EINPRESSWIRE

CISA, FBI Urge Small Businesses to Increase Protection Against Email Cyber Threats This Holiday Season

NEW JERSEY, UNITED STATES, December 1, 2022 /EINPresswire.com/ -- CISA, FBI Urge Small Businesses to Increase Protection Against Email Cyber Threats This Holiday Season
The United States government security apparatus is recommending shoppers and businesses be extra vigilant online during this holiday season, implement additional protection measures against fraud where necessary, and follow security best practices to avoid becoming a target.

CISA is urging businesses and users to stay vigilant as the holiday season is also a time for an increase in cyber attacks. CISA Director Jen Easterly said, “As the nation’s cyber defense agency, our goal is to make sure Americans are safe online, especially during the holiday season.” Easterly added that by following basic cyber hygiene measures to keep ahead of the threats.

Holiday Scams Could Cost Business
Retail businesses in particular must take precautions around the holidays, as increased transaction volumes can make it that much more difficult to spot suspicious activity. This time of year is a common time for businesses to conduct benefit enrollment, end-of-the-year raises, or other changes that are communicated via email. Often, attackers will imitate these communications resulting in a hacker gaining access to sensitive business data, passwords, or other company information.

Invoice and payment scams are particularly difficult to detect. Fake billing poses a significant risk, with a median loss of $100,000, as invoice or payment fraud is a common tactic used in business email compromise (BEC) attacks. Anyone with the authority to pay an invoice from the shipping clerk to the CEO is at risk.

Brand impersonation is another classic tactic that attackers use, with Microsoft being the most commonly impersonated brand. Reports from the Federal Trade Commission show that victims experienced $2 billion in total losses between October 2020 - September 2021.

Threats Businesses Face
Businesses in every industry have experienced several threats in 2022 and must be aware that the risk of a cyberattack only increases during the holidays. Phishing, malware, SQL injection, and distributed denial-of-service (DDoS) attacks are the most common threats for retail businesses during the holidays.

*Phishing: a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.
*Malware: software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interfere with the user's computer security and privacy
*Ransomware: a type of malware that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid.
Account Takeover: an attack involving cybercriminals compromising online accounts using stolen passwords and usernames.

How To Stay Safe Online This Holiday Season
Cybercriminals are coming up with new ways to exploit a business's vulnerabilities and break into their systems. Some basic ways to spot harmful emails include:

*Check the sender's email address: an official-looking email address doesn't necessarily mean that it's official, but a random email address with no relation to the legitimate sender should be treated with caution.
*Look for spelling, punctuation, and grammar mistakes: official emails should be free from common mistakes. Pay particular attention to phrasing in the email, as many scammers know English as a second language.
*Check links before clicking on them: hover over any links to have them displayed in your email client before clicking to verify they are actually going to the genuine website.
*Think about what the email asks for: legitimate organizations will never request your Social Security number or other account details via email.
*Avoid opening attachments in emails: opening an attachment in a phishing email can spread malware, such as ransomware, to activate locking up your computer and encrypting documents to block access.

Basic protocols are an important first step in your security strategy, however, there are several other techniques that can help maximize security efforts, including:

*Train Your Employees: training users on security policies is critical, as human error is a leading cause of data being compromised.
*Security Monitoring: IT infrastructure monitoring is a crucial part of cyber risk management, enabling organizations to detect cyberattacks as they emerge and respond to them before they cause damage.
*Compliance: ensures that transmitted data in an email meets the requirements of all the regulatory and governing bodies involved.
*Visibility: increases the level of security, effectiveness, and cost-efficiency while enabling cybersecurity planning, allocation of resources, and enforcement of company security policies.

Guardian Digital Prevents Cyberattacks & Data Breaches with Adaptive, Multi-Layered Protection
With an adaptive, multi-layered design, Guardian Digital EnGarde Cloud Email Security offers multiple layers of security that detect and block threats in real-time and build on each other to provide more effective protection. Engineered to defend against sophisticated attacks like targeted spear-phishing, ransomware, and emerging zero-day attacks, EnGarde protects your users and your business against today's most advanced threats. Drawing on a combination of features and characteristics designed to work harmoniously to offer the highest level of protection, EnGarde addresses common shortcomings of default and third-party email security to mitigate risk and defend against today's malicious threats.

About Guardian Digital
Guardian Digital, Inc. builds enterprise email solutions with an intense focus on security and unrivaled customer support, designed to ease information technology overhead for its customers. Since 1999, Guardian Digital has pioneered the open-source architecture security-as-a-service email protection model to block today's and tomorrow's sophisticated email threats. Guardian Digital continues to innovate the email security marketplace using technology unavailable from any other vendor. Its EnGarde Cloud Email Security leverages the benefits of open-source development, contemporary cloud technologies, and decades of combined experience protecting enterprises. Guardian Digital is dedicated to its customers, and their safety is the foundation of the protection the company offers and builds on.

Guardian Digital is a registered trademark or tradename of Guardian Digital, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.

Justice Levine
Guardian Digital, Inc
+1 866-435-4689
jlevine@guardiandigital.com
Visit us on social media:
Facebook
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/604060156