Digital Safety on the Road

Presented by Joe Chappell – Connected HHI

Why this class?

Most of us live a “connected life” even when away from our homes and offices

Few of us really understand what is happening while we are connected to the internet

Understanding risks allows us to make informed and conscious decisions about our actions

There are “simple” steps that we can take to protect ourselves while we are traveling

Presentation Flow

- Primary Differences
- Protecting Your Devices
- Public Networks
- Virtual Private Networks

Why the big fuss about traveling?

- At Home
  - Our network and we control access
  - We decide who is admitted to our home
  - Risk of intruders and theft is relatively low
- Traveling
  - We no longer control the networks that we use
  - Our devices are much more exposed
  - Risk of theft is relatively higher

Device and Account Protection

- Lock your Devices – phones, tablets, and laptops should require a code, password, or biometric check in order to access
- Screen timeouts of 15 minutes or less
- Backup your phones, tablets, and laptops – cloud backups are best, home backups won't help if you need to recover when traveling.
- Consider encrypting laptop hard drives if you they have personal data that you should protect.

Password Access

- Recommended to have a password and a timer to lock your screen after X minutes of inactivity
- Required for laptops and devices that travel with you
- Easy to setup in Windows and on Macs
- Don’t use the same password for multiple accounts
- Write it down or use a Password App like LastPass or Dashlane or Keychain on Mac
- Use 2FA or MFA whenever security is important

Additional Laptop Considerations

- Use a password to lock access to your system
- Do regular backups
- Use drive encryption to protect the contents of your hard drive(s)
- Consider using a cloud backup service (Carbonite)or synchronization service (OneDrive or iCloud) for access while traveling

Network Safely

- Only use Safe WiFi Connections
- Safe – US Cell Networks
- Safe – Virtual Private Networks (VPNs)
- May Be Safe – Friend and Family*
- Unsafe – Free Hotspots
- Unsafe -Hotel and other Public WiFi
- Unsafe – Some foreign Cell networks

Risks with Public Networks

- Often difficult to differentiate between legitimate networks and honeypots.
- Even on legitimate networks, your devices and traffic can be visible to others on the network.

What is a Honeypot

A honeypot is a type of technique used to lure users for malicious intents. To the user it appears legitimate from the outside, but a hacker is operating it on the inside. Honeypots are implemented using both hardware and software, with Wi-Fi hotspots being popular among hackers.

Anyone can put up a device as a Wi-Fi access point. You can use a smartphone as a free hotspot by enabling it in settings. In fact, many mobile workers use this feature on their smartphones to provide their laptops access to the Internet using their telecom providers 4G LTE network. That provides fast Internet access on the road, where there might not be public Wi-Fi available. Bad actors can provide a free hotspot using this feature as a honeypot.

The Security Issues in Using Public Wi-Fi — "Honeypots" And "Pineapples" by@Vince Tabora

One More Time!

The summer travel season is upon us, and that means many people will connect to public Wi-Fi hotspots at airports, hotels, cafes, restaurants, bus stops and more. Unfortunately, public networks have become honeypots for hackers who use them to infiltrate connected devices.

A compromised network can allow a hacker to intercept, read and modify the internet traffic that passes through it. They can then leverage this for a number of purposes, ranging from stealing passwords to downloading malware onto victims' phones and laptops.

National CyberSecurity Alliance

Your device
VPN
Internet

Virtual Private Networks

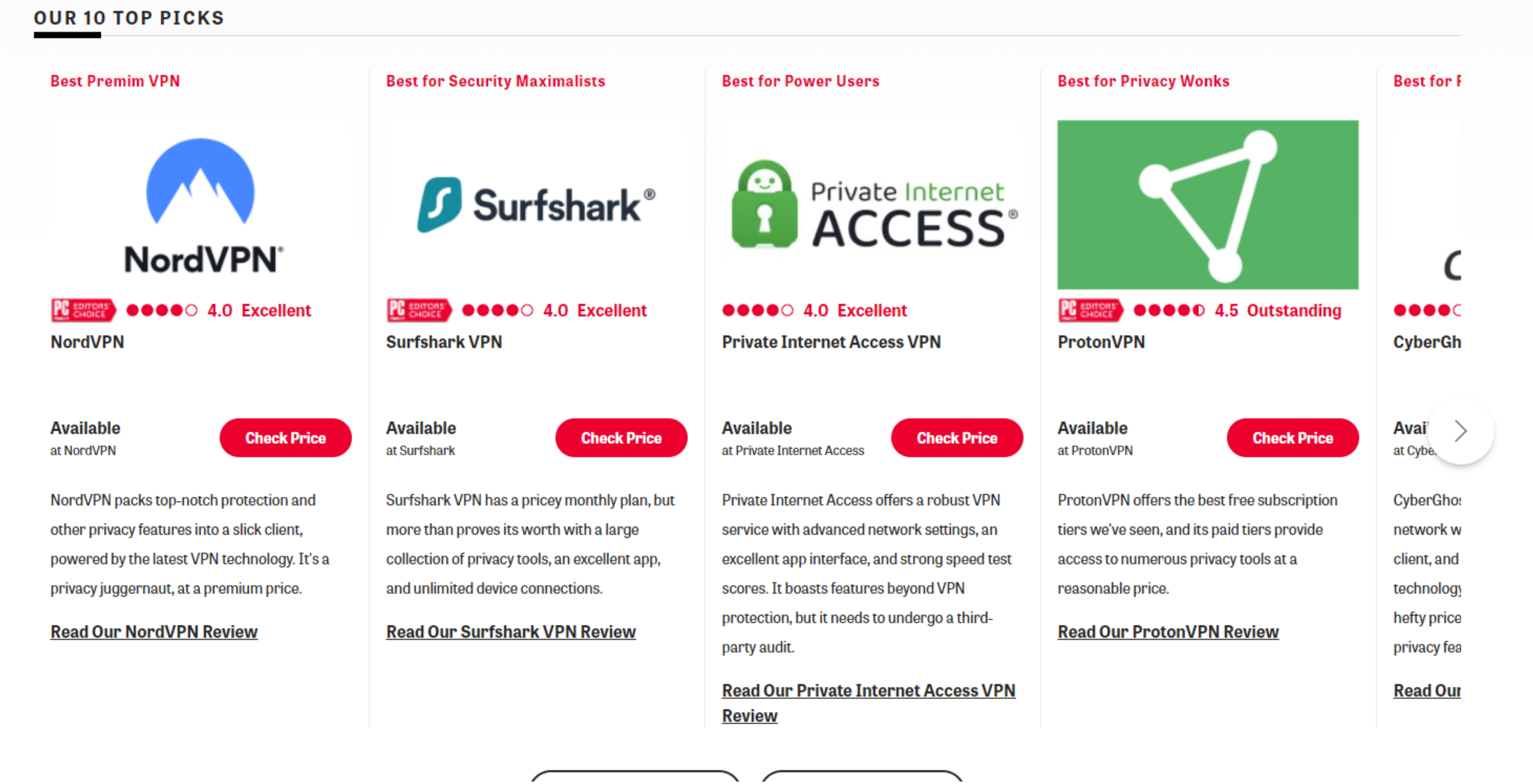
A VPN creates an encrypted **“tunnel”** over the internet to protect the data traveling between you and your Internet destination — anything from your online banking account to a video sharing website to a search engine.

This tunnel is created by first **authenticating** your client — a computer, smartphone or tablet — with a VPN server. The server then uses one of several **encryption protocols** to make sure that no one can monitor the information traveling between you and your online destination.

- Here you should remember that before being sent and received over the internet, any data needs to first be split into packets. To ensure each data packet stays secure, a VPN service wraps it in an outer packet, which is then encrypted through a process called **encapsulation**. This exterior packet keeps the data secure during the transfer, and it is the core element of the VPN tunnel. When the data arrives at the VPN server, the outer packet is removed to access the data within, which requires a **decryption** process.

- So basically, accessing the internet through a VPN tunnel is like putting a package into a box and then sending it to someone. Nobody can see what’s inside the box until it's opened, or in this case, decrypted.
- Another thing to remember: When you're using a VPN, your packets reach the internet with **another IP address**, supplied by your VPN provider. So if you keep connecting to different VPN servers, each time the internet will see you as a different person. If you connect to a server in another country, you will appear to be browsing from that country.

PC Magazine
4/27/2022



OUR 10 TOP PICKS

Best Premim VPN

PC EDITORS' CHOICE ●●●●○ 4.0 Excellent

NordVPN

Available
at NordVPN

Check Price

NordVPN packs top-notch protection and other privacy features into a slick client, powered by the latest VPN technology. It's a privacy juggernaut, at a premium price.

Read Our NordVPN Review

Best for Security Maximalists

PC EDITORS' CHOICE ●●●●○ 4.0 Excellent

Surfshark VPN

Available
at Surfshark

Check Price

Surfshark VPN has a pricey monthly plan, but more than proves its worth with a large collection of privacy tools, an excellent app, and unlimited device connections.

Read Our Surfshark VPN Review

Best for Power Users

●●●●○ 4.0 Excellent

Private Internet Access VPN

Available
at Private Internet Access

Check Price

Private Internet Access offers a robust VPN service with advanced network settings, an excellent app interface, and strong speed test scores. It boasts features beyond VPN protection, but it needs to undergo a third-party audit.

Read Our Private Internet Access VPN Review

Best for Privacy Wonks

PC EDITORS' CHOICE ●●●●◐ 4.5 Outstanding

ProtonVPN

Available
at ProtonVPN

Check Price

ProtonVPN offers the best free subscription tiers we've seen, and its paid tiers provide access to numerous privacy tools at a reasonable price.

Read Our ProtonVPN Review

Best for F

●●●●○

CyberGh

Avai
at Cybe

CyberGho
network w
client, and
technolog
hefty price
privacy fea

Read Our

Apple Private Relay

No, Apple's Private Relay is not a VPN, but you can still try it out with iOS 15

https://www.cnet.com/tech/services-and-software/no-apples-private-relay-is-not-a-vpn-but-you-can-still-try-it-out-with-ios-15/

Q&A

- Joe Chappell
- Connected HHI

- jchappell@connectedhhi.com
- www.connectedhhi.com
- 843-715-9894

Connected HHI