Public Wi-Fi Safety

TIPS TO MAXIMIZE PERSONAL CYBERSECURITY ON PUBLIC NETWORKS

According to a Norton Wi-Fi risk report, 46% of consumers cannot wait more than a few minutes before logging onto, or at least asking for the password for a Wi-Fi network upon arriving at a cafe, hotel, or similar location. 71% of consumers consider a strong Wi-Fi signal a deciding factor when traveling rather than security considerations. With public Wi-Fi use an inevitable reality, it is important for users to maximize their personal security. The following are best practices for using public Wi-Fi:

Use a Virtual Private Network

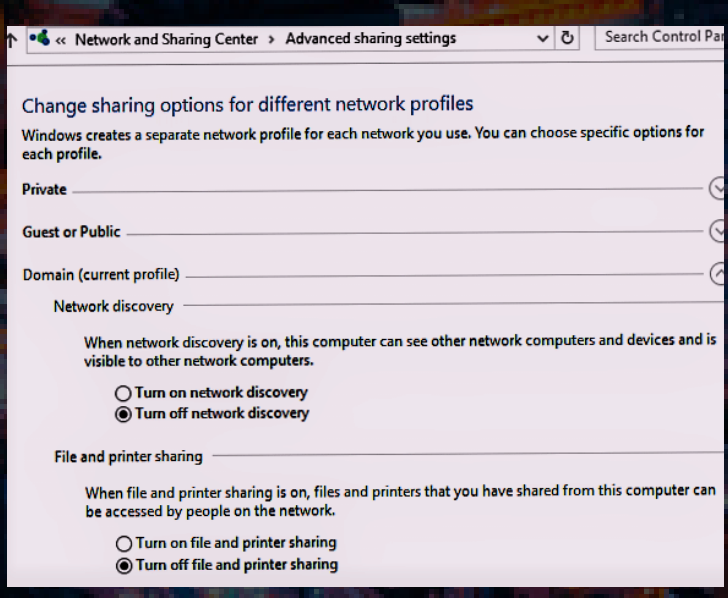
A VPN will allow you to encrypt your web traffic, allowing you to protect your browsing session from hackers and even the owners of the public network you are using. A VPN should always be used when accessing public networks. When deciding on a VPN service to use, paid services are preferable to free. It is important to also take into consideration the location of the company providing the VPN service.

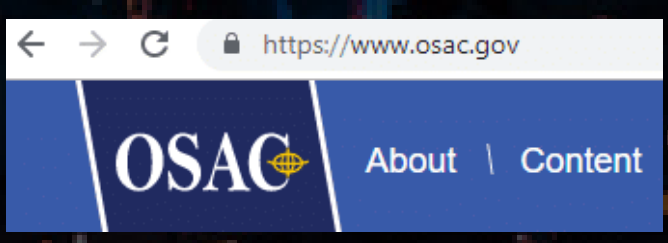
Avoid Transmitting Personal Data

Refrain from accessing any personal accounts that contain sensitive personal data, such as bank accounts, online shopping accounts, primary email accounts, etc. If you are accessing accounts that contain personal data, use the organization's secure (HTTPS) website instead of their mobile app. Lastly, be sure to log out of any accounts you accessed when you are finished.

Turn Off Automatic Connectivity

Allowing your device to connect automatically to a network at home is fine, however, it is highly recommended this feature is disabled when in public. This will prevent your device from connecting to any unsecure networks in the area. Along with automatic connectivity, it is important to also disable "file and print sharing" and "network discovery" on your device (See image on right). Leaving these enabled while accessing a public network gives malicious actors easy access to your device.





Use HTTPS Over HTTP

Only visit webpages that use HTTPs as opposed to those using HTTP. Confirm this by checking the URL (See image on left). Websites use HTTPS encryption to protect your data as it travels from your device to the websites server.

Update Software and Apps

UPDATE UPDATE UPDATE! Maximizing personal device security means updating software and operating systems when possible. These updates often fix problems with software that nefarious actors can exploit to conduct cyber attacks. This makes the process of patching software even more critical. Check for updates to your operating system and any software and applications prior to travel/accessing a public network.

Connect To Secure Networks

A public Wi-Fi network with a password is not considered "secure". A malicious person who knows the password can conduct the same nefarious activity as they would on a network without password protection. Some networks may encrypt your web traffic, but don't assume all networks are doing so. It is highly likely that any network that does not require a password, that network is also not using encryption. Unsecure networks open the opportunity for malicious individuals to view everything you see and send during your browsing session. If using a secure network is not possible, wait until you can access one or set up a hotspot.

Change Your Passwords

Prior to traveling and upon return you should change your passwords for any of the accounts or devices you might use while connected to a public network. Ensure you are using complex letter and number combinations and not something that can easily be guessed. Consider using a password manager that can generate complex passwords for you. Enable multi-factor authentication on any accounts that may contain sensitive information.

For additional information contact OSAC's Cyber Threat and Information Security team at osacCyber@state.gov