Tips & Steps to Stay Cyber Safe This Memorial Day Weekend

IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

A long weekend is ahead and that means employees are ready to unplug. Focus will soon shift to travel, sunshine, and time away the daily work tasks. While people are out of office, companies still need to prioritize cybersecurity and their resilience.

Before you set your out-of-office reply and head for the beach, make sure you've checked off the essentials to protect your organization from the threats that don't take time off.

Security Awareness Training for Employees

Employees are your first line of defense and ongoing training empowers employees to help recognize, avoid, and report threats that could lead to a breach. Security training can assist individuals in identifying phishing emails, payment card scams, hacktivist DDoS campaigns, and more.

Beware of Scams

Phishing and other scams like fraudulent charity schemes and fake solicitations can spike during holidays when people are often distracted. Avoid clicking on links or downloading attachments from unknown senders. Educate your employees with resources on how to identify and avoid phishing scams. If it sounds too good to be true, it probably is!

Update Communications Plan

During a holiday weekend, out-of-office employees are high and the typical chain of communication may be disrupted. Make sure to define and publish an escalation process for emergencies, list corresponding escalation contacts, and ensure your team and stakeholders have appropriate awareness and access to the document. In addition, confirm primary and secondary backups for your response team's shifts during the holiday weekend.

Secure Network and Devices

Employees may be working remotely this holiday weekend and it is important to remind them of the importance of secure networks and devices. Avoid using public Wi-Fi while accessing sensitive information. Use Virtual Private Network (VPN) whenever possible to encrypt their internet connection. Ensure any laptops, phones, or tablets are updated with the latest security patches and are password protected.

Current Threat Intelligence

We know cyber threats don't take time off - neither does threat intelligence. Review and monitor changes in landscape through threat intel feeds, advisories, alerts, and collaboration with partners, peers, and ISACs. Also, enable automated notifications on your threat intel platform or MSSP to receive urgent alerts via email or SMS.

Did You Know?

IT-ISAC tracked recorded a total of 1,537 ransomware attacks in Q1 2025, highlighting a 1.51% increase over the previous quarter. The top three targeted sectors this quarter were:

- critical manufacturing
- commercial facilities
- information technology

MEMBERSHIP@IT-ISAC.ORG

IT-ISAC.ORG