Understanding Virtual Private Networks (VPN)

Workshop Handout

What is a VPN?

- A **VPN** or *virtual private network* is a secure and private network connection through the public internet.
- VPN services protect your personal data, hide your IP address when you use the internet, and lets you bypass censorship, content blocks, and website restrictions.
- VPNs hide your IP address and physical location while encrypting your internet traffic so that no one can tell who you are, where you are or what you're doing online.
- VPNs aren't just for desktops or laptops — You can set up VPN on your smartphone or tablet as well.

Why is it important to hide your IP address?

- Your **IP address** is a unique set of numbers that identifies your device when you connect to the internet. Just as the postal service uses street addresses to deliver mail to the right people, IP addresses ensure that internet traffic gets sent to the right computers.
- A VPN masks your actual IP address by showing the public internet the IP address of the VPN server you're using instead of your own; this prevents anyone from finding your IP address. Some VPNs cluster multiple users under one shared IP address, which further anonymizes your internet activity.

© AJM Technology Solutions & Training LLC 2018-2021

- Pair that IP address masking with encryption, and your online activities are kept fully private from Internet service providers, hackers and government surveillance. A VPN protects you in many ways!

How does a VPN work?

A VPN works by using encryption protocols to funnel all your internet traffic through an encrypted tunnel (a virtual private network) between your computer and a remote VPN server. This hides your IP address and secures your data, preventing others from intercepting it.

Without a VPN, all your internet traffic is potentially exposed to your internet service provider (ISP), the government, advertisers, or other people on your network. That's why VPN connections boost your privacy and security online.

VPN Encryption

- **VPN encryption** is the process of using data encryption to create a secure tunnel for your data to travel through. If anyone examines your VPN connection, they'll see scrambled data. Only your device and the VPN server you're using can encrypt and decrypt (or unscramble) your data.
- Most VPNs use the 256-bit AES (Advanced Encryption Standard) algorithm. This level of encryption is so secure that it's used by banks and governments worldwide.

Why should I use a VPN?

Safety on public wifi

- The convenience of free public Wi-Fi often comes with a loss of security. Since anyone can hop onto an unsecured Wi-Fi network, there's no way to know exactly who's connected at any given time, or what they're doing. It's easy for a hacker to sit on a public Wi-Fi network and intercept all the traffic flowing across it.

© AJM Technology Solutions & Training LLC 2018-2021

- Because a VPN connection encrypts your communication with its server, anyone trying to eavesdrop on the public network will see only gibberish. That's a big part of what VPN protection is: ensuring that no one can access your data.

Stream from anywhere

- Due to licensing restrictions, streaming platforms feature different content libraries in various countries around the world — this is known as geo-blocking. If you're traveling abroad and want to keep up with your favorite shows from home, you may find that they're unavailable in your current location.

- A VPN lets you bypass location-based content blocks by giving you an IP address in any country where your VPN provider has a server. If you pick your home country from the server list, it will be like you never left home. And when you install a VPN on your phone or mobile device, you can truly stream from anywhere.

Evade ISP Tracking

- Without a VPN, your ISP (internet service provider) can track all your online activity: the websites and services you use, when you use them, and for how long.

- In the US, your ISP can store and sell your browsing history to the highest bidder — such as an advertising network, data broker, or subscription service — without your consent.

- Because of how a VPN works, it protects you from this kind of invasion of privacy. Since your device's internet connection is encrypted, your ISP can't monitor exactly what you're doing online, and **they can't see your browsing history**.

Prevents Price Discrimination

- Price discrimination happens when e-commerce sites offer different prices to different people based on their perceived ability to pay. Online retailers use a variety of criteria to calculate the price of an item for any given viewer — device type along with demographic information such as your real-world location.

© AJM Technology Solutions & Training LLC 2018-2021

Can I still be tracked online when using a VPN?

- If you pay for your VPN with a credit card, your VPN provider will likely know who you are. Since you're connecting to your VPN from your device, they'll also have your IP address.
- But that's it, most VPNs don't monitor your online activity, and many include explicit no-logging policies that prevent them from collecting any information about what you do while using their services.
- No logging means that your VPN provider doesn't keep any records of what you do while using the VPN. A no-log VPN provider won't track or store any information sent over the VPN connection.
- They know only your IP address, payment information, and the VPN server you use while connected.

Tips For Choosing a VPN

- **Premium service**: A leading premium VPN will offer the security, stability, privacy, and speed you're looking for. Many free VPN services simply cannot compete — you can expect ads, unreliable connections, or weaker security. Your free VPN provider may also collect and sell your personal data.
- **Server quantity and locations**: The more servers a VPN provider has, the better they can spread their users out, giving everyone a faster experience. Look for a VPN that ensures a stable and fast connection. And if you need an IP address in a specific country, make sure your VPN provider has servers there.
- **Shared IP addresses**: By grouping multiple users under a single shared IP address, it's more difficult to identify the actions of any individual user. Find a VPN that gives you this additional layer of protection.

© AJM Technology Solutions & Training LLC 2018-2021

- **No Logs**: VPNs with explicit no-logging policies won't keep any data about you — they won't record what you do while connected to their VPNs or track when you connect or for how long. The only information they'll have on you is your IP address and the IP address of the server you connected to.
- **Multi-device coverage**: Choose a VPN that covers multiple devices under one subscription. AVG Secure VPN protects up to 10 devices at once, allowing you to extend the security and privacy of our VPN to others in your household.

Recommended VPNs & Cost

- Private Internet Access $9.95/month
- CyberGhost $12.99/month
- NordVPN $11.95/month
- IPVanish $11.95/month
- Avast SecureLine VPN $7.50/month
- AVG $7.50/month

© AJM Technology Solutions & Training LLC 2018-2021