Build Resilience Against Malware Attacks

Malware is a term used to describe any malicious software designed to harm, exploit, or damage computer systems, networks, or devices. Malware can take various forms, including viruses, Trojans, worms, and spyware. It can be spread through infected email attachments, software downloads, or by exploiting system vulnerabilities.

Some general tips to follow:

1 Install Anti-virus & Anti-spyware

Keep your security tools up-to-date, remove detected malware promptly, and audit your files regularly to identify potential security breaches.

2 Use Secure Authentication Methods

Use strong passwords, enable multi-factor authentication, and avoid saving passwords on your computer or network. Use biometrics if possible.

3 Keep Software Updated

Keep your software up-to-date by installing the latest patches and updates, perform routine maintenance checks, and review log reports for signs of malware.

4 Secure Your Emails and Block Spam

To secure your emails, scan for malware, block spam, and limit user access to approved links and email addresses.

5 Switch On Your Firewall

Firewalls establish a "buffer zone" that separates your network from external networks, such as the Internet.

6 Use Secure Networks

A secure network ensures privacy, protects personal information, and boosts confidence while browsing the web.

7 Limit Application Privileges

Secure your business from hacking attempts by restricting application privileges. Limit access to only necessary features and functions to minimise potential entryways for hackers.

8 Educate Users

Train and educate users regularly to prevent security breaches from phishing and malware.

To build resilience against malware attacks, prioritize strong security measures such as user education, restricted privileges, and proactive monitoring. Taking preventative action and staying vigilant is key to safeguarding your network.

03456 831 111 | www.silver-lining.com | info@silver-lining.com