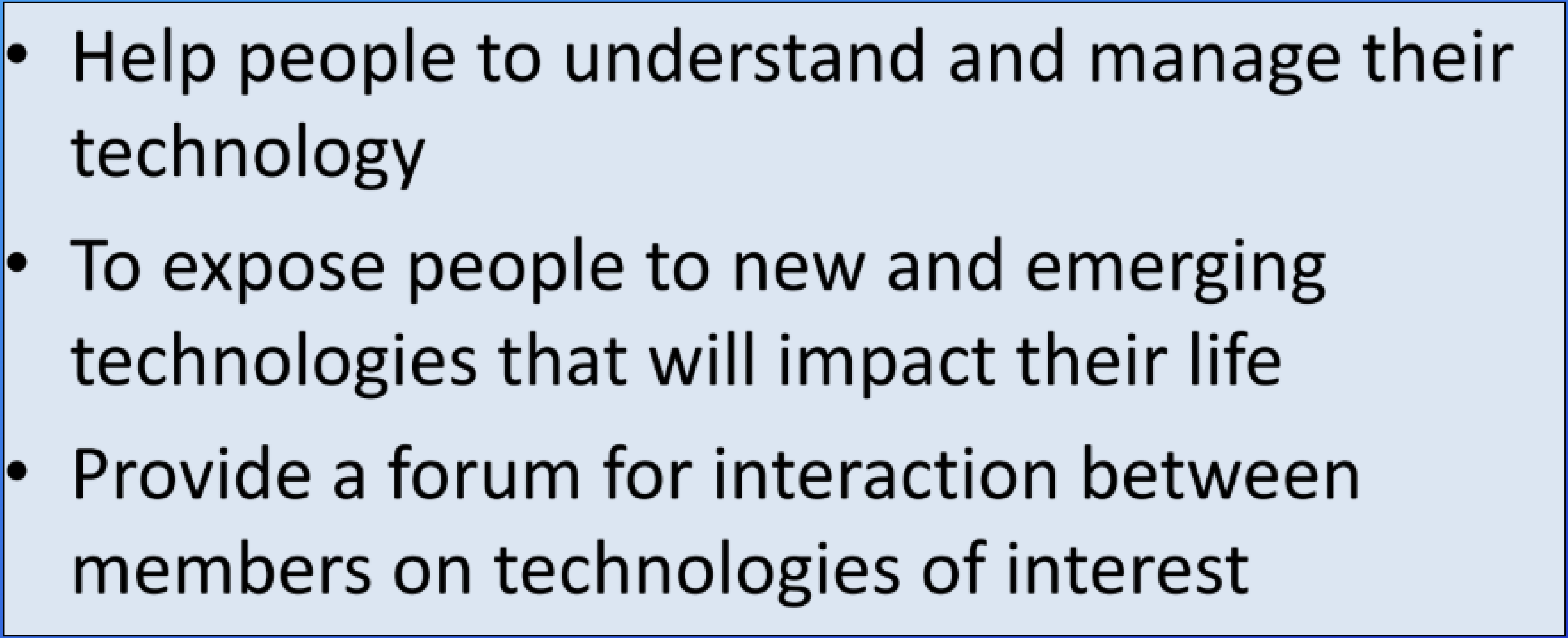
Deerfield Beach Computer Club

FEBRUARY 21, 2020

WELCOME TO CLASS

Our Mission



- Help people to understand and manage their technology
- To expose people to new and emerging technologies that will impact their life
- Provide a forum for interaction between members on technologies of interest

DISCLAIMER

Today's presentation is for information, education, and testing purposes only. The Club and CVE do not condone or promote the piracy of legally copyrighted materials. The user is responsible for any legal actions taken as a result of violating the applicable laws.

Staying Secure With A VPN

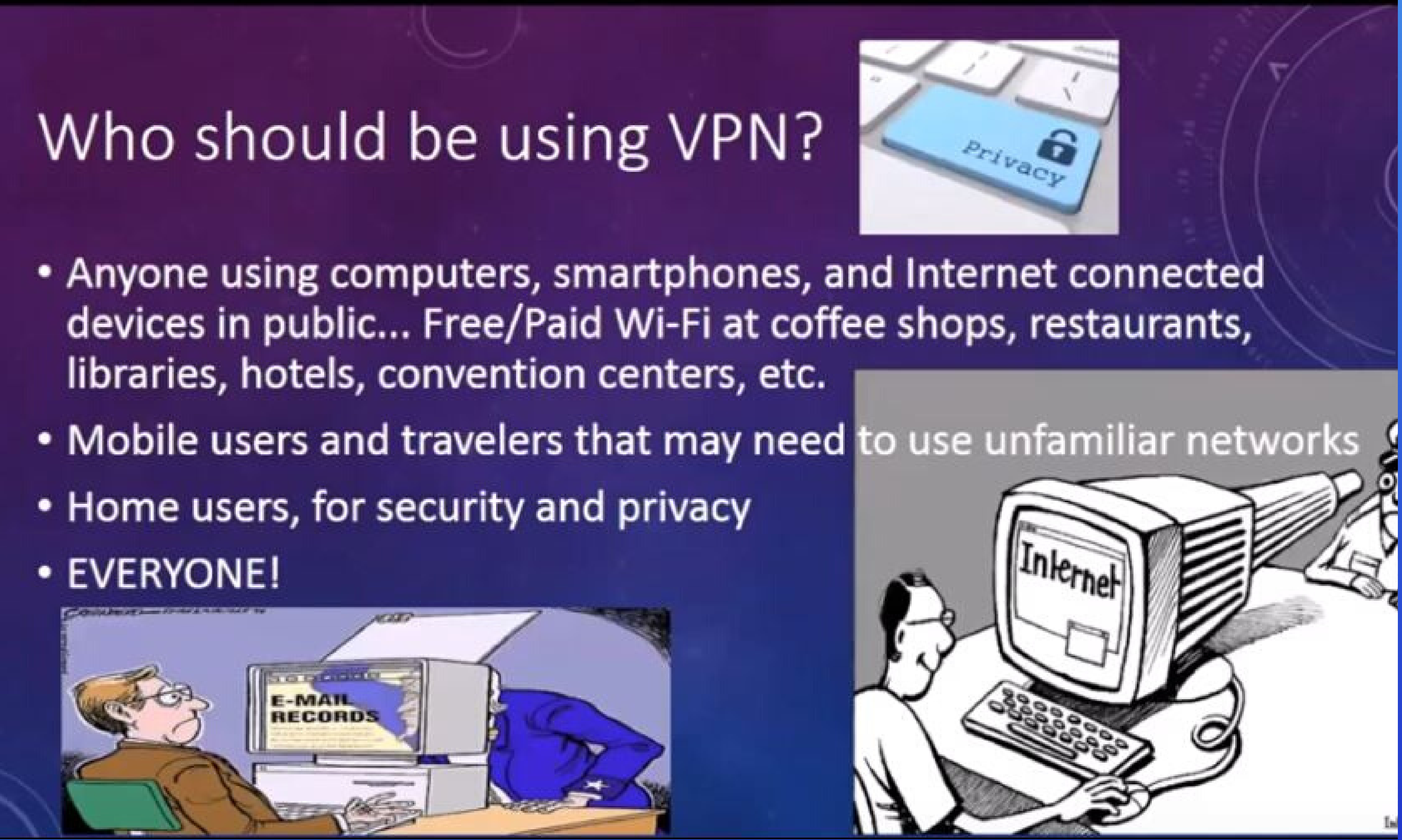
How A VPN Works

Ivacy VPN

Best VPN For Streaming - Ivacy VPN

Add a heading

Take A Free International Tour With Ivacy



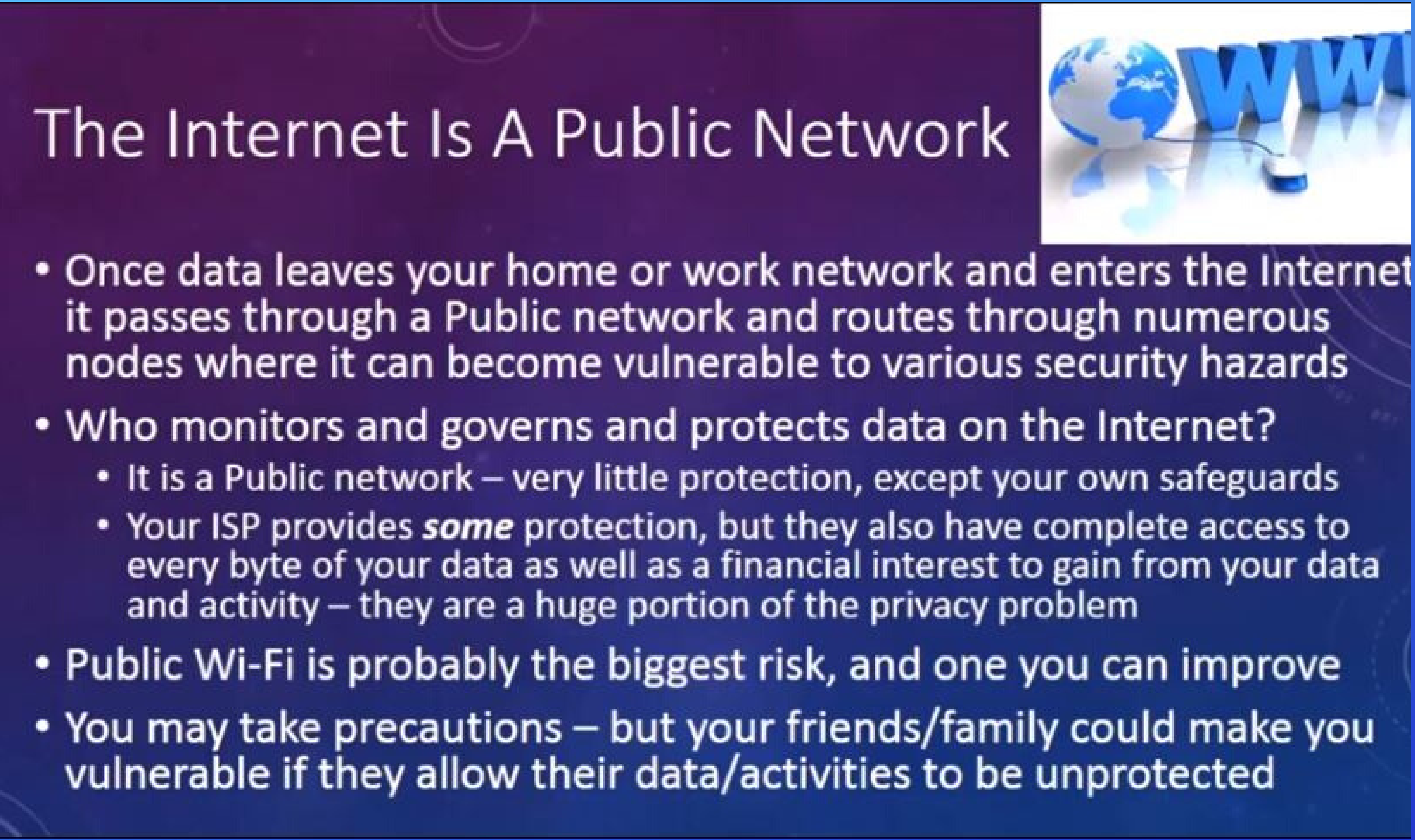
Who should be using VPN?

- Anyone using computers, smartphones, and Internet connected devices in public... Free/Paid Wi-Fi at coffee shops, restaurants, libraries, hotels, convention centers, etc.
- Mobile users and travelers that may need to use unfamiliar networks
- Home users, for security and privacy
- EVERYONE!

What Is My IP Address? IP Address Tools and More

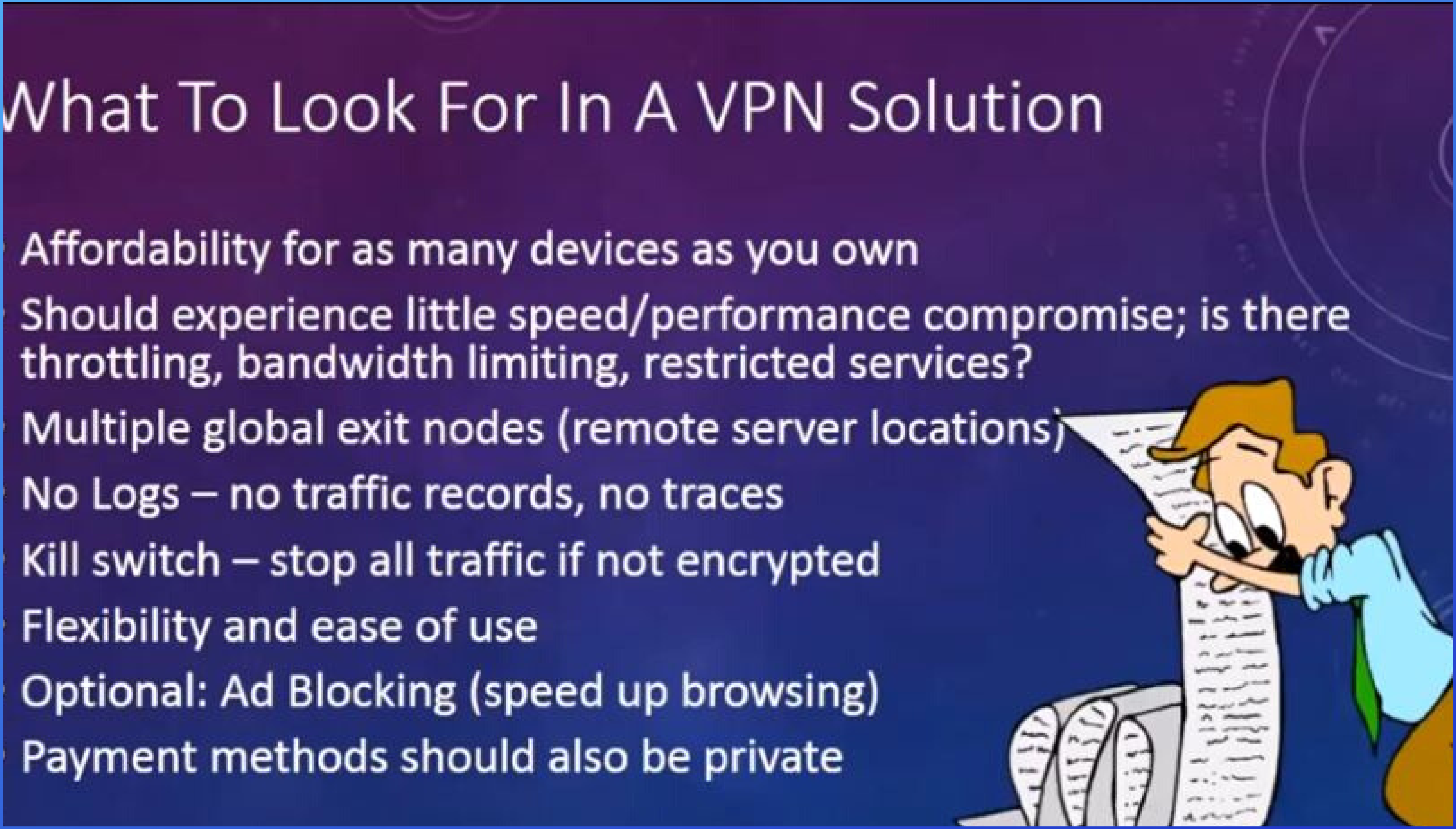
IP address lookup, location, proxy detection, email tracing, IP hiding tips, blacklist check, speed test, and forums. Find, get, and show my IP address.

WhatIsMyIPAddress.com



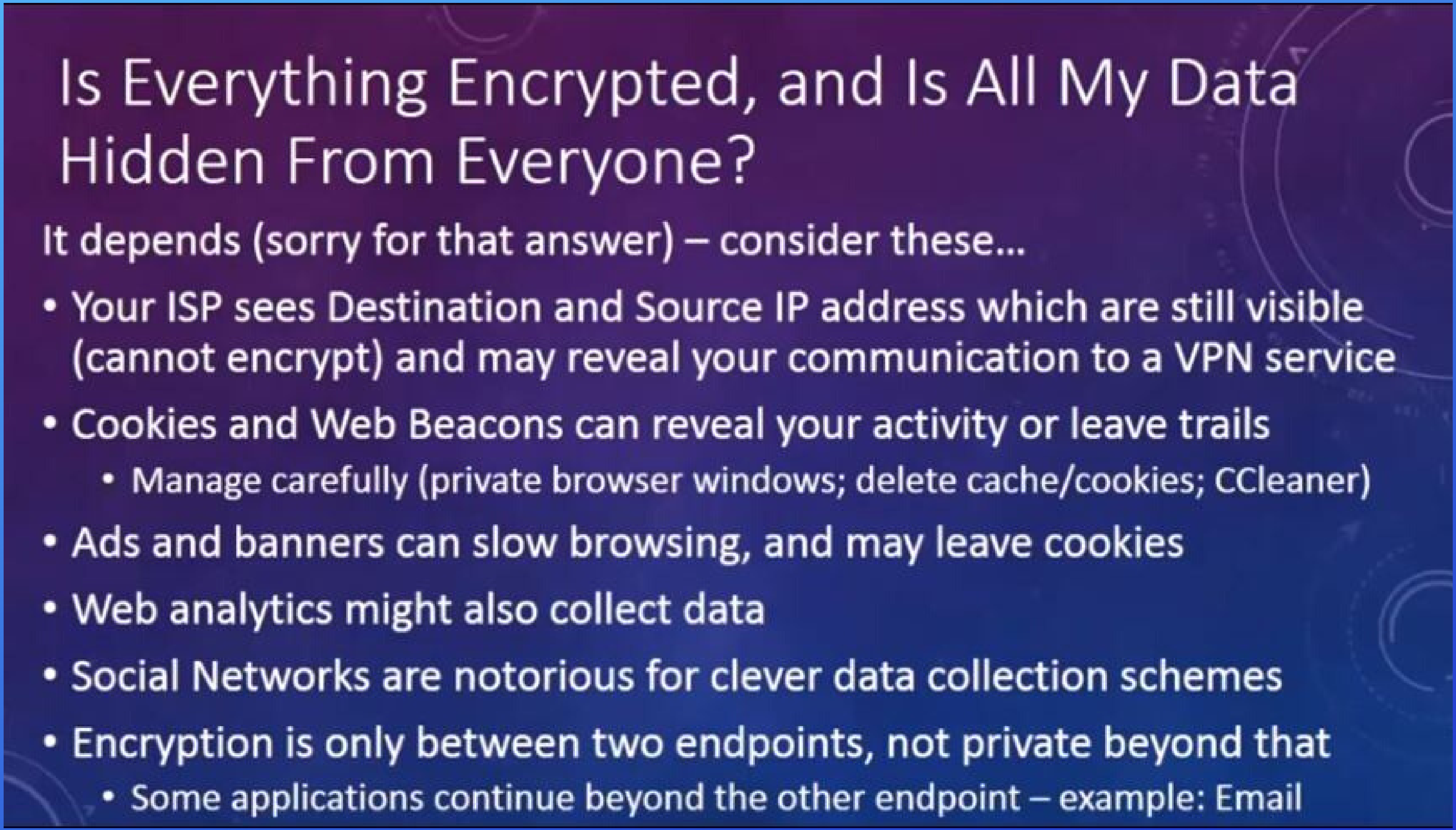
The Internet Is A Public Network

- Once data leaves your home or work network and enters the Internet it passes through a Public network and routes through numerous nodes where it can become vulnerable to various security hazards
- Who monitors and governs and protects data on the Internet?
    - It is a Public network – very little protection, except your own safeguards
    - Your ISP provides ***some*** protection, but they also have complete access to every byte of your data as well as a financial interest to gain from your data and activity – they are a huge portion of the privacy problem
- Public Wi-Fi is probably the biggest risk, and one you can improve
- You may take precautions – but your friends/family could make you vulnerable if they allow their data/activities to be unprotected



What To Look For In A VPN Solution

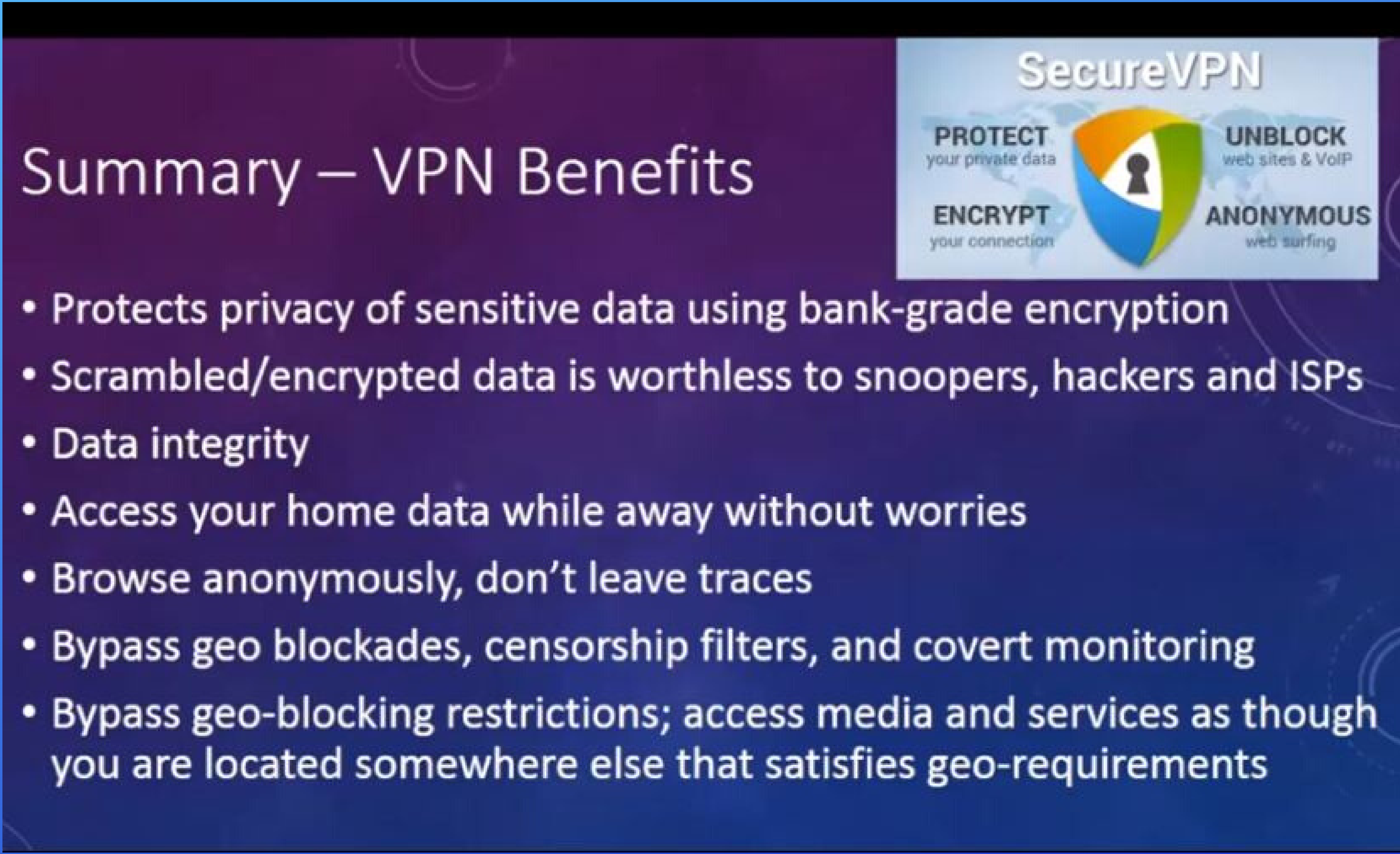
- Affordability for as many devices as you own
- Should experience little speed/performance compromise; is there throttling, bandwidth limiting, restricted services?
- Multiple global exit nodes (remote server locations)
- No Logs – no traffic records, no traces
- Kill switch – stop all traffic if not encrypted
- Flexibility and ease of use
- Optional: Ad Blocking (speed up browsing)
- Payment methods should also be private



Is Everything Encrypted, and Is All My Data Hidden From Everyone?

It depends (sorry for that answer) – consider these…

- Your ISP sees Destination and Source IP address which are still visible (cannot encrypt) and may reveal your communication to a VPN service
- Cookies and Web Beacons can reveal your activity or leave trails
  - Manage carefully (private browser windows; delete cache/cookies; CCleaner)
- Ads and banners can slow browsing, and may leave cookies
- Web analytics might also collect data
- Social Networks are notorious for clever data collection schemes
- Encryption is only between two endpoints, not private beyond that
  - Some applications continue beyond the other endpoint – example: Email



Summary – VPN Benefits

- Protects privacy of sensitive data using bank-grade encryption
- Scrambled/encrypted data is worthless to snoopers, hackers and ISPs
- Data integrity
- Access your home data while away without worries
- Browse anonymously, don’t leave traces
- Bypass geo blockades, censorship filters, and covert monitoring
- Bypass geo-blocking restrictions; access media and services as though you are located somewhere else that satisfies geo-requirements