Why employees should stop working on public Wi-Fi

As more employees work flexibly, public Wi-Fi becomes a bigger company risk.

How employees use Wi-Fi could seriously affect your business and the safety of its data.

More than half of UK businesses now allow flexible working and 1.5 million people work remotely across the UK each year – often from cafes, bars, hotels and hot-desking.

This trend will grow: future workforces will increasingly include gig-economy workers, including consultants, contractors, freelancers and part-time employees.

This means more employees potentially using open public Wi-Fi – which is often not secure.

Sitting target

Data sent over open public Wi-Fi is unencrypted, which means that anyone on the same network can 'eavesdrop' on an employee's activity and capture their data, including credentials and passwords.

> "Employees are rolling the dice every time they log on to a free network in a coffee shop."

The next potential problem is called 'honeypot'. Hackers might set up their own Wi-Fi hotspot with an unassuming name such as 'Public Wi-Fi' to tempt people to connect so that they can grab any data they send. These can be set up using just a laptop or smartphone – so employees could run into them anywhere.

Data captured on Wi-Fi can be lucrative and organised criminals have been known to target hotel guests.

In 2014 experts from Kaspersky Lab uncovered a hacking campaign called 'Dark Hotel', which targeted CEOs, government agencies, NGOs and other high-value targets while they were in Asia.

When executives connected to their luxury hotel's Wi-Fi network and downloaded what they believed were regular software updates, their devices were infected with malware. The malware could sit inactive and undetected for several months before being remotely accessed to obtain sensitive information on the device.

Even an encrypted public Wi-Fi, where the password is shared, is not completely secure.

Safety tips for employees

- Before you connect, ensure you know whose network you're connecting to. If you're not sure what the public network at a business is called, ask an employee before connecting.
- Use a mobile phone network, if you have good signal reception and sufficient data plan. Consider using your mobile data first, and bypass any Wi-Fi hotspots for activities that require you to send personal and/or confidential data.

LOCKTON®

Broking done *differently*

- Look for 'https' ('s' for secure) or a padlock symbol on the web browser address bar. Https allows for end-to-end encryption from your device and the webpage itself. This means that if someone were to intercept your encrypted traffic, it would be of little to no value. Some websites secure only some pages and not every page on its sites, so always check the address bar for 'https' when entering private information.
- Use a VPN (virtual private network) when you connect to a public Wi-Fi network – this way you'll effectively be using a 'private tunnel' that encrypts all your data that passes through the network.
- Turn off sharing – otherwise shared resources, such as folders, can be visible to anyone on the same network, eg anyone connecting to the same Wi-Fi in the café. Devices such as Windows will prompt you when you connect to a new network whether the network is Home, Work or Public.
- Protect your device – keep the software on your device updated. This can prevent the vulnerability in the software being exploited by the hacker.

> "Data captured on Wi-Fi can be lucrative and organised criminals have been known to target hotel guests."

Employees are rolling the dice every time they log on to a free network in a coffee shop, hotel lobby or airport lounge. It's not just their own data they are exposing but that of their employer. Educating employees about the risks and providing the right equipment is vital.

For more information, please contact Max Perkins on:

max.perkins@uk.lockton.com
+44 (0)20 7933 2694