FORWARD-THINKING

CYBER SAFETY TIPS FOR GROCERS

As cyberattacks rise, modern grocers need to take cybersecurity seriously.

Extortion and Ransomware

- Ransomware can cause major business interruption. One attack can shut down cash registers, disable HR systems and force grocers to close their doors.
- Ransomware attacks increased 150% between April 2020 and July 2021, according to ENISA.
- Ransomware attacks often stem from email phishing campaigns, software vulnerabilities or remote desktop protocol vulnerabilities.
- The FBI has additional tips for avoiding and responding to ransomware.

Log4J Attacks

- A Log4J vulnerability could give hackers access to your computer systems and data.
- The FTC says that organizations need to update their Log4j software by going to the Apache Logging Services website.
- Companies that fail to take remedial steps could be guilty of violating the FTC Act.
- See the FTC announcement and CISA guidance for more information.

Social Engineering Schemes

- Social engineering schemes use manipulation tactics. Examples include business email compromise (BEC) and phishing.
- The FBI's Internet Crime Complaint Center received 19,369 BEC complaints in 2020, and losses totaled more than $1.8 billion.
- Deepfake technology may result in a wave of more sophisticated BEC attacks.
- The FBI has more information on BEC schemes and tips on how to protect your business.

Cyber Safety Best Practices

- Cyberattacks can result in business interruption, fines, reputational damage, financial loss, data loss and more. Protect yourself.
- Use multi-factor authentication (MFA). MFA can protect your systems and accounts against many common cyberattacks.
- Install updates and patches. This includes Log4j updates, as well as updates for any other programs you use.
- Train workers on cybersecurity. This includes choosing strong passwords, using multi-factor authentication, avoiding malicious links and spotting red flags that could indicate fraud. Provide regular reminders on key issues.
- Question urgent requests for wire transfers or other unexpected changes to protocol. Verify that the request is legitimate before proceeding.
- Have a cybersecurity expert review your systems for vulnerabilities.
- Create a cyberattack response plan.
- Purchase cyber liability insurance. Hackers are always finding new ways to attack. Insurance gives your business an added layer of protection.

Joe Scarpello:
jscarpello@riskpointins.com
253.444.5584

CONTACT US TODAY!

Melissa Johnson:
mjohnson@riskpointins.com
253.444.5654

RISKPOINT
INSURANCE ADVISORS

Advocate | Protect | Defend | Advise