A COVID 19–DRIVEN INCREASE IN TELEWORK FROM HOTELS COULD POSE A CYBER SECURITY RISK FOR GUESTS

The Federal Bureau of Investigation is issuing this announcement to encourage Americans to exercise caution when using hotel wireless networks (Wi-Fi) for telework. FBI has observed a trend where individuals who were previously teleworking from home are beginning to telework from hotels. US hotels, predominantly in major cities, have begun to advertise daytime room reservations for guests seeking a quiet, distraction-free work environment. While this option may be appealing, accessing sensitive information from hotel Wi-Fi poses an increased security risk over home Wi-Fi networks. Malicious actors can exploit inconsistent or lax hotel Wi-Fi security and guests' security complacency to compromise the work and personal data of hotel guests. Following good cyber security practices can minimize some of the risks associated with using hotel Wi-Fi for telework.

DANGERS OF USING HOTEL WI–FI

Attackers target hotels to obtain records of guest names, personal information, and credit card numbers. The hotel environment involves many unaffiliated guests, operating in a confined area, and all using the same wireless network. Guests are largely unable to control, verify, or monitor network security. Cyber criminals can take advantage of this environment to monitor a victim's internet browsing or redirect victims to false login pages. Criminals can also conduct an "evil twin attack" by creating their own malicious network with a similar name to the hotel's network. Guests may then mistakenly connect to the criminal's network instead of the hotel's, giving the criminal direct access to the guest's computer.

Hotel networks are often built favoring guest convenience over robust security practices. Smaller hotels will often post placards at the service desk stating the password for Wi-Fi access, and change this password very infrequently. At its most robust, access to a hotel Wi-Fi network is typically governed by a combination of room number and password. This combination only governs devices accessing the hotel's network but does not provide a secure internet connection. Currently, there is no hotel industry standard for secure Wi-Fi access. If teleworking from a hotel, guests should not implicitly trust that the hotel has properly secured their network or is monitoring it for attacks.

SECURITY FACTORS OUTSIDE OF GUEST CONTROL

Much of a hotel's network infrastructure is entirely out of the control of the hotel guest. Guests generally have minimal visibility into both the physical location of wireless access points within the hotel and the age of networking equipment. Old, outdated equipment is significantly more likely to possess vulnerabilities that criminal actors can exploit. Even if a hotel is using modern equipment, the guest has no way of knowing how frequently the hotel is updating the firmware of that equipment or whether the hotel has changed the equipment's default passwords. The hotel guest must take each of these factors into consideration when choosing whether to telework on a hotel network.

SPECIFIC RISKS TO BUSINESS DATA

Connecting personal or business devices to the hotel's wireless network may allow malicious actors to compromise the individual's device and then access the business network of the guest's employer. Once the malicious actor gains access to the business network, they can steal proprietary data and upload malware, including ransomware. Cybercriminals or nation-state actors can use stolen intellectual property to facilitate their own schemes or produce counterfeit versions of proprietary products. Cybercriminals can use information gathered from access to company data to trick business executives into transferring company funds to the criminal.

SIGNS YOUR DEVICE HAS BEEN COMPROMISED

If your device is hacked, it probably will not resemble the entertainment industry's portrayal of computer hacking. There may be no visible changes to your device. Some signs that may indicate your computer, phone, or tablet has been compromised include:

- mobile device slows down suddenly;

- websites automatically redirect away from the website you are attempting to visit;
- the cursor begins to move on its own;
- a mobile device begins to launch apps on its own;
- an increase in pop-up advertising;
- a sudden increase in data usage;
- faster than usual decrease in battery life;
- unexplained outgoing calls, texts, or emails.

WHAT TO DO IF YOUR DEVICE HAS BEEN COMPROMISED

- Do not forward any suspected e-mails or files.
- Disconnect the device from all networks immediately and turn off Wi-Fi and Bluetooth.
- Consult with your corporate IT department, ensuring they are notified of any significant changes.
- If there is no IT department, consult with qualified third-party cyber security experts.
- Report cyber attacks or scams to the Internet Crime Complaint Center at IC3.gov.

RECOMMENDATIONS FOR REDUCING THE RISKS OF HOTEL WI-FI

- If possible, use a reputable Virtual Private Network (VPN) while teleworking to encrypt network traffic, making it harder for a cybercriminal to eavesdrop on your online activity.
- If available, use your phone's wireless hotspot instead of hotel Wi-Fi.
- Before travelling, ensure your computer's operating system (OS) and software are up to date on all patches; important data is backed up; and your OS has a current, well-vetted security or anti-virus application installed and running.
- Confirm with the hotel the name of their Wi-Fi network prior to connecting.
- Do not connect to networks other than the hotel's official Wi-Fi network.
- Connect using the public Wi-Fi setting, and do not enable auto-reconnect while on a hotel network.
- Always confirm an HTTPS connection when browsing the internet; this is identified by the lock icon near the address bar.
- Avoid accessing sensitive websites, such as banking sites, or supplying personal data, such as social security numbers.
- Make sure any device that connects to hotel Wi-Fi is not discoverable and has Bluetooth disabled when not in use.
- Follow your employer's security policies and procedures for wireless networking.
- If you must log into sensitive accounts, use multi-factor authentication.
- Enable login notifications to receive alerts on suspicious account activity.

The FBI encourages victims to report information concerning suspicious or criminal activity to their local field office (www.fbi.gov/contact-us/field-offices) or to the FBI's Internet Crime Complaint Center (www.ic3.gov). For additional resources and best practices for staying safe while teleworking—such as guidance on managing VPNs, videoconferencing, or using wireless devices for telework—visit https://www.cisa.gov/telework.