Reduce the security risk of your web-enabled devices

Your 10-step guide

When you look around your organisation, how many of the appliances are web-enabled, and are you aware of the security risk they pose?

More and more of our everyday devices are being connected to the Internet. Everything from smartphones, laptops and cameras to more unexpected gadgets like toasters and even kitty litter trays are being connected to the network known as the 'Internet of Things' (IoT).

While this connectivity brings convenience, it also introduces significant security risks, and protecting your devices from cyber threats is essential.

Securing your web-enabled devices is an ongoing process requiring vigilance and proactive measures – but it is possible to ensure a safer online experience for your workplace and clients.

Here are ten effective strategies to lower the security risks associated with your web-enabled devices. Use this for your business operations and offer the same guidance to your home care clients, where relevant.

1. Regularly update software and firmware

Keeping your devices' software and firmware up to date is crucial. Manufacturers frequently release updates that patch security vulnerabilities and fix bugs. Enable automatic updates whenever possible, or manually check for updates regularly to benefit from the latest security enhancements.

2. Use strong, unique passwords and enable Multi-Factor Authentication

Create strong, unique passwords for each device and online account. A strong password includes a mix of letters (both uppercase and lowercase), numbers and special characters. Use a reputable password manager to generate and store your passwords securely. Enable Multi-Factor Authentication (MFA) wherever possible for an extra layer of security, requiring a second form of verification like a text message code.

3. Secure your home network

Your home or office network is the gateway to all your web-enabled devices. Change the default login credentials of your router, use a strong password for your Wi-Fi network, and enable Wi-Fi Protected Access 3 (WPA3) encryption if supported. Set up a separate guest network to prevent visitors from accessing your main network. Regularly check for unknown devices and update your router's firmware to ensure it has the latest security patches.

4. Implement network segmentation

Network segmentation divides your network into smaller, isolated segments to limit the spread of a potential security breach. Create separate segments for work devices, smart home devices and guest devices. Many modern routers support network segmentation through features like Virtual Local Area Networks (VLANs), offering substantial security benefits despite the technical setup required.

5. Educate yourself and others

Human error is often the weakest link in cybersecurity. Educate yourself, your team and your clients about security practices, including recognising phishing attempts, the importance of regular updates and securing each type of device properly. Stay informed about the latest cybersecurity threats and trends by following reputable sources and regularly reviewing your security settings and practices.

6. Maintain a device inventory

Keep track of all connected devices on your network and review this list regularly. Remove or secure any unused devices to maintain better control over your network and reduce potential entry points for attackers.

7. Use IoT-specific security software

Consider using security solutions designed specifically for IoT devices. These can provide additional protection against threats unique to connected devices, enhancing overall security.

8. Ensure physical security

Ensure that IoT devices, especially those placed in accessible areas, cannot be tampered with or stolen. Physical access to a device can often lead to a security breach, so it's important to secure these devices physically.

9. Conduct regular security audits

Perform periodic security assessments of your entire IoT ecosystem. Regular security audits help identify potential vulnerabilities before they can be exploited, ensuring ongoing protection.

10. Consider Artificial Intelligence risk

As Artificial Intelligence (AI) becomes more prevalent, be aware of the risks associated with sharing information that can be mined, profiled and used by AI systems. Be mindful of data sharing, read privacy policies and be cautious with biometric data like facial recognition and fingerprints. Regularly review and clean up your digital footprint to mitigate these risks.

QPS Benchmarking
qpsbenchmarking.com