ThreatDown™
Powered by Malwarebytes

12 Days of Cybersecurity Tips

It's easy to overindulge in the holiday season but there's only so much cybersecurity info you can consume in one sitting. So, to save you from information indigestion, here are 12 bite-sized security morsels to satisfy your appetite for cybersecurity this holiday season.

1

To err is human. Human error is responsible for **74%** of data breaches. Train your people to recognize threats, but don't leave them high and dry. Support them with a mixture of proactive and reactive technology, like MDR and ransomware rollback.

2

Your customers and suppliers could be weakening your defenses—**91%** of organizations experienced a supply chain incident in 2023. Protect your business by vetting third-party software and implementing strict access controls for external partners.

3

Be careful what you share with AI—it can be a very powerful tool, but it never forgets, and it could share what you tell it with other people. Don't share company data or PII with public AIs like ChatGPT or Gemini.

4

You should change your admin credentials from time to time as a precaution, but doing it too often costs money and doesn't improve security. The sweet spot to rotate passwords for service accounts is **30 to 90 days.** Everyone else should choose a unique password and then leave it alone!

5

Ransomware gangs want to explore your network as quickly and quietly as possible. Segment your network to slow them down—the slower and harder they have to work, the easier it is to spot their activity.

6

Hardcoded API keys are a security no-no that leads to a **lot of compromises**. Never hardcode authentication credentials like tokens, keys, or app-related secrets into your code. Instead, consider using a secret manager.

7

48% of APT groups use administration tools and commercial penetration testing tools. Restrict their use to administrators and authorized penetration testers and block any popular tools they don't use.

8

Backups are your last line of defense against ransomware, but they can only help you if they work. Keep your backups offline, so ransomware gangs can't delete them, and restore your backups regularly to test they work.

9

Most ransomware attacks happen between 1AM and 5AM in the morning. Attackers know when you turn the lights out and go home, so that's when they go to work. Protection requires around-the-clock alertness from a SOC, MSP or MDR team.

10

Although cybercriminals can turn security patches into exploits very quickly, most attacks rely on old vulnerabilities because many organizations struggle with patching. Automate your protection with Vulnerability Assessment and Patch Management.

11

In 2023, 82% of data breaches involved data stored in the cloud. Protecting your hybrid and cloud environments is just as important as protecting your physical devices.

12

Attackers increasingly use hands-on keyboard activity to stay hidden and adjust their tactics to match whatever environment they find themselves in. Defenders need to be ready to detect suspicious commands, isolate compromised machines, and kill malicious processes in real-time.

ThreatDown™ Powered by Malwarebytes | threatdown.com | sales@threatdown.com