WEBROOT
an opentext company

HOW MSPs AND BUSINESSES CAN AVOID RANSOMWARE ATTACKS

By following a few simple tips, businesses and MSPs can drastically reduce the chances they'll fall victim to ransomware.

- [ ] **Deploy reputable, next-gen endpoint security with AI.**

  Look for endpoint security solutions that use AI to predictively and proactively stop phishing and other threats, and which continuously monitor individual endpoints.

- [ ] **Deploy backup and business continuity solutions.**

  If you get infected with ransomware, you need to recover data quickly to minimize business downtime. Implement a secure backup and disaster recovery plan, and test backups regularly.

- [ ] **Disable unnecessary services, like macros, scripts, and autorun.**

  Many types of malware take advantage of macros, scripts, and autorun to infect systems and propagate. While these services have legitimate uses, they are often unnecessary; and can present a massive security risk. Disabling them is an easy way to help prevent infections.

- [ ] **Use Windows® policies to your advantage.**

  Set policies to mandate the use of strong passwords, enforce access privilege, and block certain paths and file extensions from running. You can set these up in groups, too, allowing different teams to have different levels of network and application access.

- [ ] **Keep plugins, applications, and operating systems patched.**

  Malware authors specifically target unpatched vulnerabilities in older Windows operating systems, software, firmware, and plugins. Keep them up to date and disable or uninstall unnecessary apps and plugins where applicable.

- [ ] **Restrict remote desktop protocol (RDP) access.**

  Criminals look for systems with commonly used RDP ports and attack them using brute-force tactics, hoping to break through weak usernames and passwords. By restricting or disabling RDP, or simply requiring two-factor authentication, you can help close this security gap.

- [ ] **Educate your end users.**

  Plain and simple: phishing scams are still a threat because people still fall for them. Providing training and phishing simulations will help you create a security-aware culture so your users (and business) can avoid becoming a ransomware victim.