WEBROOT
Smarter Cybersecurity™

WHAT CAN MSPs AND BUSINESSES DO TO SECURE THEMSELVES AGAINST ATTACKS?

- [ ] **Implement strong endpoint security.**

  Be sure you're using a solution that offers real-time protection and automatic remediation capabilities. If you haven't already, look into automated detection and response.

- [ ] **Add preventive protection at the DNS layer.**

  DNS-layer security can stop up to 88% of attacks[1] before they even hit employees and their endpoints. Plus, it protects remote/mobile workers and can help you secure any guest WiFi networks you provide.

- [ ] **Invest in a security awareness training solution.**

  After 12 months of ongoing phishing simulations and security awareness training courses, end users are 70% less likely to click through on a phishing message.[2] Enough said.

- [ ] **If you don't need RDP, turn it off.**

  Cybercriminals target commonly used RDP ports and attack them using brute-force tactics, hoping to break through weak usernames and passwords to access systems. If you're not actively using RDP, just disable it.

- [ ] **Disable other unnecessary (and vulnerable) services.**

  Malware variants can be delivered through email attachments, typically a zip archive that contains a script. That means you can help prevent attacks simply by disabling scripts. Additionally, Microsoft® Office macros are typically unnecessary, and some ransomware types use macros in documents to deliver malicious payloads. Disable those too.

- [ ] **Do your updates. Yes, all of them.**

  Major news-making hacks (think WannaCry a few years back, etc.) exploit vulnerabilities in out-of-date operating systems. Make sure the systems you manage are up to date on software and OS patches, security fixes, and other updates.

- [ ] **Back everything up and test your backups regularly.**

  A well-planned backup and disaster recovery strategy can ensure you're back up and running without missing a beat, in the event of a security breach or malware attack.

- [ ] **Embrace 2FA and enforce good password policies.**

  It'd look pretty bad if your organization or clients got breached because of a weak (or default) password. Set security policies to ensure that doesn't happen, and implement 2FA wherever possible.

[1]Based on threats identified by Webroot after scanning real-world network traffic

[2]Webroot Inc. "2019 Webroot Threat Report." (February 2019)