



# Project Upskill II

Basic Cybersecurity for  
Personal Computers and Mobile Devices

Al Williams

February 11, 2025

# In the first presentation

We want to protect our personal information through cybersecurity but we give away our personal information by agreeing to Privacy Policies.

Review the Privacy Policies of the apps and web pages you're using to determine what personal information you're giving away.

Be aware that you're also giving away your location. You can control app access to location services, but you need an RFID device to block cell tower tracking.

# Can we remove our personal information?

We can't remove our personal information exposed in data breaches because it is in the hands of criminals

We can remove our personal information from data brokers (information resellers)

A good choice is Malwarebytes' *Personal Data Remover*, which remove personal information from 175+ data brokers

# Can we remove our personal information?

But to remove our personal information from web sites and apps, we need to go to each app or web site and ask that our information be removed.

We can choose not to use an app that collects personal information.

We can also choose to delete it so that it can't collect additional personal information.

This Basic Cybersecurity presentation  
provides an overview of best practices.  
For how-to information, see the Source notes  
at the bottom of each slide.

Cybersecurity fatigue is real.  
Please implement just one or two things at a time.  
Pause.  
Implement one or two more things...

Computer Club volunteers are available to help.

Phone: 717-464-6330, option 1

Email: [GetHelp@wvcomputerclub.org](mailto:GetHelp@wvcomputerclub.org)

Website: [wvcomputerclub.org](http://wvcomputerclub.org), click on *Get Help*  
for lists of volunteers

# Massive Amounts of Malware

In the first three quarters of 2023, there were an estimated 5.6 billion attempted malware attacks globally.

560,000 new pieces of malware are detected daily and over 1 billion malware programs exist currently.

Global Malware Attacks Source: *100 Chilling Malware Statistics and Trends (2023-2025)*, Osman Husain, <https://controld.com/blog/malware-statistics-trends/>, 4 February 21, 2025

New Malware Source: *30+ Malware Statistics You Need To Know in 2025*, Nivedita James Palatty, <https://www.getastra.com/blog/security-audit/malware-statistics>, January 9, 2025



# Massive Amounts of Malware

Some threat actors add malware to legitimate software apps and offer the re-packaged software on community forums such as CNET.

# Basic Cybersecurity Concerns

- Vet technologies before using them
- Keep your device's operating system and apps up to date
- Ensure OS Antivirus and Malware Protections are active
- Avoid hardware with known vulnerabilities
- Protect the physical security of your digital devices
- Implement User Account Control to protect your computer
- Manage application permissions for privacy and security

# Vet Technologies Before Using Them

Research the manufacturer, developer, or vendor's track record on privacy and security for products you are considering using.

Check where the company making the product is located and operates.

Check the product's security profile to confirm your data is encrypted and not shared with third parties.

Source: *Vet Technologies Before Adding Them to Your Network*,  
<https://www.cisa.gov/resources-tools/training/vet-technologies-adding-them-your-network>,  
Retrieved January 21, 2025

# Vet Technologies Before Using Them

Confirm that the vendor has an acceptable privacy policy.

Confirm that you can change the product's settings to meet your cybersecurity needs.

Confirm that the developer issues regular security updates for your product(s).

Source: *Vet Technologies Before Adding Them to Your Network*,  
<https://www.cisa.gov/resources-tools/training/vet-technologies-adding-them-your-network>,  
Retrieved January 21, 2025

# Basic Cybersecurity Concerns

- Vet technologies before using them
- Keep your device's operating system and apps up to date
- Ensure OS Antivirus and Malware Protections are active
- Avoid hardware with known vulnerabilities
- Protect the physical security of your digital devices
- Implement User Account Control to protect your computer
- Manage application permissions for privacy and security



Don't let criminals access your personal information  
by using software  
with known vulnerabilities

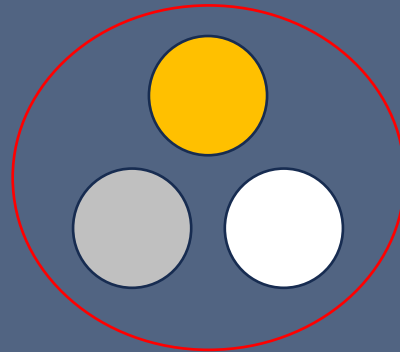
# An Illustration

Assume:

Some of your information is very important – GOLD

Some of your information is somewhat important - SILVER

Some isn't important - WHITE

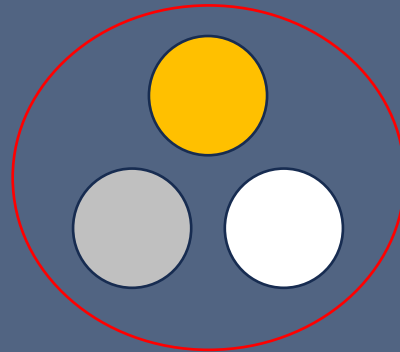


All of your information  
is inside the red circle.

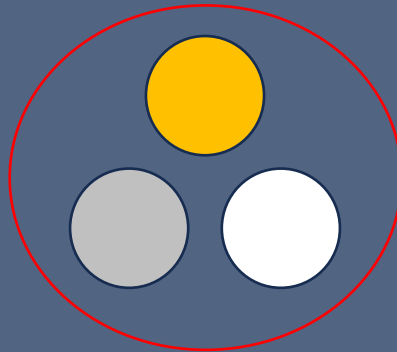


Software apps

What software has access to  
your information?



Operating  
system



The operating system is the Executive software for the computing device. The operating systems are listed in the recommended order:

Cell Phone:

GrapheneOS

iOS

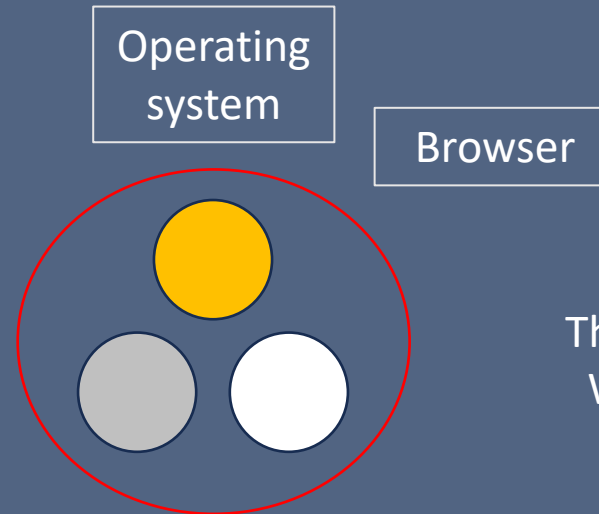
Android

Desktop or Laptop:

A Linux distribution

macOS

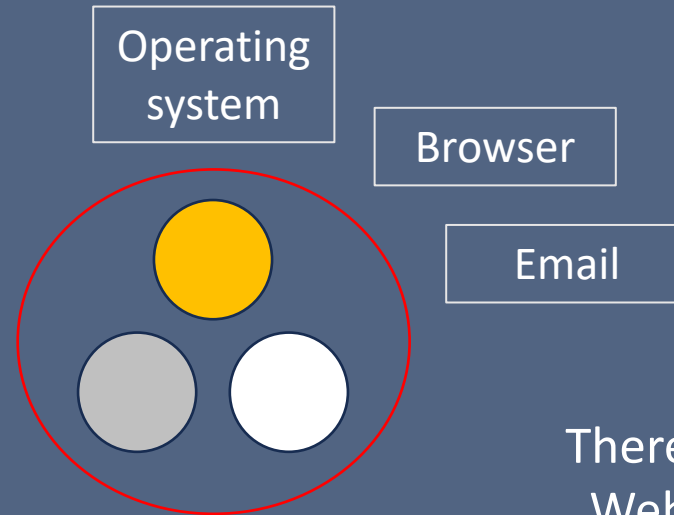
Windows



The browser could be:  
Windows, macOS  
Firefox (Recommended)  
Brave  
iOS (iPhone, iPad)  
Safari

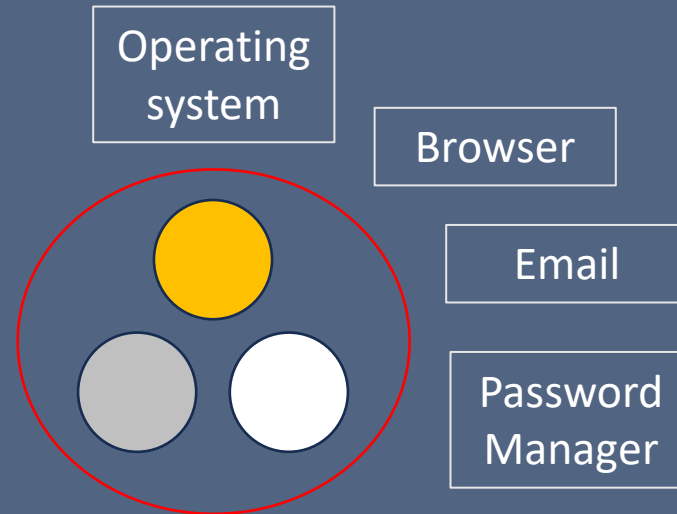
Chrome (Not recommended)  
and many others

We'll cover Browsers on April 22



There are many email clients  
Webmail (using browser)  
Mail on iOS  
Mail on Android  
Thunderbird (Windows, macOS,  
Linux)  
and many others

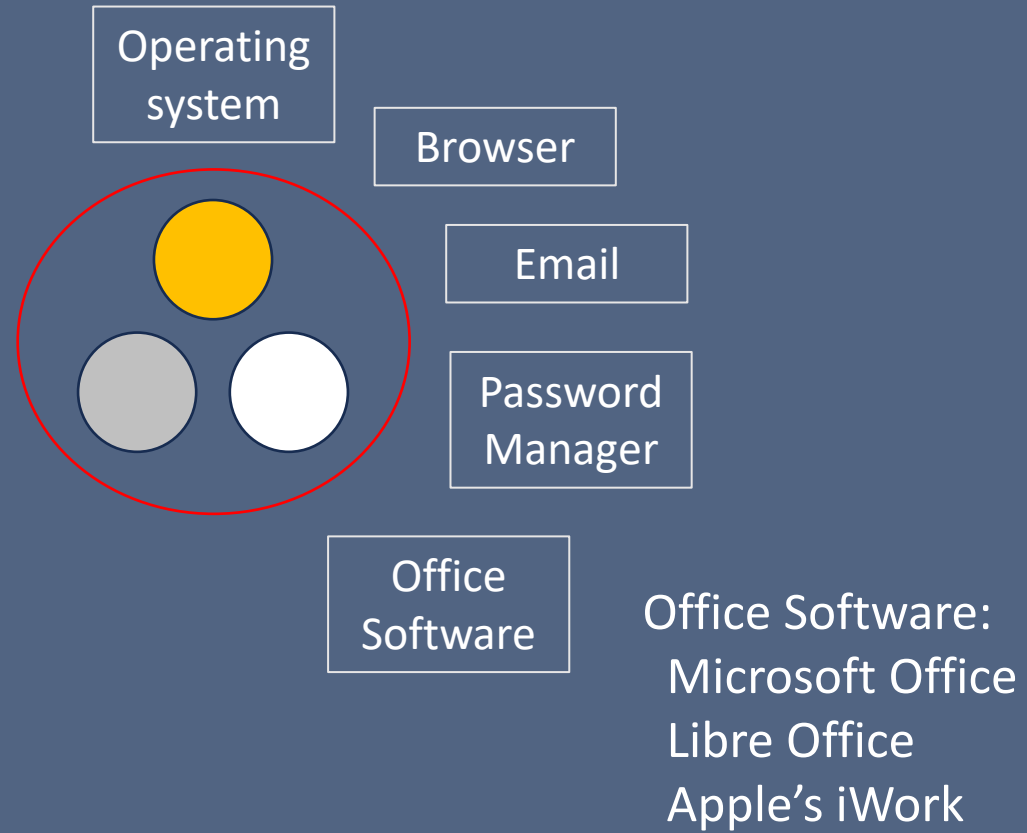
We'll cover Email on April 22

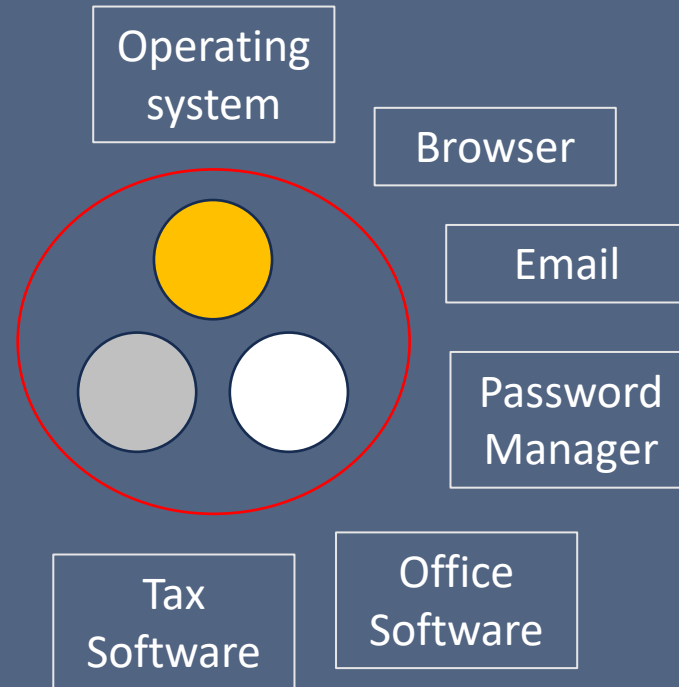


Password managers:  
Bitwarden (Recommended)  
1Password

We'll cover Password Managers on February 25

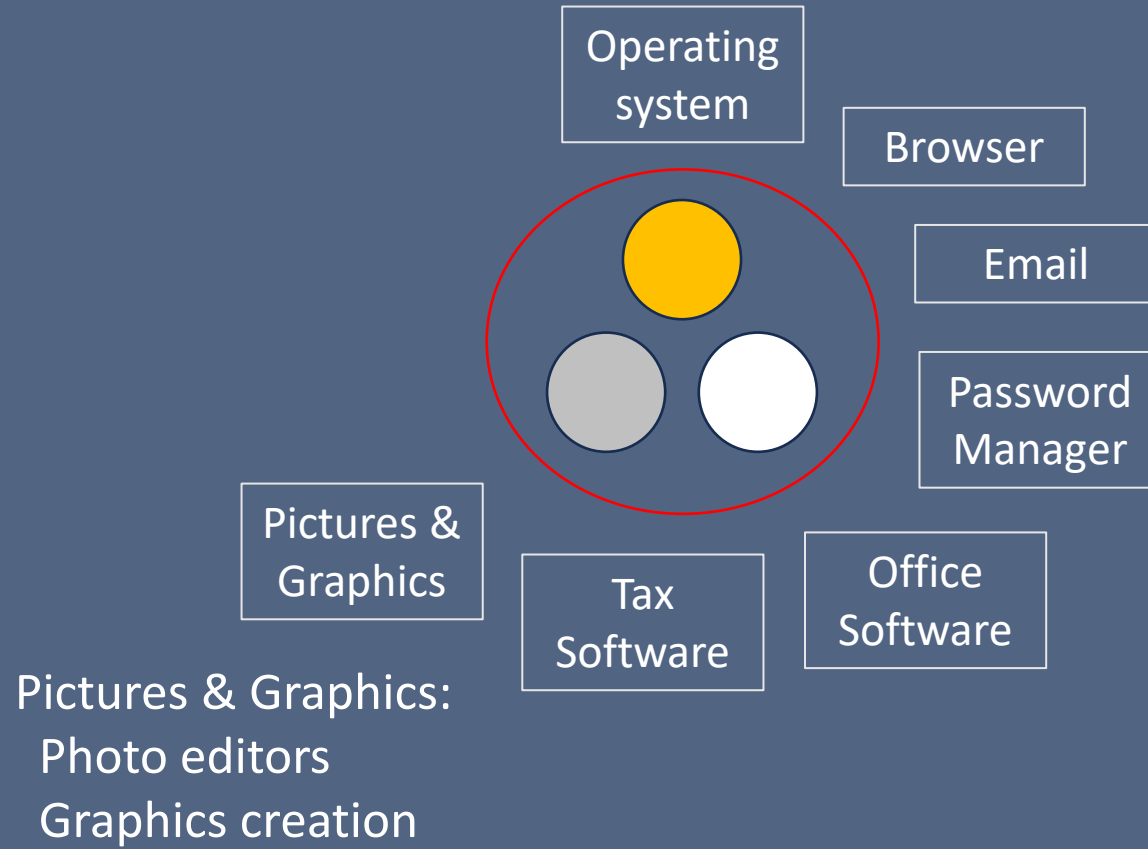
And in the future (more time for maturity is needed):  
Apple's Passwords  
Proton's Pass





Tax Software:  
TurboTax  
Others





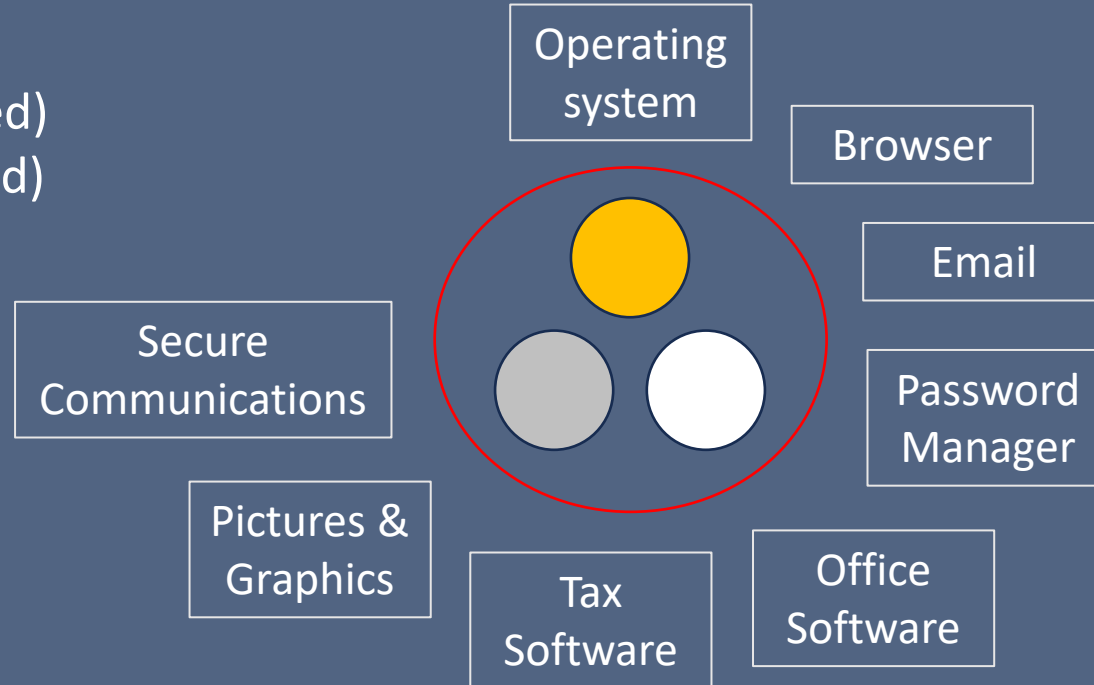
## Secure Communications:

Signal (Recommended)

Proton Mail (Recommended)

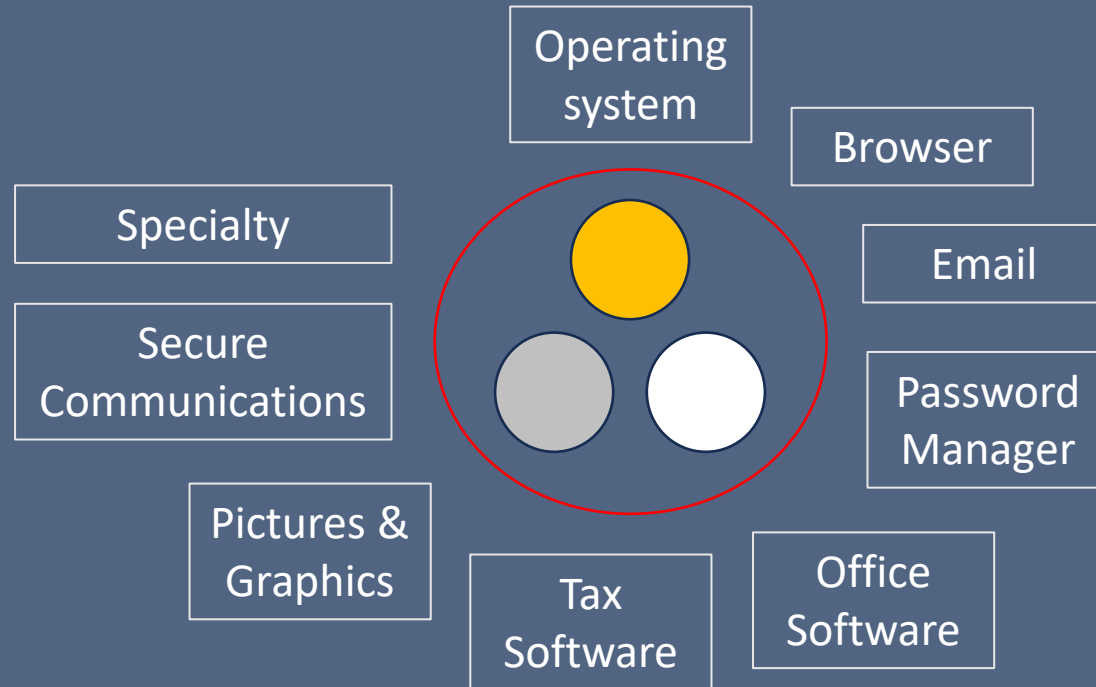
Proton VPN (Recommended)

And others



We'll cover Secure Communications on March 25

Specialty:  
Genealogy  
Obsidian (note taking)  
And others



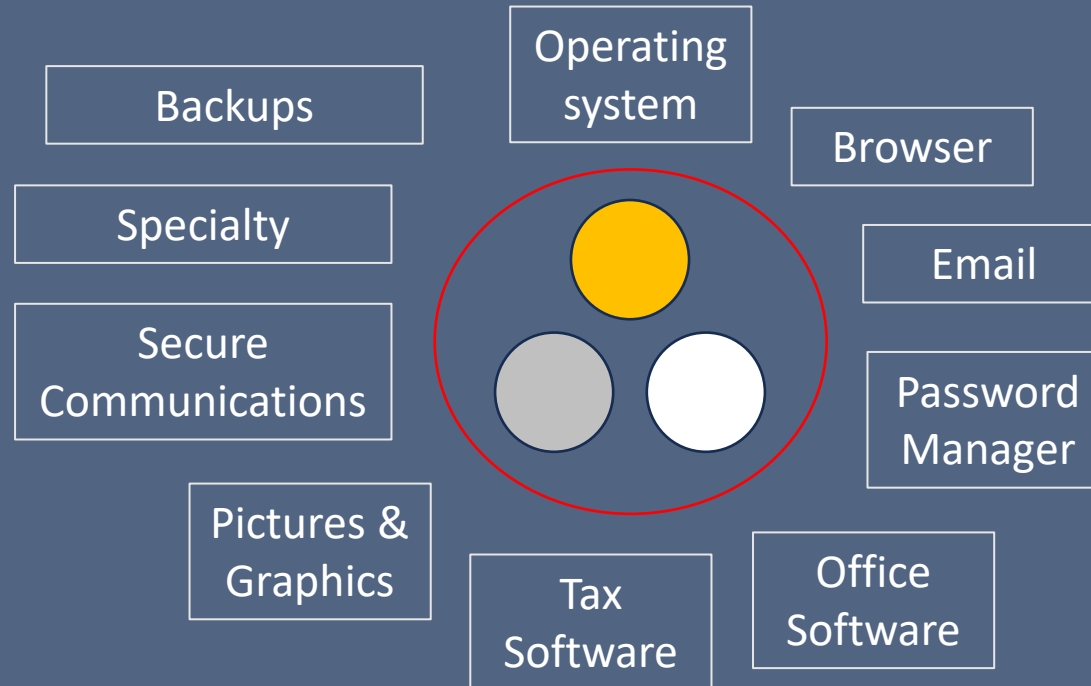
Backups:

Proton Drive (Recommended)

Macrium Reflect (Recommended)

One Drive

And others



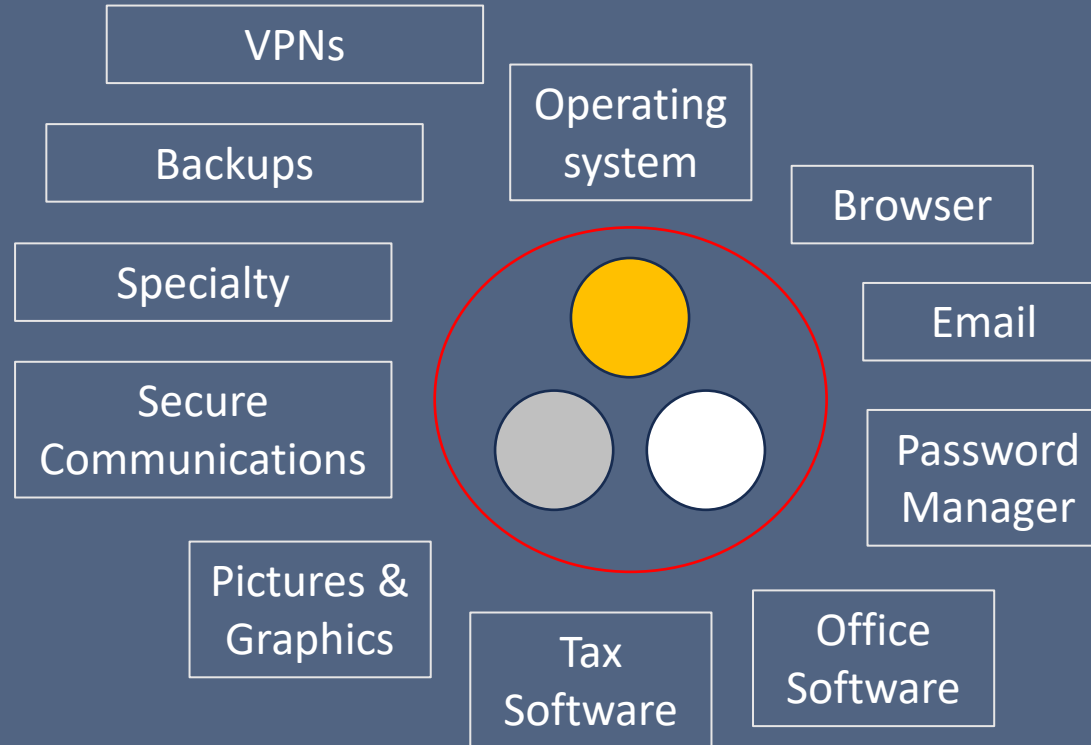
We'll cover Backups on March 11

VPNs:

Proton VPN (Recommended)

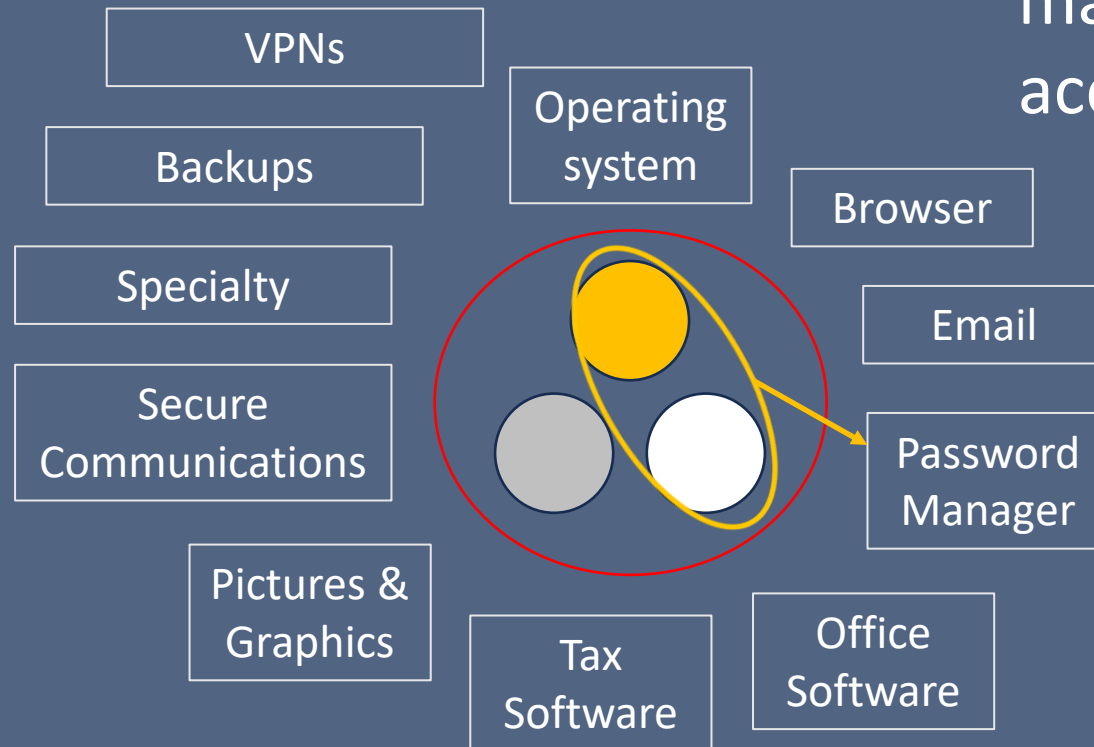
Mullvad VPN

And others



We'll cover Virtual Private Networks (VPNs) May 13

Move sensitive information to a password manager to minimize access by other software.



We'll cover Password Managers on February 25

# Keep Operating Systems and Apps Up to Date

- Routinely update the OS and apps on all your devices
- Enable automatic updates for your OS and apps when available.
- For operating systems and apps without automatic updates, set aside a time in your schedule to check for and install updates manually.

Source: *Keep Your Device's Operating System and Applications Up to Date*,  
<https://www.cisa.gov/resources-tools/training/keep-your-devices-operating-system-and-applications-date>, Retrieved January 21, 2025

# Keep Operating Systems and Apps Up to Date

- Ensure you install updates from official sources, such as your device's standard OS update feature or a trusted app store.
- Exercise caution if prompted to install an update through a browser pop-up or email, as these may be phishing attempts.
- Remove (delete) any apps you are not using.

Source: *Keep Your Device's Operating System and Applications Up to Date*,  
<https://www.cisa.gov/resources-tools/training/keep-your-devices-operating-system-and-applications-date>, Retrieved January 21, 2025



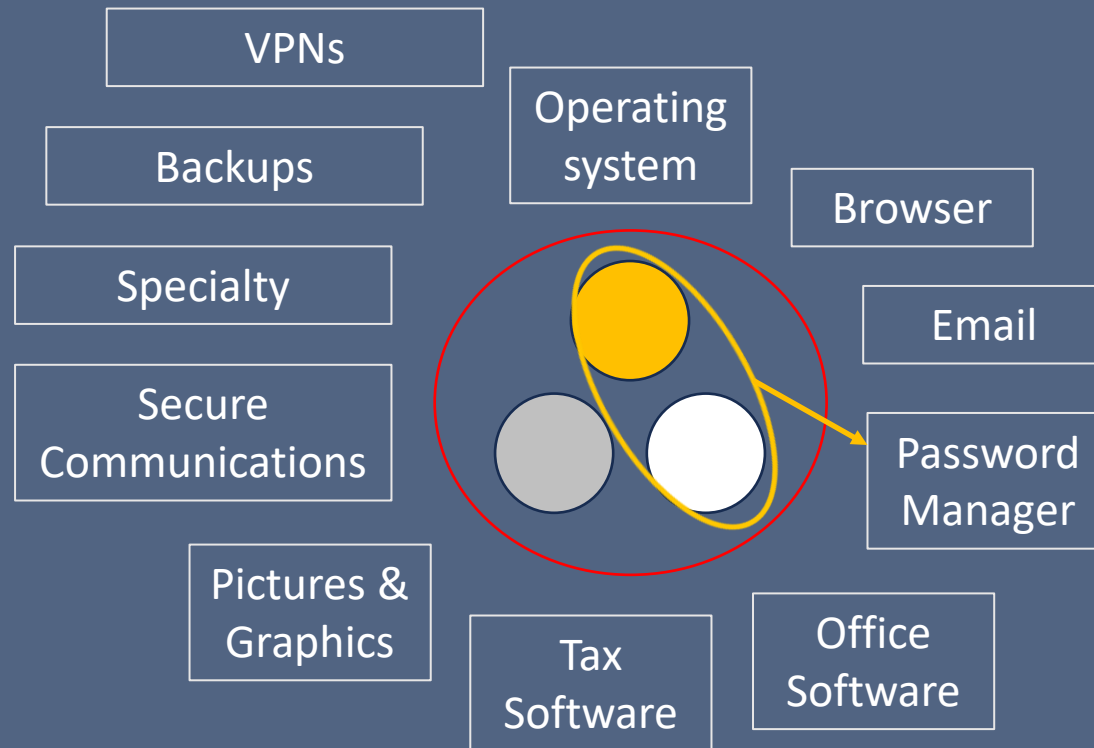
# Keep Operating Systems and Apps Up to Date

- For detailed how-to instructions for Windows, macOS, iOS, and Android, see the CISA Source below.
- If you're using Windows and not using a Microsoft account, use *Patch My PC Home Updater*  
<https://patchmypc.com/product/home-updater>

Source: *Keep Your Device's Operating System and Applications Up to Date*,  
<https://www.cisa.gov/resources-tools/training/keep-your-devices-operating-system-and-applications-date>, Retrieved January 21, 2025

# Basic Cybersecurity Concerns

- Vet technologies before using them ✓
- Keep your device's operating system and apps up to date ✓
- Ensure OS Antivirus and Malware Protections are active
- Avoid hardware with known vulnerabilities
- Protect the physical security of your digital devices
- Implement User Account Control to protect your computer
- Manage application permissions for privacy and security



# Malware

Malware is also software.

Sometimes malware is embedded in real software. The software does what it is supposed to do, while the malware steals personal information.

# Malware causes harm and exploits vulnerabilities

Steals sensitive information such as login credentials, credit card numbers, social security numbers and other data

Disrupts operations through ransomware or denial-of-service attacks

Gains unauthorized access through backdoors to remotely access or control a system or spyware to monitor or collect personal information

Destroys data or damages computing devices

# Malware causes harm and exploits vulnerabilities

Spreads misinformation, manipulate public opinion, or interfere with political processes

Source: *Malware, Phishing, and Ransomware*, <https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>, No Date

Source: *What Is the Purpose of Malware?*, <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware>, No Date

Source: *Identity theft is being fueled by AI & cyber-attacks*, Kennedy Meda, <https://www.thomsonreuters.com/en-us/posts/government/identity-theft-drivers>, 3 May 2024

Source: *What Is the Purpose of Malware?* Prompt, Gemini 1.5 Flash, January 14, 2025

# AntiMalware recommendations

## Cell phones

### iPhones

- have iOS Security and App Store Security

- have “Find My” feature allowing remote wiping

- Malwarebytes

### Android phones

- Use Google Play Protect to keep apps safe and data private

- Malwarebytes

- Bitdefender Mobile Security

Source: *Use Google Play Protect to help keep your apps safe & your data private*,  
<https://support.google.com/googleplay/answer/2812853>, Retrieved Jan 21, 2025

# Antimalware recommendations

Desktops and laptops

macOS

- Has a three-layer defense against malware

  - Prevents the launch or execution of malware

  - Blocks malware from running

  - Remediates malware that has executed

- Malwarebytes for Mac

- Bitdefender Antivirus for Mac

Source: *Protecting against malware in macOS*, <https://support.apple.com/en-bw/guide/security/sec469d47bd8/web>, Retrieved Jan 21, 2025

# Antimalware recommendations

Desktops and laptops

Linux distributions

Bitdefender

ClamAV



# Antimalware recommendations

For how-to instructions for  
Windows,  
macOS,  
iOS,  
Android  
see the CISA Source below.

Source: *Ensure Your OS Antivirus and Anti-Malware Protections are Active*,  
<https://www.cisa.gov/resources-tools/training/ensure-your-os-antivirus-and-anti-malware-protections-are-active>, Retrieved Feb 6, 2025

# Basic Cybersecurity Concerns

- Vet technologies before using them ✓
- Keep your device's operating system and apps up to date ✓
- Ensure OS Antivirus and Malware Protections are active ✓
- Avoid hardware with known vulnerabilities
- Protect the physical security of your digital devices
- Implement User Account Control to protect your computer
- Manage application permissions for privacy and security

Don't let criminals access your personal information  
by using hardware devices  
with known vulnerabilities

# Best Hardware Practices

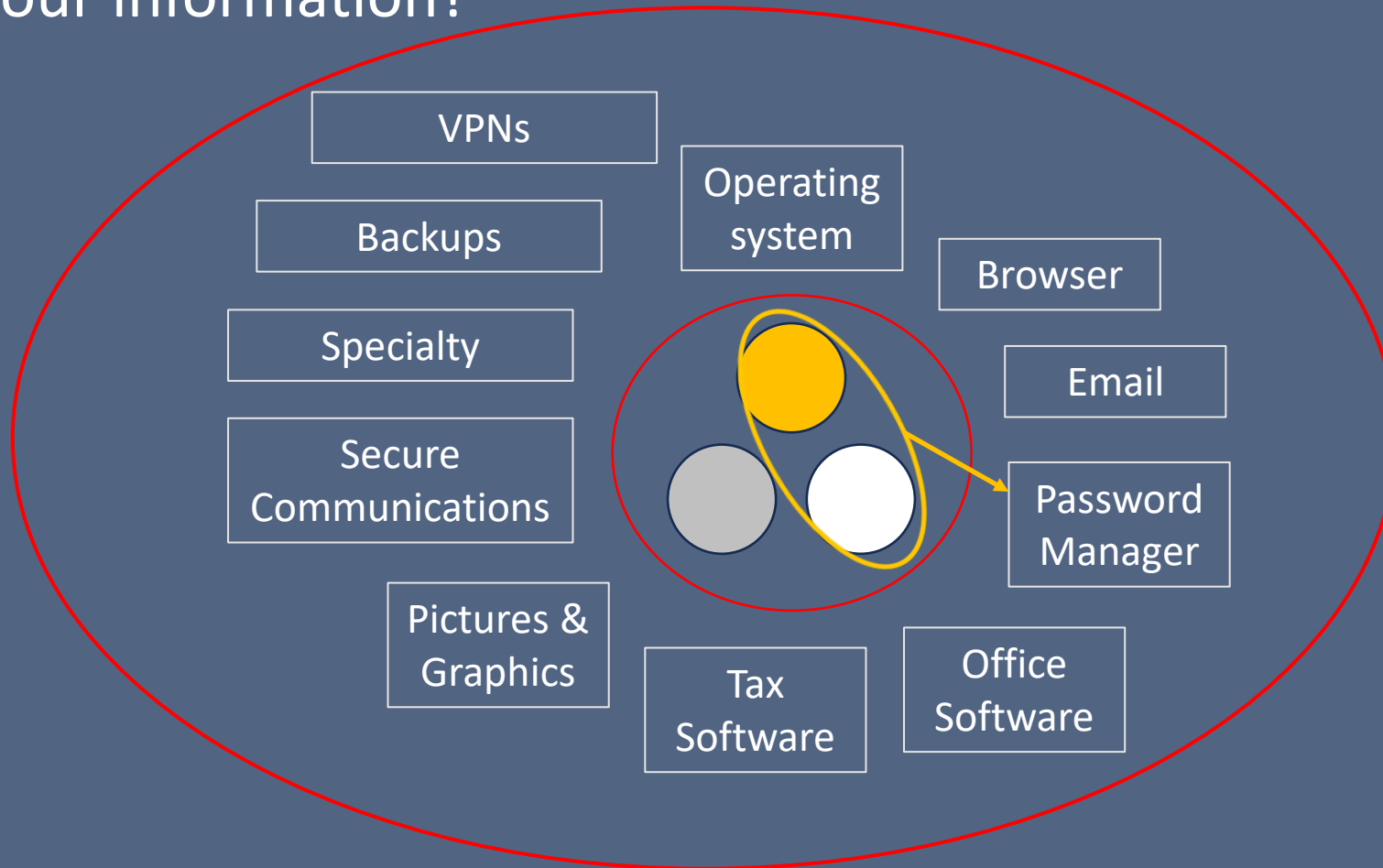
Purchase and use hardware devices from reputable vendors (not headquartered in China or Russia)

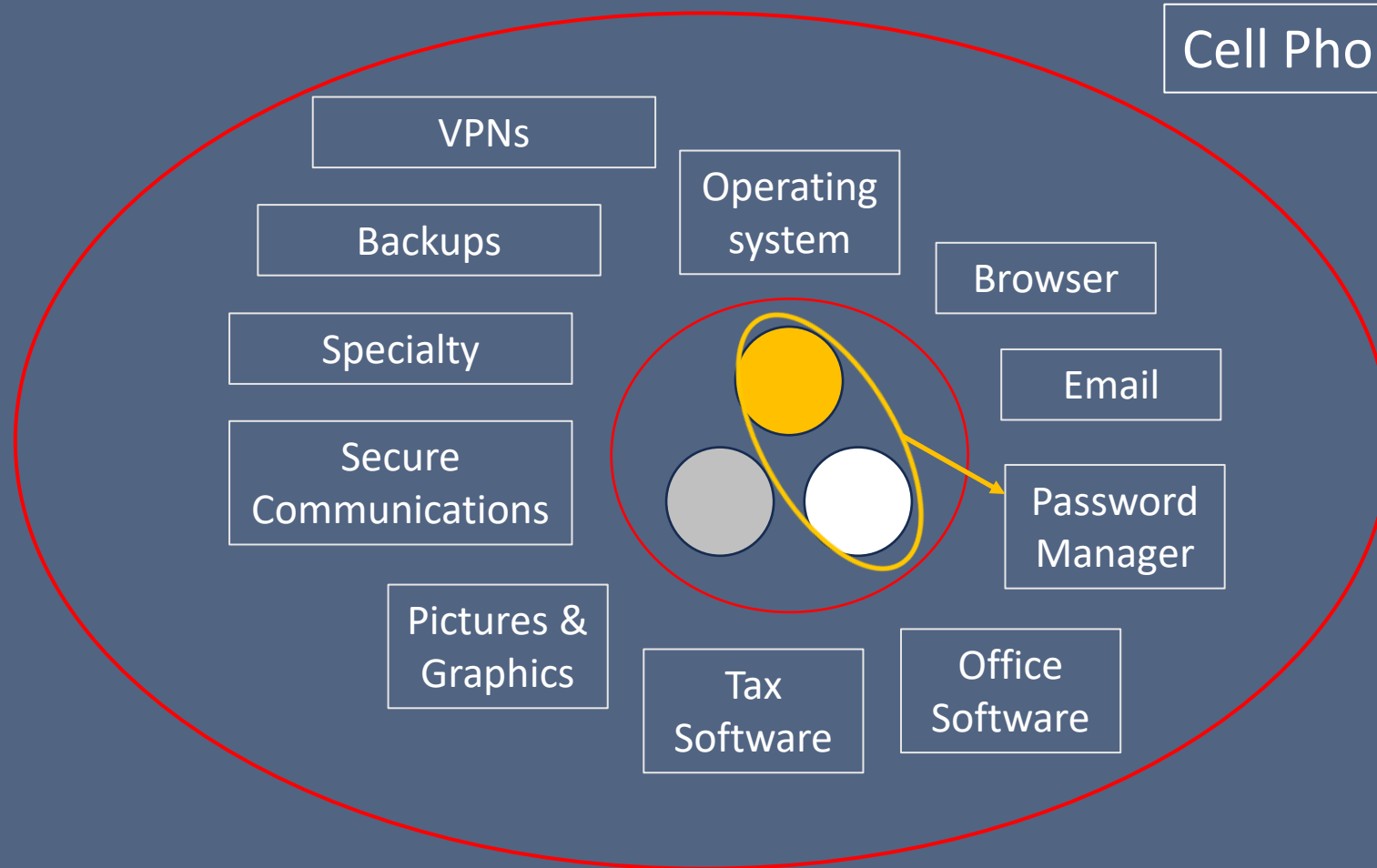
Replace the device after 5 to 7 years

Turn off and dispose of any hardware devices you are not using

Don't discard computers and cell phones until they're "scrubbed"

What hardware devices have access to your information?





Cell Phones

Vendors:  
Apple  
Google  
Samsung (South Korea)  
Sony (Japan)



Cell Phones

Towers - Desktop

Vendors:

HP

Dell

Falcon Northwest

Origin PC

System76

Asus (Taiwan)

Acer (Taiwan)



Cell Phones

Towers - Desktop

Laptops

Vendors:

HP

Dell

Falcon Northwest

Origin PC

System76

Asus (Taiwan)

Acer (Taiwan)





Cell Phones

Towers - Desktop

Laptops

Keyboards

Vendors:  
Logitech  
Razer



Cell Phones

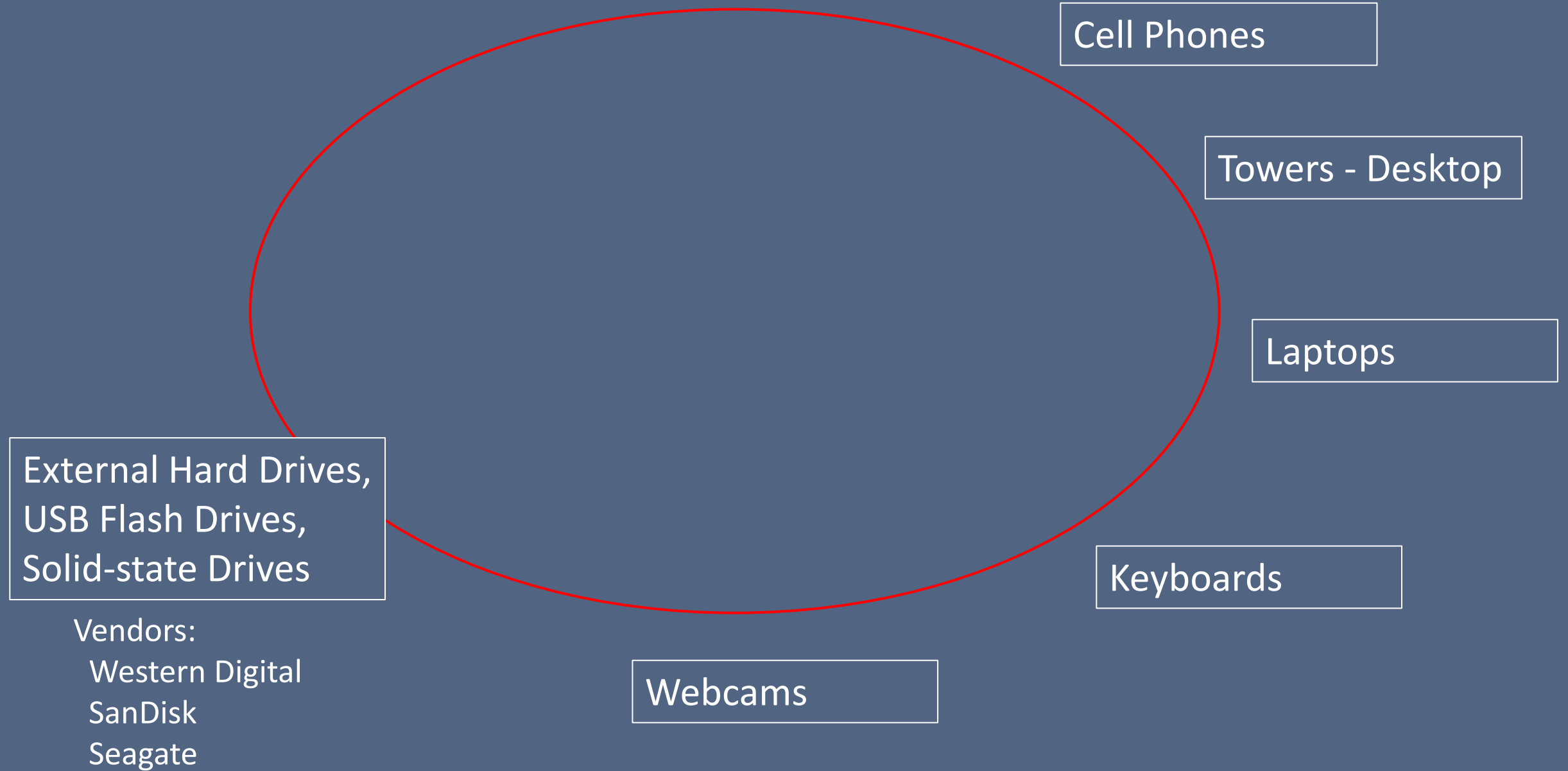
Towers - Desktop

Laptops

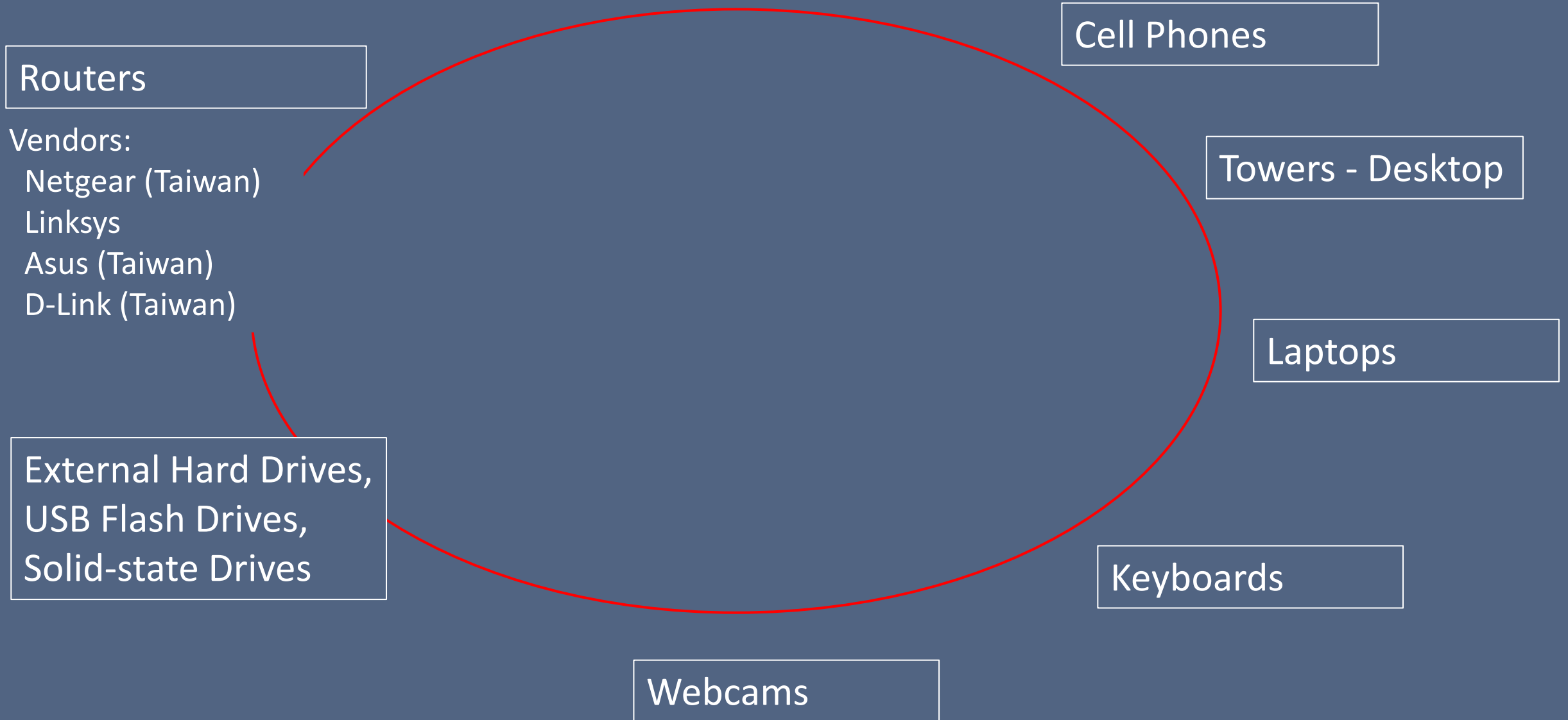
Keyboards

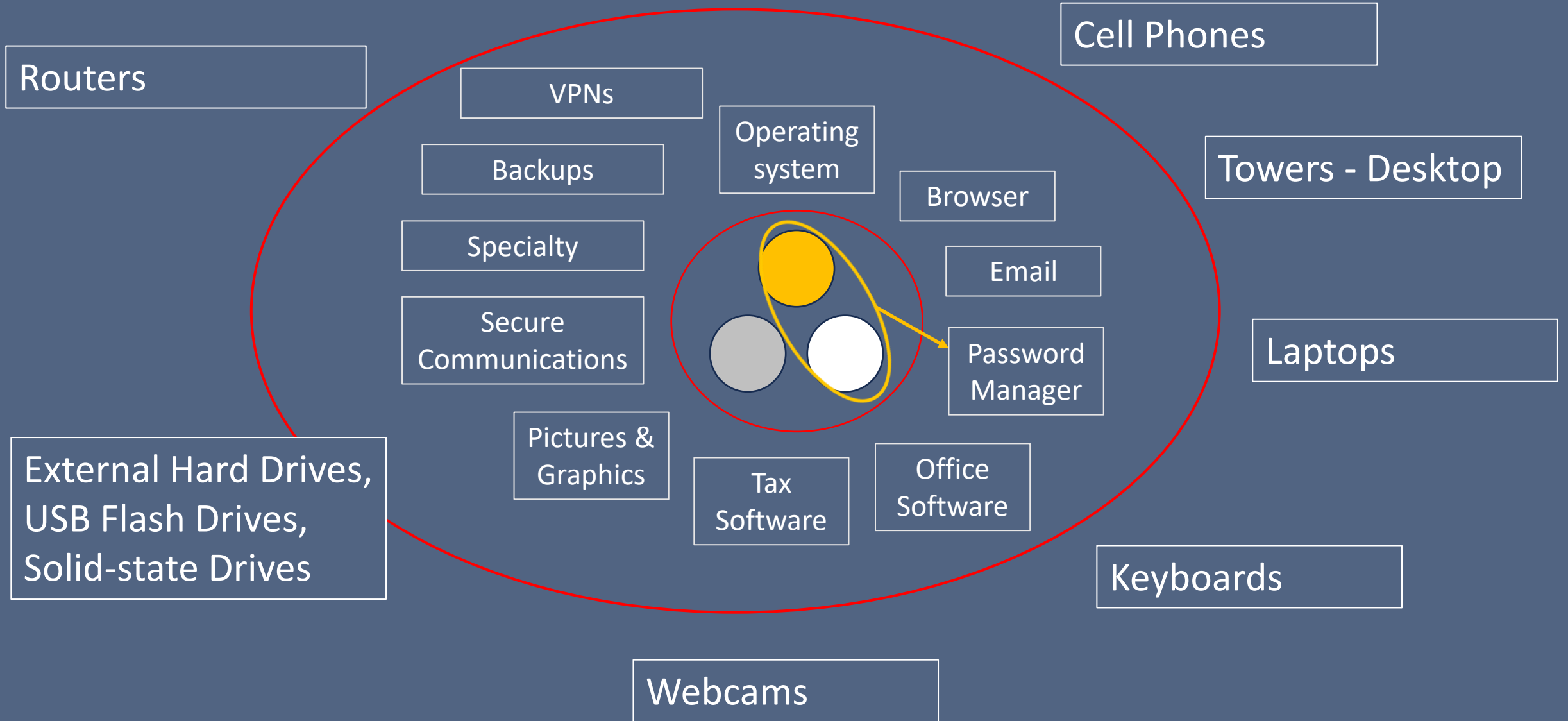
Vendors:  
Logitech  
Microsoft

Webcams



TP-Link routers are made by a company headquartered in China. They consistently have multiple vulnerabilities that are being exploited. TP-Link routers are *not* recommended.





# Basic Cybersecurity Concerns

- Vet technologies before using them ✓
- Keep your device's operating system and apps up to date ✓
- Ensure OS Antivirus and Malware Protections are active ✓
- Avoid hardware with known vulnerabilities ✓
- Protect the physical security of your digital devices
- Implement User Account Control to protect your computer
- Manage application permissions for privacy and security

# The Physical Security Problem

Without physical safeguards, these compromises could happen:

- Direct installation of malware or spyware

- Loss or theft of computing devices or your personal data

- Unauthorized access of your personal data

# Protect Your Device's Physical Security - Access

- Ensure there are physical security controls in the areas where you store your devices

To protect your devices (including your home Wi-Fi router), keep them locked in a secure physical area with limited access by others (*lock your apartment or house when you aren't home*).

- Keep important documents in a secure location

Documents containing security information, such as the master password to your password manager, should be kept in a safe or similar security system

Source: *Protect the Physical Security of Your Digital Devices*, <https://www.cisa.gov/resources-tools/training/protect-physical-security-your-digital-devices>, Retrieved Jan 21, 2025



# Protect Your Device's Physical Security – Access

- Lock your device if you have to step away from the screen
  - Especially in a public area
  - Auto-lock the screen if the device is idle for more than 15 minutes
- Do not leave your devices unattended in a public space

Source: *Protect the Physical Security of Your Digital Devices*, <https://www.cisa.gov/resources-tools/training/protect-physical-security-your-digital-devices>, Retrieved Jan 21, 2025

# Protect Your Device's Physical Security - Loss

- Have a plan for data loss or theft
- Regularly back up your computers or mobile devices
- Have a plan to reduce further damage if your device is stolen
  - Use remote factory reset for mobile devices
  - Use full disk encryption for laptops / desktops
- Make a list of all accounts that your devices are automatically logged into, such as email and messaging apps, so that you can immediately reset those account passwords

Source: *Protect the Physical Security of Your Digital Devices*, <https://www.cisa.gov/resources-tools/training/protect-physical-security-your-digital-devices>, Retrieved Jan 21, 2025

# Protect Your Device's Physical Security - Dispose

- Do not throw away or sell your old devices  
Protect your personal information on your device first
- Windows: *Before you recycle, sell, or gift your Xbox or Windows PC,*  
<https://support.microsoft.com/en-us/account-billing/before-you-recycle-sell-or-gift-your-xbox-or-windows-pc-78ee8071-c8ab-40c4-1d89-f708582062e4>
- macOS: *What to do before you sell, give away, trade in, or recycle your Mac,*  
<https://support.apple.com/en-us/102773>
- iOS: *What to do before you sell, give away, trade in, or recycle your iPhone or iPad,*  
<https://support.apple.com/en-us/109511>
- Android: *Reset your Android device to factory settings,*  
<https://support.google.com/android/answer/6088915?hl=en>

Source: *Protect the Physical Security of Your Digital Devices*, <https://www.cisa.gov/resources-tools/training/protect-physical-security-your-digital-devices>, Retrieved Jan 21, 2025

# Protect Your Device's Physical Security - Usage

- Do not insert unknown media storage devices (e.g., thumb drives) into your computer.  
It may contain malicious software that will infect your computer.
- Do not charge your device in a public USB port without a data blocker  
Don't plug your phone into a rental vehicle's USB port  
The threat is low but it can happen

Source: *Protect the Physical Security of Your Digital Devices*, <https://www.cisa.gov/resources-tools/training/protect-physical-security-your-digital-devices>, Retrieved Jan 21, 2025

# Basic Cybersecurity Concerns

- Vet technologies before using them ✓
- Keep your device's operating system and apps up to date ✓
- Ensure OS Antivirus and Malware Protections are active ✓
- Avoid hardware with known vulnerabilities ✓
- Protect the physical security of your digital devices ✓
- Implement User Account Control to protect your computer
- Manage application permissions for privacy and security

# Implement User Account Control

- When you set up your computer, usually you'll be asked to set up an Administrator account.
- Administrator accounts make it easier for threat actors to access your data or make changes to your computer, effectively taking over your computer.
- A Standard account requires an administrator password to install software.
- To set up a Standard account, see the how-to information at the below CISA Source.

Source: *Implement User Account Control to Protect Your Personal Computer*,  
<https://www.cisa.gov/resources-tools/training/implement-user-account-control-protect-your-personal-computer>, Retrieved Feb 6, 2025

# Basic Cybersecurity Concerns

- Vet technologies before using them ✓
- Keep your device's operating system and apps up to date ✓
- Ensure OS Antivirus and Malware Protections are active ✓
- Avoid hardware with known vulnerabilities ✓
- Protect the physical security of your digital devices ✓
- Implement User Account Control to protect your computer ✓
- Manage application permissions for privacy and security

# Manage Application Permissions

- Apps can access personal information about you.
- Only install apps you need.
- Remove apps you no longer use.
- Manage app permissions to deny access to data or functions you do not want an app to have.
- How-to information for managing app permissions on iOS, Android, macOS, and Windows is at the CISA Source below.

Source: *Manage Application Permissions for Privacy and Security*,  
<https://www.cisa.gov/resources-tools/training/manage-application-permissions-privacy-and-security>, Retrieved Feb 6, 2025



# Basic Cybersecurity Concerns

- Vet technologies before using them ✓
- Keep your device's operating system and apps up to date ✓
- Ensure OS Antivirus and Malware Protections are active ✓
- Avoid hardware with known vulnerabilities ✓
- Protect the physical security of your digital devices ✓
- Implement User Account Control to protect your computer ✓
- Manage application permissions for privacy and security ✓

Thank You,

Bill Skelly

Computer Club volunteers are available to help.

Phone: 717-464-6330, option 1

Email: [GetHelp@wvcomputerclub.org](mailto:GetHelp@wvcomputerclub.org)

Website: [wvcomputerclub.org](http://wvcomputerclub.org), click on *Get Help*  
for lists of volunteers

The slides for this presentation will be available on our website, [wvcomputerclub.org](http://wvcomputerclub.org), under *Presentations* in the next few days.

An email will be sent notifying Computer Club members when the slides are available.

*Protecting Your Accounts from Compromise*

February 25, Tuesday, 10 am

Cultural Center Education Room

# Articles

For the latest cybersecurity information, these are accurate and reliable sources:

*Ars Technica*

[arstechnica.com](https://arstechnica.com)

*Bleeping Computer*

[bleepingcomputer.com](https://bleepingcomputer.com)

*CISA*

[cisa.gov](https://cisa.gov)

*Forbes*

[forbes.com](https://forbes.com)

*Proton Blog*

[proton.me/blog](https://proton.me/blog)

*Proton VPN Blog*

[protonvpn.com/blog](https://protonvpn.com/blog)

# Books

*Beginner's Introduction to Privacy*, Naomi Brockwell, (Independently Published, 2023)

*Means of Control: How the Hidden Alliance of Tech and Government is Creating a New American Surveillance State*, Bryon Tau, (Crown, 2024)

*Your Face Belongs to Us: A Tale of AI, A Secretive Startup, and the End of Privacy*, Kashmir Hill, (Crown, 2024)

*Extreme Privacy: What It Takes To Disappear, 5<sup>th</sup> Edition*, Michael Bazzell, (Independently Published, 2024)

*Firewalls Don't Stop Dragons, 5<sup>th</sup> Edition*, Carey Parker, (Apress, 2024)

# YouTube Channels

*David Bombal*, [Cybersecurity, Privacy, IT] <https://www.youtube.com/@davidbombal>

*Naomi Brockwell TV*, [Privacy]  
<https://www.youtube.com/channel/UCSuHzQ3GrHSzoBbwrlq3LLA>

*PC Security Channel*, [Cybersecurity, Malware]  
[https://www.youtube.com/channel/UCKGe7fZ\\_S788Jaspxg-\\_5Sg](https://www.youtube.com/channel/UCKGe7fZ_S788Jaspxg-_5Sg)



Questions?