Holiday Shopping Tips for Retailers

The holiday shopping season is in full swing, and retailers all around the globe are gearing up for the surge of orders that come in the weeks before the holidays. In light of the challenges retailers face, **it is essential to prioritize cybersecurity risks.**

Below are cyber readiness tips retailers should follow to **stay safe** while shopping online.

Tip #1 Keep Software Updated

- Turn on **auto-updates** for all software.
- Each update contains the latest fixes and patches, which can protect you against potentially dangerous threats.
- **Rebooting your computer** is also another way to ensure patches get installed.

Tip #2 Define Your Cybersecurity Policies

- **Train all your employees** on your cybersecurity policies.
- Show employees the significance of cybersecurity and the role it has in their personal and professional lives.
- **Enroll in our free Cyber Readiness Program** and access other CRI resources to develop good cyber readiness habits.

Tip #3 Ditch the USBs

- USB drives are handy for transferring files between computers, but they can also be used to deliver **viruses and malware**.
- Set up a **non-company network computer** that can be used to scan USB drives for malware and remove the information from the drives.
- Adopt an **online or cloud-based file-sharing system** that is access protected so you don't need to use a USB.

Tip #4 Watch for Holiday Phishing

- **Remain vigilant for phishing scams** and malicious messages that try to take advantage of busy and distracted shoppers.
- Check the sender email address and **review emails carefully** to make sure the sender is legitimate. If it sounds too good to be true, it probably is!
- **Never click on links**, download attachments or respond with information from unknown senders! Even if you do "know" the person, it's always good to message or call them to verify before taking action.

Tip #5 Keep Passwords Secure

- Make sure your passphrases are **strong and unique** to every account.
- Enable **multi-factor authentication (MFA)** on all your accounts, "where available."
- Never disclose your passwords with anyone and always **change your passwords after trips** or activities where you have logged in to an account on another person's device.

Is your organization Cyber Ready? Discover how you can create your own policies to prepare for, respond to, and recover from a ransomware attack.

Sign up for free at **BeCyberReady.com**

CYBER READINESS
INSTITUTE