Tourists warned to beware ‘Evil Twin’ Wi-Fi trap amid summer cyber bonanza

Cyber experts at University of Gloucestershire warn tourists planning UK trips to be aware of hackers trying to imitate and infiltrate free Wi-Fi hotspots.


Public Wi-Fi may be really convenient but security is often non-existent.

GLOUCESTER, GLOUCESTERSHIRE, UNITED KINGDOM, May 24, 2023 /EINPresswire.com/ -- As the traditional summer holiday period begins the University has found tourists are a prime-time target for criminals seeking to take advantage of busy travel locations, a particular issue for Gloucestershire which already attracts around 23 million tourists annually.

Last year, nearly 5,000 out of every million internet users in the UK were the victims of cybercrime – up 40% on 2020 figures – as criminals increasingly target people’s devices that become easier to break into when users choose to use Wi-Fi over a mobile connection when travelling.

> These so-called ‘evil twin’ Wi-Fi spots take, for example, the name of a restaurant, shop or café and trick an unsuspecting victim to log in, before infiltrating their device.”
>
> *Professor Buck Rogers, University of Gloucestershire.*

University of Gloucestershire cybersecurity expert, Professor Cameron ‘Buck’ Rogers, said:
“Our ongoing research is identifying an increase in malicious ‘free Wi-Fi’ hotspots that appear to be legitimate but are being used to access the public’s mobile phones and computers.

“These so-called ‘evil twin’ Wi-Fi spots take, for example, the name of a restaurant, shop or café and trick an unsuspecting victim to log in, before infiltrating their device.

“Another common threat is when cyber-criminals take control of public networks and then use

these established connections to control a victim's device and redirect activity to their own network."

"Public Wi-Fi can be really convenient, particularly when travelling in the UK and wanting to keep your data costs down. At the same time, while business owners are trying to provide a helpful service for their customers, security is often non-existent.

"According to Norton's 2022 Cyber Safety Insights report, more than 600 million users worldwide are victims of cybercrime, and most of these begin with hackers accessing public networks.

"In addition, Google's own safety page now states that users should "be careful about using public or free Wi-Fi, even if it requires a password."

University of Gloucestershire cybersecurity expert, Professor Cameron 'Buck' Rogers.

University of Gloucestershire has created a 10-point Guide to Public Wi-Fi Safety, providing invaluable safety tips and scam-busting-signs for UK tourists, international visitors and students to watch out for when exploring local areas of interest for the first time.

Drawing from the Guide to Online Safety, Professor Rogers highlights five top tips that are particularly important to be aware of:

1. Use a Virtual Private Network (VPN) - A VPN is an essential tool for anyone using public Wi-Fi. Easy to download onto your device as an app, it encrypts your data, making it more difficult for hackers to intercept and read. VPNs also mask your IP address, making it more difficult for third parties to track your online activity- its like a protected tunnel for your data.

2. Only connect to 'HTTPS' websites – These are websites where data is encrypted. If it says only HTTP don't use it on public networks. Some browsers show a padlock to indicate an encrypted link and these sites can normally be trusted.

3. Verify network name and security – always double-check the network name and security before connecting to a public wi-fi network. Hackers often create fake wi-fi networks that look legitimate on a quick scan, so it's important to ensure you're connecting to the right one. Look for networks that indicate 'WPA2' encryption – the most secure type of encryption available.

4. Avoid public wi-fi for sensitive activities – accessing your online banking, or business or

personal emails? It's best to avoid accessing sensitive information while connected to public wi-fi. Wait until you're on a secure network before conducting these types of activities.

5. Keep your phone, laptop or tablet updated – before travelling, if you get a new software update alert from your trusted device manufacturer or internet-browser service activate it. This will help ensure your devices are less-exposed to online vulnerabilities and threats.

Mark Ferguson
More Fire PR Ltd
+44 7925 077867
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
Instagram
YouTube
TikTok
Other
