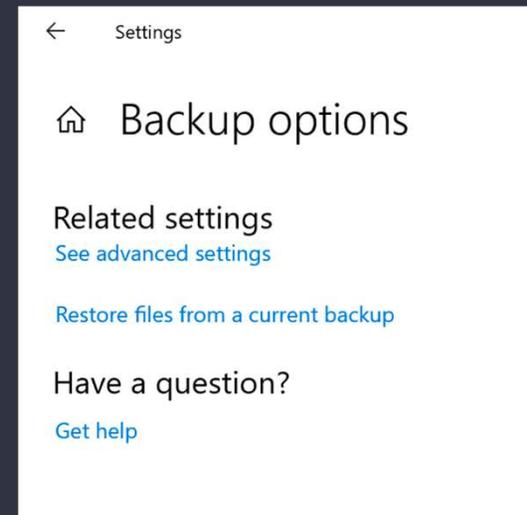
Choose Add a drive if you do not have one yet.



BACKUPS ARE SETUP

Key Points to Remember

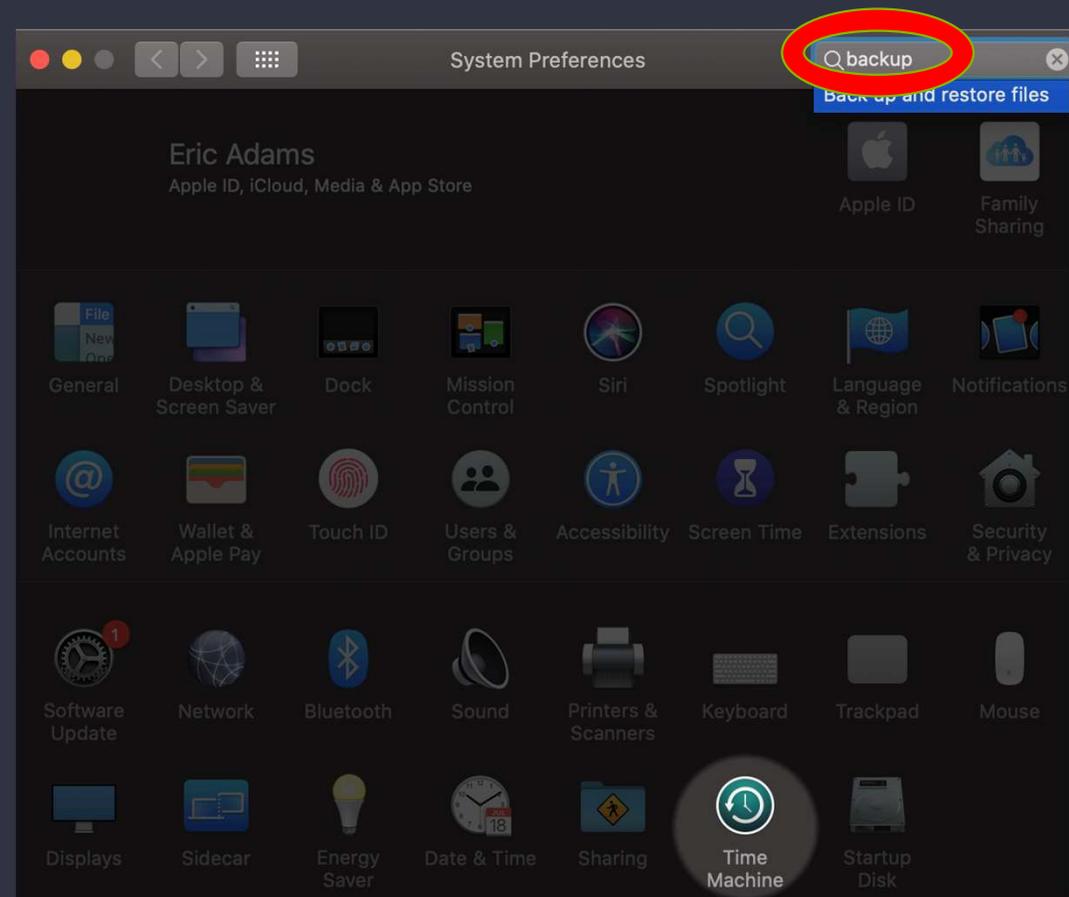
- Ensure you are backing up the files you need
- Test backups periodically to ensure they are working to restore files
- Create a strategy of redundancy – second backup devices
- Make sure backups are secured



APPLE MAC OS

🍏 > System Preferences

- Just type the word 'backups' in the search by text box in Mac OS



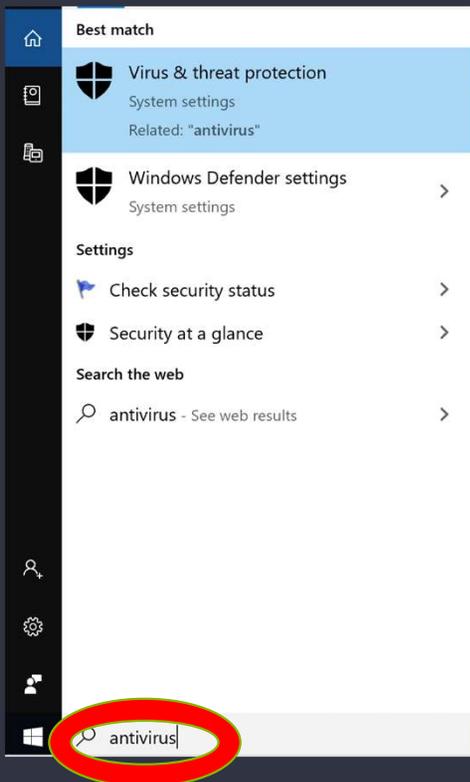


WHY IS **ANTIVIRUS** IMPORTANT?

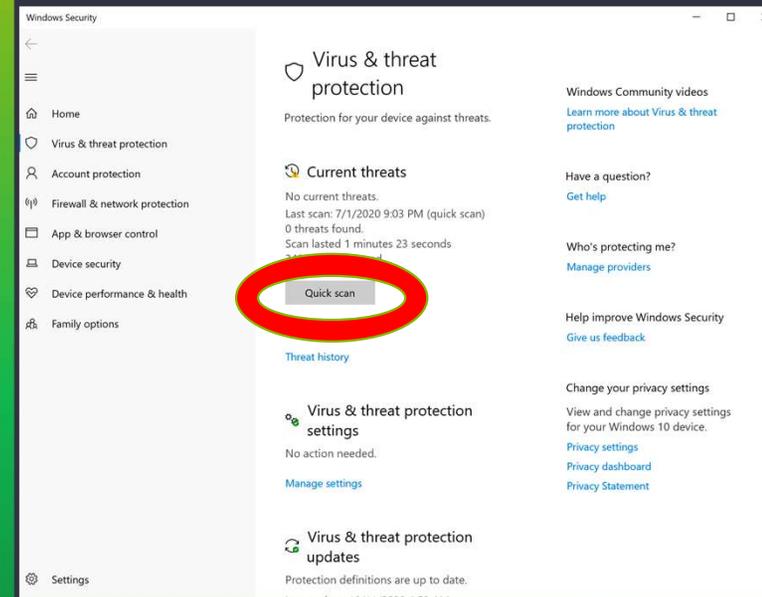
Configuration of Antivirus

- Built-in Antivirus
- Addition Antivirus
- Malware Protection

Just type the word 'antivirus' in the search by text box in Windows.



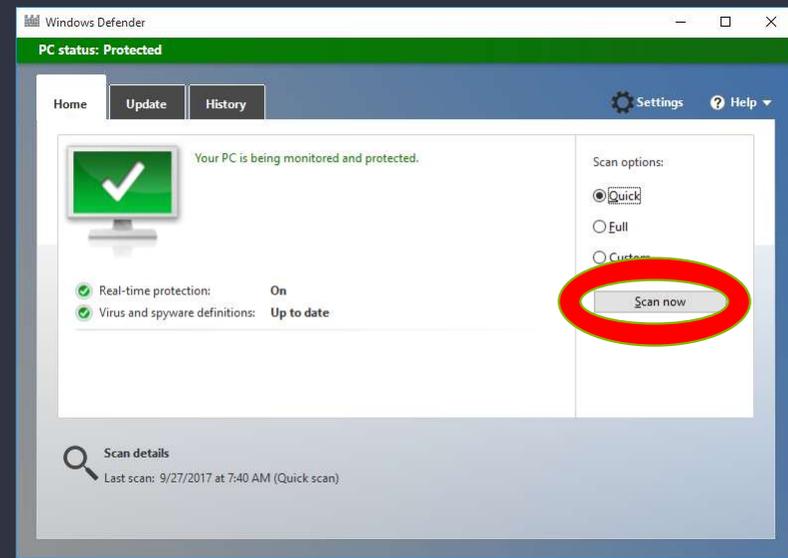
Click the the quick scan button.



VIRUS PROTECTION

Key Points to Remember

- Ensure automatic antivirus updates are active
- Complete a quick scan
- Then make sure scheduled scans are active
- Use cautious navigation on the web to only known sites
- Be vigilant of email attachments from unknown or also known email addresses



Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Threat definitions

Windows Defender Antivirus uses files called definitions to detect threats. We try to automatically download the most recent definitions, to help protect your device against the newest threats. You can also manually check for updates.

Threat definition version: 1.325.586.0
Version created on: 10/11/2020 6:17 AM
Last updated on: 10/11/2020 4:59 AM

APPLE MAC OS

🍏 Antivirus not built-in

- Mac does not have a system antivirus native to the MacOS
- However use the same caution navigating the internet and opening email attachments
- There are pay-for antivirus vendors for both Mac OS and Windows





WHAT ABOUT EMAIL **PHISHING**?

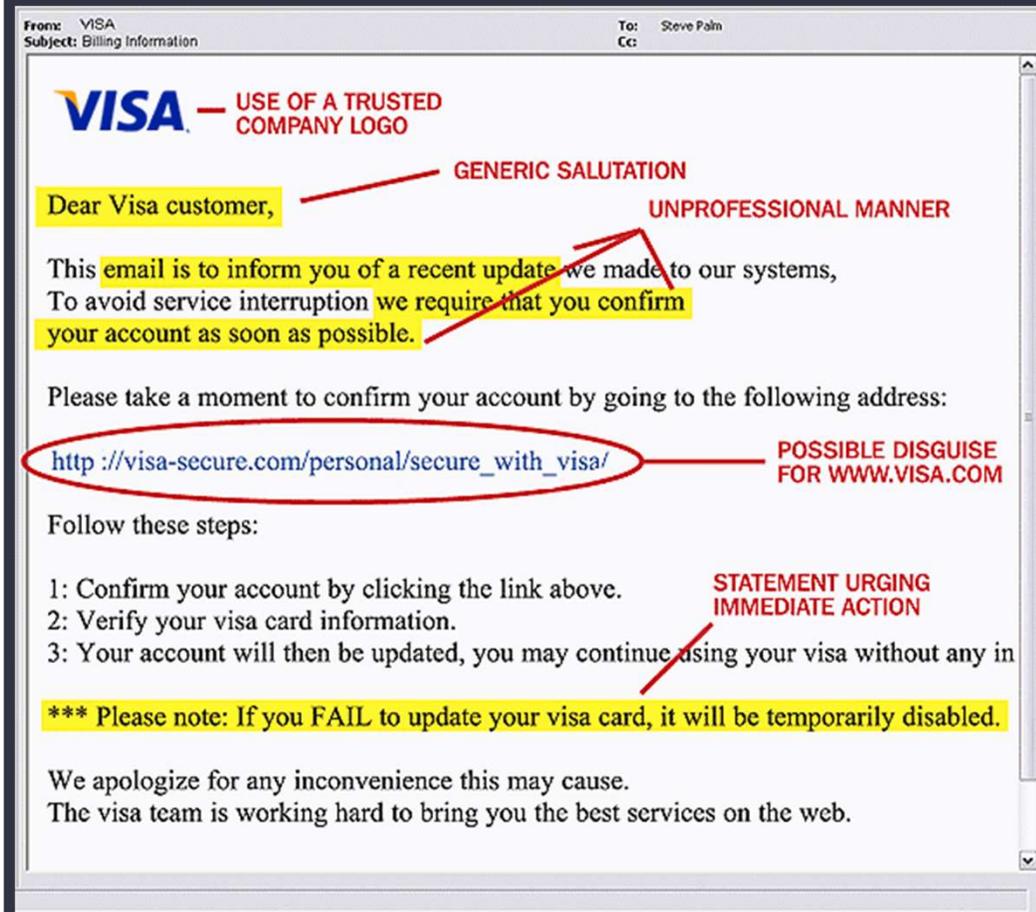
Attackers trick users via email

- “The practice of using fraudulent e-mails and copies of legitimate websites to extract financial data from computer users for purposes of identity theft”
- Phishing emails can deliver malware
- Defense: awareness and identification training

WINDOWS OR MAC OS

Phishing gets them all

- The appearance looks legitimate with familiar graphics and logos
- Attackers can steal your personal credit card or bank information
- Attackers request you to open or download a document, often requiring you to sign in
- Warning signs of an unfamiliar internet address
- Warning signs of immediate urgency



MALWARE

CryptoLocker attack

- An attacker has gained access to your files and encrypted them with their key
- You are locked out of your own files
- The attacker asks the user to pay bitcoins to get their files back
- Even if the ransom is paid, the user may or may not get back their files
- Backups and ability to restore are key



WWW.KNOWBE4.COM/HOMECOURSE

The screenshot shows a web browser window with the URL `training.knowbe4.com/ui/dashboard`. The page is titled "Tools" and lists five security tests, each with a description and a "Get Started" button.

- Free Phishing Security Test**: The Phishing Security Test helps you see how vulnerable your users are to phishing attacks by sending out simulated phishing emails. At the end of the test, you will get a Phish-prone percentage of your users who clicked on the phishing email.
- Free Phishing Reply Test**: The Phishing Reply Test helps you see how vulnerable your users are to falling victim to targeted phishing attacks. This test will track how many of your users reply to a spoofed email.
- Free Social Media Phishing Test**: The Social Media Phishing Test helps you see how vulnerable your users are to social media phishing attacks that mimic platforms like Facebook, LinkedIn, and Twitter. This test will track what percentages of your users will click on a link as well as which users will expose their credentials to these popular social media sites.
- Free Phish Alert Button Add-in**: The Phish Alert Button add-in gives your users a safe way to forward email threats to the security team for analysis. The email is deleted from the user's inbox to prevent future exposure.
- Free USB Security Test**: Find out how your users will react to unknown USBs with KnowBe4's new Free USB Security Test. You can download and rename our special "beaconized" files and place them onto any USB drive(s). Then, label the drive with something enticing and drop the drive at an on-site, high traffic area. If an employee picks it up, plugs it in their workstation, and opens a file, it will "call home" and report the "failure" to your KnowBe4 console. And for Office documents, if the user also enables macros, additional data is tracked and geotagged.

WWW.CYBRARY.IT/COURSE/PHISHING/

← → ↻ cybrary.it/course/phishing/

CYBRARY Browse ▾ Search courses, labs, instructors... Community ▾ Business

The Cybrary Pro Day Sale Starts October 12th
Biggest sale of the year! Discount automatically applied at checkout

Phishing

CYBRARY COURSE

| TIME | DIFFICULTY | CEU/CPE |
|---------|------------|---------|
| 2 hours | Beginner | 2 |

In this online course, you will learn how to craft the perfect phishing email to allow you to teach your team how to avoid actual phishing attempts.

[CREATE FREE ACCOUNT](#) ★★★★★ 3.7 [SHARE](#)

[NEED TO TRAIN YOUR TEAM? LEARN MORE](#)

Start your free 3-day trial and become one of the 3 million Cybersecurity and IT professionals advancing their career goals

SIGN UP WITH

[Facebook](#) [Google](#) [LinkedIn](#)

OR

Email ^{*}

[CREATE FREE ACCOUNT](#)

Already have an account? [Sign In »](#)

END USER SECURITY REVIEW

| NETWORK | UPDATES | BACKUPS | ANTIVIRUS | PHISHING |
|--|---|--|--|--|
| Type 'Firewall' in the search text box | Type 'Update' in the search text box | Type 'Backups' in the search text box | Type 'Antivirus' in the search text box | Take Phishing Awareness security training |
| Turn the computer firewall on | Check for Critical OS Updates | Configure an initial backup | Update antivirus definitions | Be vigilant of suspicious looking emails |
| Use VPN connection if remote | Check for Critical Security Updates | Enable automatic backups | Run an initial virus scan | Never enter credentials, but go directly to the site instead |
| Configure your router firewall with your internet service provider support | Ensure Automatic updates are turned on | Test the restore from backup process | Enable automatic virus scanning | Beware of ransomware – ensure backups and restore process is operational |

THANK YOU

End User & System Protection



Questions?

CUSTOMIZE THIS TEMPLATE

Template Editing
Instructions and Feedback