In-Flight & General Away from Home WiFi Safety Tips

By Shaun Murphy, CEO Private Giant

Signs displaying "Free Wi-Fi" are a common sight in airports, cafes, hotels and lounges. When people see "FREE Wi-Fi" they don't think... they connect. People are unaware of the threats when they sync up to open Wi-Fi. Security breaches and attacks by hackers due to logging into unsecured networks to check email or personal accounts when traveling or staying in hotels, puts your email credentials, bank accounts, credit card information and other personal accounts at risk.

1 — Listen to your apps/devices when they say your connection is not secure.
• Web browsers have an indicator in the URL bar if the site is safe or not (place where you type in the site's name). The generally accepted icon is a closed or locked padlock. If there is a red X or warning sign on top, you might be on an unsafe connection.
• Web browsers warn if a connection is not secure (where a website is normally displayed. If this appears, do not hit continue, or override this warning.
• If you connect to a WiFi access point requiring you to login via a web browser before using, connect to a basic website first (I recommend http://example.com). These WiFi access points have a system called a "captive portal" to capture the URL/data you send the first time, and will redirect you to their login system.
• If a WiFi access point makes you install software, plugin, or security certificate before connecting, disconnect ASAP. This scam can install malicious software causing immediate damage (ransomware, malware, viruses, etc. or install a security setting called a "certificate" that is not noticeable, but will permanently weakens all secure connections you make so the WiFi operator can read or modify all your internet data.
• Most operating systems warn if you connect to an unsecure WiFi. If you do information is readable by anyone in close proximity to you. Only connect to WiFi access points requiring a password via the operating system's WiFi connection screen (not in a web browser).

2 — Install a separate web browser if connecting to unknown WiFi access points. Keep your main web browser logged into favorite sites, save passwords etc... as a seperate browser won't have the information. If you connect to an unsafe WiFi exposure is limited to that browsing session. Use the seperate browser for basic surfing; don't log into your email, social media accounts, post personal or identifiable information. Try, https://www.mozilla.org/firefox. It's terrific, and on most desktops, laptops and android-based mobile devices. If you can't install an alternative browser, check if your browser supports a Private or Incognito browsing mode. It won't be as strong as a separate browsing application, but prevents most data leakage.

3 — Does your home internet router have a virtual private network option? It's a little complex to set up, but you can safely connect to your home network from WiFi access points, secure or not. Surf and email like you do at home, but traveling from 30,000ft in the air. Cool!
• Companies sell VPN hosted services offering a secure and safe browsing experience, but there's no way to know what they do with your data. Instead, of connecting to an unsafe/unknown internet connection, you have two!

4 — Instead, of connecting to an unknown or potentially unsafe WiF — use your cell phone in tethering mode. If you have Verizon, turn off that horribly invasive super cookie tracking! https://www.techdirt.com/articles/20150115/07074929705/remember-that-undeletable-super-cookie-verizon-claimed-wouldnt-be-abused-yeah-well-funny-story.shtml.

5 — Only type in websites with https:// — not just plain http://. This tells the browser to connect securely or display an error if it can't, to your online service and gives you very strong protection.

Shaun Murphy, is one of the nations leading communication security experts with more than 20 years experience. He has worked as a subject matter expert on high-level government communication software and hardware systems for numerous agencies. His mission is to create a protected communications platform in a world where privacy has almost ceased to exist.

The Travel Org
All In One Real Leather Travel Organizer Exudes Luxury And Style

British-designed Travel Org is the **"Must-Have"** travel accessory consisting of 1 large zip wallet with internal pockets, 15 document sleeves and a card holder compartment that holds up to 8 cards. The Travel Org comes in four limited edition colors: black, tan, navy and orange. Available to match The Travel Org are sleep masks and luggage tags also made from high-quality leather. The Travel Org is essential and convenient for a universal audience whether it be a solo traveller, frequent traveller, family vacation, or anyone interested in adding fashion to their travel ventures. It was featured in the 2016 Golden Globe gift bags, which is why it should be in the hands of everyone as the Number 1 Travel Organizer for 2016.
Travel Org RRP: $295.00 Travel Org Insert Packs: $27.01
Travel Org Luggage Tags: $45.00 Travel Org Sleep Masks: $45.00
Visit: www.thetravelorg.com