IT ISAC

FOUNDED 2000

CSaaS SIG
An IT ISAC Community

Tips & Steps To Stay Cyber Safe This Holiday Season

It is one of the most joyful times of the year - employees look forward to the festivities, family, and out-of-office time. With the focus shifting during the holiday season, and with many staff taking time off, companies must still maintain their cyber defenses and stay vigilant across the organization.

We recommend making your list and checking it twice to protect you from the people that are not nice with these tips for the holiday season.

EMPLOYEE AWARENESS TRAINING

We completed Cybersecurity Awareness Month in October, but this is an ideal time to continue to inform and train employees on the various attacks and methods employed during the holidays – including but not limited to phishing, payment card scams, typosquatting domains, and hacktivist DDoS campaigns. Ensure that temporary employees and contractors undergo the same security awareness training as permanent employees.

BEWARE OF PHISHING SCAMS

Be cautious with holiday-related emails, deals, or shipping notifications. 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!

CHECKS AND BALANCES

- ✓ Review access controls for critical assets and sensitive data, including removal of temporary access and/or entitlements that are no longer required to reduce potential attack surface and risks.
- ✓ Run a quick administrative account audit to ensure only appropriate employees have access to critical resources.

UPDATE COMMUNICATIONS PLAN

- 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.
- Confirm primary and secondary backups for your response team’s shifts during the holiday season.
- Understand and document how to contact critical vendors or clients during the holiday season.
- Remember: attackers may take advantage of limited staffing and attention, so it's important to stay vigilant.

CONDUCT PLAYBOOK PRACTICE EXERCISES

Assess your incident playbooks, contacts, and ownership roles and conduct one or more practice exercises or drills to be ready and prepared for any potential security events that occur with holiday-limited available staff and expertise.

CURRENT THREAT INTELLIGENCE

Review holiday-specific threat intelligence reports/IoCs and implement monitoring and detection capabilities accordingly for the unique holiday risk timeframe.

SECURE NETWORK AND DEVICES

Remind employees while traveling and on the road to avoid using public Wi-Fi for online shopping or accessing sensitive information. They should use a Virtual Private Network (VPN) whenever possible to encrypt their internet connection.

UPDATE SOFTWARE AND DEVICES

Ensure that all software, operating systems, and devices are up-to-date with the latest security patches and updates.

CHARITABLE DONATION SCAMS

- Be wary of charitable donation scams and associated malicious holiday donation domains; provide guidance on how to identify legitimate organizations over fraudulent ones and verify employee donations supported by the organization for accreditation validation, matching, etc.
- Business Email Compromise scams can also increase during the holidays. Ensure that employees are trained in the correct processes for financial transactions and don’t circumvent them during the holiday rush.