Holiday Travel Tip: Use Public Wi-Fi Safely

It's the holiday season and airports are busier than ever. After waiting in seemingly endless lines, you find yourself at the boarding gate with over an hour to wait before your flight home. You decide to check some emails while connected to a public Wi-Fi network that doesn't offer data encryption. Unfortunately, there is an adversary at the same airport waiting to board their flight home. They are passing the time by staying connected to the same public Wi-Fi network as you, capturing unencrypted network traffic. They are able to see all the websites that you're navigating to, which inadvertently reveals sensitive information. How can you help protect your mobile device?

Public Wi-Fi networks are wireless local area networks that are available to the public and do not require a password. Unfortunately, many public Wi-Fi hotspots and access points do not provide encryption. While it is convenient to use public wireless networks while traveling, an ineffectively secured mobile device that establishes a connection to a public Wi-Fi hotspot may expose sensitive data. This is because networks that lack data-in-transit protections are at risk of unauthorized eavesdropping taking place to access their sensitive information.

Employees can use public Wi-Fi to work remotely from numerous public places such as hotels, airports, and coffee shops. Public Wi-Fi users may have important, sensitive, and personal information on their portable mobile devices, or they may use those devices to remotely access organizational resources. If information is compromised, it may lead to serious harm, financial loss, or reputational damage for an organization.

What is Eavesdropping?

Eavesdropping is a data-in-transit attack in which an adversary intercepts, modifies, or deletes information that is transmitted between two devices. This attack can occur when a user connects to an unsecured network in which traffic is not encrypted.

Even if the transmitted data was encrypted by the application, an attacker would be aware of the domains, internet protocol (IP) addresses, and services (as indicated by port numbers) to which the device connects; an attacker could use such information for an adversary-in-the middle attack against the device or the user.

Such visibility could also result in the theft of personally identifiable information (PII). PII theft is extremely dangerous and has far-reaching concerns. PII comes in many forms, such as:

- Login credentials
- Financial information
- Personal data
- Photos

- Location data
- Unique device identifiers (e.g., Universal Device Identifier (UDID), International Mobile Equipment Identity (IMEI))

Once an adversary collects unencrypted mobile device network traffic through a compromised public Wi-Fi connection, they may get access to a user's login credentials and log into his/her personal accounts and pages causing damage or stealing PII. With public Wi-Fi, an adversary can intercept information sent over the Internet.

Mitigating the Threat

To mitigate this threat, individuals or enterprises can be mindful of using secure connections to websites and resources. A couple of options include:

- A virtual private network (VPN) solution can ensure all communication to and from their applications is encrypted prior to leaving the device.
- Websites that use Hypertext Transfer Protocol Secure (HTTPS), which is HTTP transmitted over Transport Layer Security, help maintain the privacy and integrity of data, and the authentication of websites is also validated.

While public Wi-Fi networks may not provide data-in-transit protection, if the proper protections are in place their convenience can be fully utilized with increased confidence.

More information on how to protect against these and other potential mobile threats can be found in NIST Special Publication 1800-22 *Mobile Device Security: Bring Your Own Device.*

Mobile Device Security: Bring Your Own Device NIST SP 1800-22 Practice Guide Draft | NCCoE