SAFE BROWSING TIPS WHILE TRAVELING

The likelihood of data theft increases when you travel.

Not only is there an inherent physical risk, as your computer could get stolen during your time at the airport, but traveling often means you are forced to use public Wi-Fi networks, which generally are insecure.

It's imperative you take extra precautions to protect your personal information, as well as sensitive company information, while you are traveling.

Avoid Using Public Wi-Fi Networks

- Public Wi-Fi networks should be avoided if possible.
- If you must use a public Wi-Fi network, ensure your virtual private network (VPN) is enabled before accessing any corporate data.
- A VPN will protect your online activity by encrypting the data and sending it through a secure tunnel to the VPN server.
- While using a VPN, anyone monitoring the Wi-Fi network wouldn't be able to decipher the actual data.
- VPNs also will mask your IP address, making it harder for cybercriminals to track your online activities.

Use Caution When Accessing Company Data

- While VPNs help, you still have to be careful when accessing company data in a public setting.
- Refrain from pulling up company data while at the airport, coffee shop or other public place with a lot of foot traffic.
- Instead, access that data when you are in your hotel room or in another private area.

Don't Leave Your Computer Unattended

- Leaving a computer unattended is just asking for it to be stolen.
- If you do have to leave it temporarily, lock your computer by holding the Windows key and pressing "L."
- Never leave sensitive data on a screen when you aren't around.

Contact Hungerford Technologies

If you have any questions regarding safe browsing tips, email us at support@hungerford.tech or call (616) 949-4020.