CTPAT Bulletin – Cybersecurity: Threat of Phishing

September 21, 2023

Companies (both large and small) face increasing threats from cyber criminals. One of the most difficult threats to defend against is an attack through a phishing scheme. Phishing is a type of social engineering, which uses psychology to trick people into providing sensitive information to cyber criminals. Phishing scams usually involve fraudulent emails that appear to be from a legitimate source. According to the Cybersecurity and Infrastructure Security Agency (CISA), more than 90% of all cyber-attacks begin with phishing attempts. No matter how sophisticated your cyber security is, you are still vulnerable to just one person falling victim to phishing.

Phishing emails are crafted to instill a sense of urgency, requesting an immediate response. The emails are designed to look legitimate, as if coming from a trusted source such as a bank, credit card, a colleague, government agency, or service provider. The emails play upon people's desire to be helpful, sense of fear to avoid something bad happening, or in some cases eagerness to receive a reward from a "free giveaway."

Phishing schemes are becoming more sophisticated. Previous phishing attempts were easier to identify since they were often sent from unknown senders, contained misspelled words, and used poor grammar. Now, phishing scammers have learned to make emails look more legitimate by spoofing real sites. Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. To identify more savvy phishing attempts, look for generic and more formal greetings, urgent action requests, and requests for personal information.

Defending Against Phishing Scams

Training:

- The best defense against phishing is training! Implement frequent refresher training stressing the consequences of falling for a phishing scheme and how damaging it can be.
- Provide current examples of the most recent types of phishing schemes.
- Training should emphasize that employees should never click on links in suspicious emails or otherwise respond to information in these types of emails.
- If unsure of the legitimacy of the email, double check by contacting the purported source of the information another way. Call your colleague or look up the company or agency contact information via a search engine.
- Make sure training is required company wide, including all senior personnel. The Sony Pictures hack in 2014 was the result of targeting the top executives via phishing emails.

Reporting Phishing Attempts

- Make sure employees know how to report phishing attempts and stress the importance of reporting any suspicious email. According to CISA, when tested, only 13% of targeted employees reported a phishing attempt.
- Create a companywide campaign to advertise how to report an attempted cyber-attack – if in doubt, report all suspicious emails!

Simulated Exercises:

- Test employees using simulated exercises based on real examples of phishing attacks.
- For those employees that fail the test, ensure refresher training is mandated.

Publication Number: 3328-0823