Business travelers are easy targets fo cybercriminals

.ess than one-third of business travelers avoid unsecured Wi-Fi networks, according to World Travel Protection.

3y **Steve Hallo** | January 04, 2024 at 12:27 AM

Around 8% of companies don't ask employees to take any security measures at all, according to a survey from World Travel Protection. Credit: jumlongch/Stock.Adobe.com

From unsecured networks to sensitive documents on unprotected mobile devices, business travelers offer ample ways for cybercriminals to gain access. Despite this, only about one-third of companies require employees to use basic cybersecurity measures when traveling, according to **World Travel Protection**.

When it comes to steps companies insist on, 36% of U.S. firms require two-way authentication on devices, while 30% mandate VPN use and 32% deploy antivirus software on devices, the travel risk management company reported.

Further, less than one-third ask that their traveling employees avoid unsecured Wi-Fi networks, and just 28% use a laptop screen protector while working in public. Around 8% of companies don't ask employees to take any **cybersecurity measures** at all.

Frank Harrison, regional security director, Americas, World Travel Protection explained that business travelers are easy targets to exploit because they often carry sensitive corporate information and frequently use laptops and mobile devices. He added business travelers should be particularly protective of their cell phones.

Threat actors now have the capabilities to identify and target mobile devices, deliver malicious code to the device, access a device to track your location, activate your device’s microphone, and intercept messages,” Harrison said in a release. “Adopting cyber secure measures that ocus on risk mitigation is essential for all organizations’ travel policies to protect travelers and heir data.”

To help keep business travelers safe, World Travel Protection recommends:

- Keep software updated.
- Use antivirus software that includes a VPN component.
- Require strong passwords and **multifactor authentication**.
- Utilize secure mobile Wi-Fi hotspots instead of public Wi-Fi.