5 Tips to Stay Cyber-Secure This Holiday Season

December 7, 2017
By SentinelOne

From Black Friday through Christmas, the holiday season is a busy time for most companies. However, no matter how frantic things get in the workplace, it is important to remain vigilant about security threats. Cyber criminals are also trying to earn some extra cash at this time of year, and they will be ready to exploit any weakness in cyber security systems. Follow these five tips to stay cyber-secure your business safe as we move toward the new year.

1. Patch Software and Operating Systems

Businesses that have not yet installed the latest security patches for their operating systems, software, and applications are at increased risk of becoming the victim of a cyber attack. Patches include fixes for security flaws in the applications people in the organization use every day. Be sure to download and install them across the business network.

2. Protect Against Malware

If hackers manage to install malware on a computer network, they may be able to steal sensitive financial and personal data about customers. This kind of data leak is the last thing any company needs as the holiday season approaches, as protecting reputation is vital to ensuring sales at this time of year. Install anti-malware software and endpoint protection to ensure that you are monitoring your network for any abnormal activity.

3. Train Employees to Spot Spear Phishing Attacks

Employee training is vital to keep organizations safe at this time of year. Eighty percent of data breaches involve an employee making a mistake, such as clicking on a dangerous link or downloading an infected file. Another common type of online attack is the spear phishing attack, in which criminals target employees inside a company with messages that supposedly come from someone higher up in the organization. These emails can trick employees into sending money or valuable data to the criminals. Train employees to tell the difference between a genuine internal email and one that comes from outside the company. Encourage them to always check instructions they receive in emails to avoid falling victim to scams.

4. Be Careful with New Hires

Many businesses need to bring in extra employees to help over the holiday period, but it's important to ensure that these temporary hires don't expose the company to serious security risks. Always carry out background checks on new hires. Give them access only to the parts of the network that they need to carry out their roles. Finally, be sure to give all temporary hires the same security training that permanent staff receive.

5. Review the Disaster Recovery Plan

Experiencing a data breach or ransomware attack during the holiday season can cost a company. In addition to the value of any data that the hackers manage to steal, it is also necessary to consider the cost of the time employees will spend dealing with the attack during this busy period. Having a solid disaster recovery plan in place can help businesses quickly restore normal operations if they experience a successful cyber attack. Check the disaster recovery plan to be sure it is up to date and relevant to the current state of the business.

Conclusion

December can be a dangerous time for companies with the amount of information being processed during the holiday rush. However, with a little forward planning business can stay safe. Use these tips to promote good cyber hygiene and stay cyber-secure as we move into the new year.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Cyber Insurance – Is it Enough?
- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022
- More Evil Markets | How It's Never Been Easier To Buy Initial Access To Compromised Networks
- 4 Steps Toward Successfully Measuring the Effectiveness of Your Security Controls
- Advancing Security | The Age of AI & Machine Learning in Cybersecurity