SecurityAwarenessNews

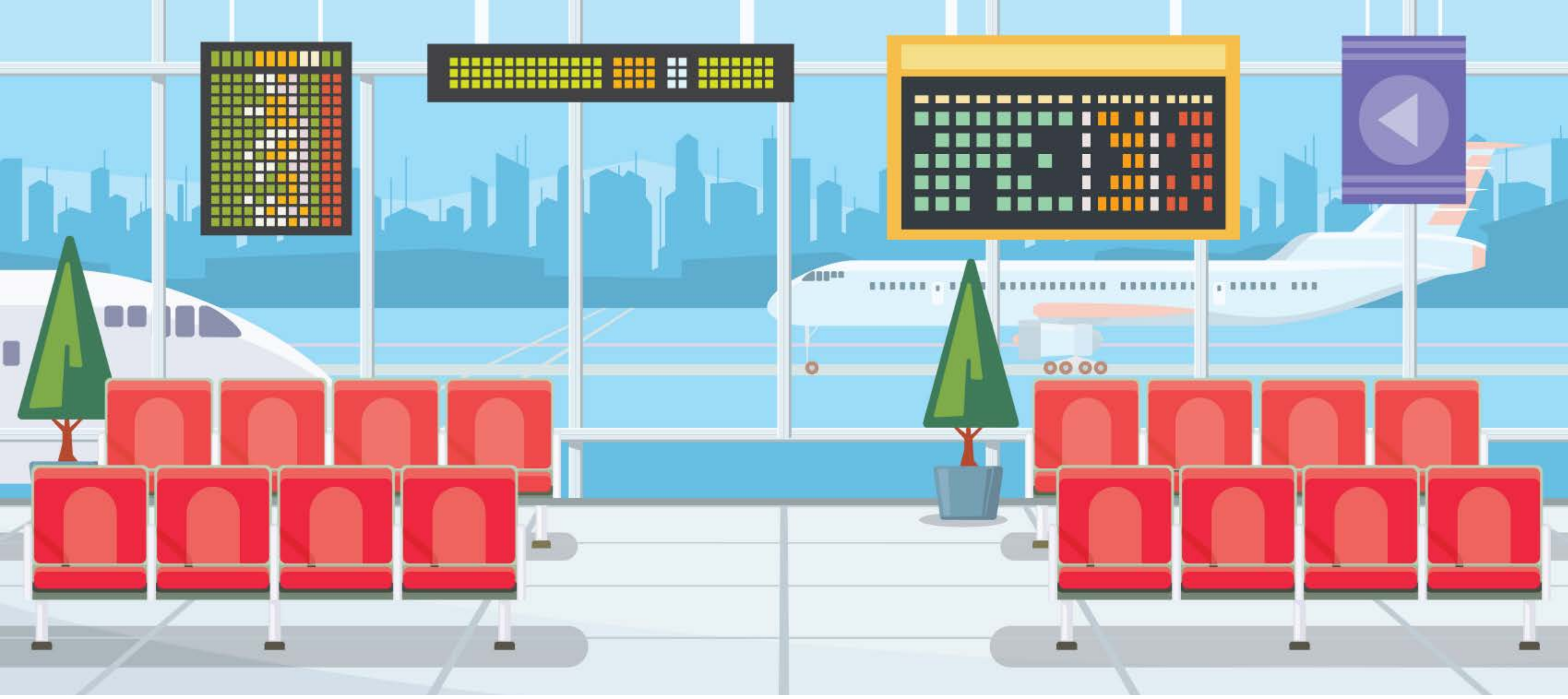
the security awareness newsletter for security aware people

The Travel Issue

How People Spy on You

The Human Firewall's Guide to Working Remotely

Safe Travel to Dangerous Places



How People Spy on You

Long security lines. Crowded airports. Cramped airplanes. Tight connections. Traveling, whether for business or pleasure, blends a hectic mix of physical discomfort and emotional distress. It's in these situations where security awareness becomes even more important. Imagine that you have a 90-minute layover in a busy airport. It's just enough time to grab a quick meal and knock out some work. You find a seat at an overwhelmed café and open your work laptop.

But did you notice…

The person sitting behind you? They can easily see your laptop screen. Known as "shoulder surfing," any sensitive data on your screen will surely catch the eye of a social engineer.

That everyone else is using the same WiFi? Connecting to public networks essentially makes anything you access on the network also public. Cybercriminals use public WiFi to steal information.

The person sitting next to you eavesdropping on your conversation? Whenever you find yourself in a public setting, discretion is key. You wouldn't want someone overhearing your private conversation with a client or business associate.

The USB cable left on a public charging station? Did you know that cybercriminals can not only infect USB devices—including cables—with malware (a tactic they call "juice jacking"), but they can also "leave behind" malware on public charging stations?

These threats, in addition to physical threats such as device (or luggage) theft, require heightened awareness when traveling. When you hit the road, always keep an eye on your possessions, never ask someone to watch your items for you, and remember that organizational policies must be followed regardless of where you go! If you have any questions about secure travel, please ask.

The Human Firewall's Guide to Working Remotely

Wherever you go, there you are. Escorting you on the journey are security threats that eagerly await a simple misstep or lapse in security awareness. Avoid becoming a victim with these five steps:

Prioritize situational awareness. If you're visiting a local coffee shop for the 50th time, or a faraway country for the first time, it's imperative that you keep your guard up. Mind your surroundings, shield your device screens from prying eyes, and never let your personal items out of sight.

Avoid public WiFi. If possible, use a cellular data connection, and don't log into accounts that contain highly sensitive information. If you have to connect to public WiFi, use a virtual private network—software that provides an encrypted connection to help prevent data theft.

Use discretion. If you must access sensitive information in a public setting, make sure no one can see your screen, and no one can overhear your phone calls.

Be wary of USBs. Never use a charging cable or plug in a USB flash drive that doesn't belong to you, especially if it's one you found at random. Criminals hack USB devices—including public charging stations—to spread data-stealing malware.

Always follow policy. Whether you work from home, on location, or at the office, it's your responsibility to know and follow our organization's policies.

Public WiFi:
What's the big deal?

Order a coffee. Grab a seat. Connect to the public WiFi. Get hacked. Surely, it's not that simple, right? Believe it or not, stealing data over unencrypted connections *(as most public networks are)* takes no special hacking skills. Instead, all it takes is data-stealing software *(such as packet analyzers)* and a motivated cybercriminal. The technical details of how packet sniffing or WiFi hacking work aren't important, though we encourage you to research it and watch a few real-world attacks. What's important is understanding the vulnerabilities of public WiFi.

Login credentials, credit card information, email conversations—anything you send over an unencrypted internet connection can be intercepted and captured. There are two ways to avoid this type of attack.

ONE:

Don't connect to public WiFi. It's not ideal, but it's also not paranoia. Security first!

TWO:

Always use a virtual private network (VPN) on every device. VPNs provide encrypted connections that help prevent criminals from stealing your data. But even with a VPN enabled, it's still wise to avoid logging into sensitive accounts or making purchases online.

Safe Travel to Dangerous Places

Regardless of where your travel takes you, security awareness remains a top priority. A cozy little town in the mountains may seem safer than a major metropolis, but security threats, both cyber and physical, exist everywhere. Of course, there are some areas of the world that pose additional levels of risk due to political turmoil, drug violence, extreme poverty, etc. Stay out of harm's way by following a few guidelines. Note that we aren't going into details about cyber threats, because they are location agnostic and deserve your attention regardless of where you are.

1. **Notify your embassy:** Several weeks before your trip, be sure to inform your embassy of the when and where of your travels. Keep contact details of the nearest embassy or consulate with you on your journey.

2. **Plan ahead:** Stay up to date on travel advisories, and research the area. Seek information from local news outlets to gain a perspective of what the risks are and how much danger you may face when you visit.

3. **Make color copies of your identification:** The misfortune of losing a passport is eased if you have color copies, both digital and physical. If traveling with others, exchange copies, and store them in a different place than your actual passports.

4. **Memorize contact information:** In the event of an emergency, you can't always rely on having access to your smartphone or a data connection. Memorize contact information (phone number, email, home address) of friends and family in case you need to reach them.

5. **Know how to contact local authorities:** If a situation arises where you need local authorities, you'll be glad to have their contact information on hand rather than having to seek it out, especially if it's an emergency.

6. **Distribute your itinerary:** Give a family member or trustworthy friend your entire itinerary, and routinely check in. Use social media to update your status. (Social media can also be used to signal for help.)

7. **Have an exit strategy:** A risky area could become suddenly life-threatening while you're there. Have an exit strategy in place, and keep tabs on local news.

8. **Never assume you'll have access to supplies:** If possible, take "survival packs" of small food items (such as protein bars) with you, and ensure you have more than enough prescription drugs as necessary.