Guest Internet Solutions
WI-FI HOTSPOTS MADE EASY

Business Solutions

Implement Network Cyber-security with Managed WiFi

Managed WiFi Cybersecurity Controls

- □ Access control to the network, choose to authorize the device or authorize the user.
- □ Device authorization via a database of device MAC addresses, monitoring of MAC duplication (MAC spoofing).
- □ User authorization via a database of passwords that permit the user to access on any device.
- □ User authentication can also be made using 2-factor authentication (code via text)
- □ Block Internet access to categories of websites evaluated as harmful (Cisco Umbrella).
- □ Block access to services that might be used to install a Trojan virus, for example, personal email accounts.
- □ Monitor the WiFi network for attempted unauthorized access.

The post-pandemic trend to hybrid work from home and office has meant that staff has switched from wired desktop computers to wireless computers and mobile devices.

Businesses have expanded WiFi networks while reducing security requirements.

WiFi is now an easy attack vector both locally and remotely for a hacker intent on stealing data or planting ransomware.

Businesses must evaluate WiFi as part of a security assessment.

Managed WiFi is a technology that was developed to control and monitor the use of WiFi networks in order to protect the WiFi network from access by unauthorized devices that may be used by hackers to steal information, of lock-down the business database using Ransomware.

1. SECURITY ASSESSMENT

Ensure that the business WiFi network is included in the security assessment, consider upgrading the encryption from WPA2 to WPA2-enterprise or WPA3 to make hacking harder.

2. DEPLOYMENT OF SECURITY PROTECTIONS

In addition to the Internet firewall and business email filtering to remove harmful links, consider adding the Managed WiFi cybersecurity controls listed in the box at left.

3. ON-GOING MONITORING

The Managed WiFi access control provides a real-time display of attempted accesses to the WiFi network. Monitor the situation and block access to unauthorized MAC addresses that request an IP address.

4. ADDITIONAL BENEFITS OF MANAGED WiFi

Managed WiFi will monitor the performance of the WiFi network and can provide a failure alarm when any WiFi device fails. This is very important as a wireless access point failure is not noticed because the wireless device will connect to another wireless access point further away with a slower data speed. Eventually users will complain that the “network is slow”. The managed WiFi device failure detection will identify the device that must be replaced.

Call 1-800-213-0106 or write to: support@guest-internet.com

Guest Internet Solutions is a business unit (DBA) of Fire4 Systems Inc., a Florida Corporation. Copyright © Fire4 Systems Inc., 2022. All rights reserved.
Fire4, Guest Internet, Hospitality Internet and the respective logos are registered marks of Fire4 Systems Inc.
All other registered marks, trademarks, service marks and logos are the property of their respective holders.