Secure WiFi check-list

This checklist for securing WiFi is based on our experience and working from home should now include these organisational measures.

Organisation, router or access point (AP) methods

- [ ] Set a strong WPA2/WPA3 password on your router. As a bare minimum, we suggest 12 characters, but this can be up to 64 characters.
- [ ] Use WPA2 authentication as a minimum (do not use WEP or WPA). Upgrade to WPA3 if the budget permits.
- [ ] Ensure client certificate validation is enforced on WPA2-Enterprise networks and connection from non-compliant devices is disallowed.
- [ ] Enable ‘Encryption of Management Frames’ in the router. Unfortunately only high-end routers typically support this feature.
- [ ] Keep your router firmware up to date.
- [ ] Activate MAC address restrictions in your router to connections from trusted devices only.

  *Regular monitoring and safe-listing of devices is recommended.
- [ ] Disable WPS and UPnP.
- [ ] Change your default router administration credentials.
- [ ] Disable remote administration and administration via WiFi for the router (internal fixed network only).
- [ ] Hide your SSID.

Organisation, router or access point (AP) methods

- [ ] Use the router firewall to restrict access to the minimum services (ports) and IP addresses required.
- [ ] Reduce the WiFi range on your router to the minimum possible without disrupting normal use.
- [ ] Switch off the wireless router when not required. This can be scheduled in the device or setup using a simple power socket timer.
- [ ] Establish AP safelists and actively monitor, track and locate unauthorised APs and other malicious activity.
- [ ] Avoid open sharing of WiFi access credentials.
- [ ] Make staff aware of common WiFi phishing and Man-In-The-Middle attacks.

End user and WiFi device methods

- [ ] Disable WiFi on your device and only enable it when you are connecting to a known trusted Access Point.
- [ ] Avoid automatic connections when setting up a new WiFi connection or, at the very least, remove stored automatic connections for Access Points you do not regularly use.

End user and WiFi device methods

- [ ] Use a VPN when accessing the internet over untrusted connections where possible, but be aware that VPNs themselves need to be well vetted as they have direct access to your communications and like any system have potential vulnerabilities.

- [ ] Never enter or view sensitive information with a web site that does not support encrypted (HTTPS) communications (the lock symbol in your browser).

- [ ] Never connect to an open WiFi network (no password required) unless you are actively managing the risk.

- [ ] Ensure all internal network server endpoints such as printers have encrypted (HTTPS) communications. Printers for example are often overlooked, allowing all printed documents to be viewed by packet capture if WPA2 network credentials can be obtained.

- [ ] Make yourself familiar with common WiFi exploits, particularly if you are dealing with sensitive information.

- [ ] If outside a secure environment, consider using portable unauthorised WiFi device detection and tracking equipment before exposing any sensitive data.

Of course the best way to take care of unauthorised WiFi is to locate and remove it. With HackHunter's Pursuit portable WiFi tracker, you can actually locate WiFi to within a few centimetres.

If you're interested in learning more, contact us today at info@hackhunter.io or on (03) 8669 2090