CYBER READINESS
INSTITUTE

Seasons Greetings! Tips for Staying Cyber Safe Over the Holidays

Around the holiday season, businesses and consumers are both at risk when it comes to cyber attacks. Many governmental organizations, including the FBI, Critical Infrastructure Security Agency (CISA), and the UK's National Cybersecurity Centre have released guidance on the best ways to stay safe throughout this holiday season. The Cyber Readiness Institute (CRI) has packaged up the highlights of these notices into a two-part holiday guide for consumers and retailers.

Consumers

Be aware hackers are always looking for the most efficient ways to reach you.

Holiday phishing (or smishing) via text messages (SMS) have nearly doubled from last year according to a report released by Proofpoint.

Hackers are sending messages through text and emails **mimicking delivery notifications**, tracking notifications, or holiday deals.

Best Practices:

- Check your devices: Use strong passwords or passphrases of at least 15 characters, update your software, and turn on multi-factor authentication.
- Shop only through trusted sources: Think about how and where you're making purchases online.
- Recognize phishing scams: Don't click links or download attachments unless you're confident where they came from. Double-check the sender's email address and be wary of requests for personal information.
- Never provide your password, personal or financial information in response to an unsolicited email or phone call.
- Use safe methods for purchases: Never provide financial information when using public Wi-Fi.
- Use a credit card, when possible, as opposed to a debit card and check your account statements frequently.

guide@cyberreadinessinstitute.org

Retailers

This is the busiest time of the year not only for you, but also for hackers.

Be aware of ransomware attacks. In 2020, many attacks hit well known businesses over U.S. holidays when adversaries knew companies would be scrambling to fulfill orders.

Sophos Labs estimated that in 2020, **retail was the most hit sector for cyber attacks**. Remember, hackers may try to go through you to get at your customers or suppliers.

Sources:

https://www.cisa.gov/news/2021/11/23/cisa-shares-tips-keep-your-personal-data-and-financial-data-safe-holiday-shopping?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202

https://www.politico.com/newsletters/national-security-daily/2021/11/22/chinas-missile-turducken-495192

https://us-cert.cisa.gov/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats

https://www.cisa.gov/news/2021/11/22/cisa-and-fbi-urge-organizations-remain-vigilant-ransomware-and-cyber-threats

https://www.proofpoint.com/us/blog/corporate-news/holiday-shopping-themed-mobile-attacks-increase-dramatically

https://us-cert.cisa.gov/ncas/alerts/aa21-243a

https://www.washingtonpost.com/politics/2021/11/24/happy-hacksgiving-officials-warn-surge-cyber-threats/

Best Practices:

- Identify technology and cybersecurity workers who can respond rapidly over the holiday if there is a cyber incident.
- Give staff extra warnings about being wary of phishing emails and other cyber scams over the holidays.
- Make sure software patches are up to date on all company devices and all personal devices used by your staff to do their job.
- Mandate strong passwords, ensuring they are not reused across multiple accounts.
- Make sure every computer system requires users to use multi-factor authentication, especially for remote access and administrative accounts.
- Remind employees not to click on suspicious links, and conduct exercises to raise awareness.
- Review and, if needed, update incident response and communication plans to list actions an organization will take if impacted by an incident.
- Make sure your important systems and data are securely backed-up to a location that is not connected to your network.

Reminder:

If you are a victim of a cyber attack, please report the incident to your government's cybersecurity agency, for example: CISA, FBI, UK National Cybersecurity Centre, Interpol.

Visit becyberready.com, cisa.gov/shop-safely, us-cert.cisa.gov/ncas/alerts/aa21-243a, and stopransomware.gov for more information and best practices on how to stay safe through this holiday season.

CYBER READINESS INSTITUTE