Millions of Brits risk identify theft because they are so eager to use free public Wi-Fi

Submitted by: The PR Room
Monday, 29 July 2019

Is a hotspot real or malicious? Many consumers simply don't check

London – 29th July 2019: New research of 2,000 Brits has revealed that 79% of public Wi-Fi users take significant risks when choosing hotspots. Instead of taking the time to check that a hotspot is legitimate, users are selecting hotspots based on Wi-fi- strength, a name that seems appropriate, or just picking any free option.

Unexpectedly, the figure is highest for the most experienced Brits, with 86% of daily public Wi-Fi users putting convenience ahead of safety when choosing hotspots.

The survey carried out by cybersecurity company, BullGuard (http://www.bullguard.com/), revealed that 4 in 10 users look for a Wi-Fi name that somewhat matches their location, for example 'coffee shop Wi-Fi' – but this is exactly the type of name hackers set up to try and fool people into choosing a malicious hotspot with the intention of stealing personal data.

Even though they've spent little or no time checking that a hotspot is legitimate, many respondents are accessing websites using very confidential data. More than a third of daily public Wi-Fi users log into personal accounts requiring a password, 22% use credit cards, and 31% log into online banking, exactly the type of data hackers are looking to steal.

Despite their eagerness to get online, most people are also very concerned about safety with less than one in ten being 'very confident' that they know how to stay safe when using public Wi-Fi. Furthermore, 62% of daily public Wi-Fi users admit to being afraid that their devices will be hacked and their information stolen. Consumers are most worried about the safety of banking info (68%), passwords (56%) and email content (27%).

"Brits are choosing convenience over safety, when using public Wi-Fi. The findings show that respondents do not feel safe online, yet they are ignoring their fears and are using hotspots without checking they are safe," said Paul Lipman, CEO at BullGuard. "Hackers can easily set up malicious hotspots which appear to be legitimate and yet can intercept and record people's personal data, allowing them to steal usernames, passwords, credit card details, bank account information and more."

The BullGuard survey also revealed that 63% of people that use public Wi-Fi daily have their devices set up to 'automatically connect to the strongest Wi-Fi signal', or to 'automatically connect to Wi-Fi hotspots they've used before.'

"If your device is set up this way, and if you're not paying attention when you first choose a hotspot, even once, and you accidentally choose something malicious, your device will automatically select it every time its within range," Lipman added.

Even if users think they're protected, worryingly the results show that consumers aren't sure how to

keep themselves safe when using public Wi-Fi with almost half (47%) believing antivirus will prevent their data from being intercepted.

“Although essential for detecting and removing malware from your device, antivirus offers no protection at all from having your data intercepted by a malicious hotspot,” said Lipman.

A VPN (https://www.bullguard.com/products/bullguard-vpn.aspx), or Virtual Private Network, is an effective way of keeping you safe online when using public Wi-Fi. It creates a secure connection tunnel between your device and the websites and services you are accessing to keep you safe whether you’re using a smartphone or laptop on public Wi-Fi in a café, or if you want to check online banking accounts from an airport or hotel.
However, the survey revealed that 60% don’t use a VPN, with 57% of those respondents saying they think it’s too complicated or that they don’t know how to use one.

“A VPN doesn’t need to be complicated. For example, BullGuard VPN (https://www.bullguard.com/products/bullguard-vpn.aspx) is designed for regular users. It doesn’t require technical knowledge, install it on your device and it just works 24/7 giving you the peace of mind that you are not being tracked online and that hackers can’t intercept your personal data,” concluded Lipman.

Top activities carried out whilst on public Wi-Fi

Logging into a personal email account (42%)
Using Social Media or any other account with auto login (36%)
Logging into any account requiring a password (31%)
Filling in forms with personal details - e.g. name, address, date of birth, telephone number (18%)
Online banking (17%)

Most popular places to use public Wi-Fi

Hotels (53%)
Coffee shops/restaurants (51%)
Airports (48%)
Public transport (37%)
Retail shops (31%)

STAYING SAFE ON PUBLIC WI-FI NETWORKS

TERMS OF SERVICE

The majority of genuine public networks will ask the user to agree to their terms of service before linking up.
Instead, if you gain immediate access to unrestricted browsing tread carefully - it could be a rogue access point.

BEWARE OF ‘FREE’

Fake public Wi-Fi hotspots typically copy public domain names and add the word ‘free’ as a hook to lure users.
For example, if you’re in a coffee shop, you might see two Wi-Fi options - one called 'Coffee Shop Wi-Fi ' and the other called 'Free Coffee Shop Wi-Fi '.
One of these could be a malicious network and it’s likely to be the free one -
if you’re not sure ask an employee.

WRONG PASSWORDS

If you purposely enter a wrong password to a password protected hotspot and you don’t get an error message the access point is likely fake.
Fake hotspots will commonly let anyone access them regardless of the password entered.

SLOW NETWORK CONNECTIONS

Look out for very slow network connections.
This could be a sign the hacker is using mobile internet to connect you to the web using the fake hotspot.

SECURE WEBSITES

Pay attention to the address bar of the websites you visit.
If for instance a banking website shows HTTP instead of HTTPS - your connection is unsafe.
HTTPS with a padlock symbol means data is encrypted.
HTTP connections without a padlock are unsafe.

USE VPNS

Always use a VPN such as BullGuard VPN on your tablet, phone or laptop.
The VPN tunnel stops people from seeing what you are doing and VPN encryption scrambles your data rendering it useless to hackers.

WHAT IF YOU CONNECT TO A POTENTIAL FAKE HOTSPOT

If you suspect you have connected to a compromised hotspot, follow these steps:

Disconnect as quickly as possible.
Clear your list of saved Wi-Fi connections to avoid connecting to the same one in the future.
Clear your browser cache.
Run antivirus and malware checks.
Change the password to any site you logged in to, and any other websites that use the same login information.
Call your bank and cancel any bank cards if you used them over the connection.

-ENDS-

About BullGuard
BullGuard is a multi-award winning, smart home cybersecurity company. We make it simple to protect everything in your digital life – from your data, to your identity and privacy, and to your Smart Home. The BullGuard product portfolio extends to PCs, tablets and smartphone protection, and includes internet security, comprehensive mobile security, 24/7 identity protection and VPN which provides the highest levels of privacy and protection. BullGuard released the world's first IOT vulnerability scanner and leads the consumer cybersecurity industry in providing continuous innovation. Dojo by BullGuard is an award-winning intelligent defense system and service that provides the highest level of protection to consumers across all of their connected devices and smart homes. Dojo by BullGuard is the cornerstone of a Smart Home, ensuring a connected world where every consumer in every home, is smart, safe and protected.

Follow us on Twitter @BullGuard (http://www.twitter.com/BullGuard) and @DojoSafe (http://www.twitter.com/DojoSafe), like us on Facebook at BullGuard (https://www.facebook.com/BullGuard/?fref=ts) and Dojo (https://www.facebook.com/meetdojo/?fref=ts), or learn more at https://www.bullguard.com or https://dojo.bullguard.com.

Press Contacts:

Sarah Chard
The PR Room
Mail: sarah.chard@theprroom.co.uk
Tel: +44 (0) 333 9398 296
Web: www.theprroom.co.uk

Michelle Cross
The PR Room
Mail: michelle.cross@theprroom.co.uk
Tel: +44 (0) 333 9398 296
Web: www.theprroom.co.uk