Issued 12/18/18

Why Email Phishing Persists

One reason why bad actors use spoofing to steal sensitive information is they can. Despite all we know about practicing good cyber hygiene, spoofing works. One of the most popular forms of spoofing is phishing, which the U.S. Computer Emergency Readiness Team defines as “an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques.” Although phishers are using social media, instant messages, text messages and voice calls, they most commonly rely on email. That’s because of inherent flaws in how email was designed, Neil Wynne, principal and analyst for secure business enablement at Gartner, told GCN. Specifically, Simple Mail Transfer Protocol, the standard for sending and relaying email, is more than 30 years old and was not designed to authenticate senders or verify the integrity of received messages, he said via email. To demonstrate how easily phishing works, Al Bailey, a special agent at the Environmental Protection Agency’s Office of the Inspector General’s Office of Investigations, walked through a scam that affected EPA. To steal office supplies to resell for a profit, attackers in a foreign country compiled a list of about 1,700 EPA employee email addresses and sent a mass message out pretending to be part of the agency’s online security team. “The email told these employees that the EPA was undergoing a system upgrade and that they had to reset their remote log-in credentials or else their email accounts would be frozen,” Bailey said in a 2017 podcast. “And of course, the email included a link that took these employees to a page that was supposedly the EPA’s remote log-in page.” The employees entered their usernames and passwords into the fake page, and the attackers used those real credentials to

buy thousands of dollars' worth of office supplies. For years, government agencies have been issuing reports -- intended for workers and the public at large, too -- describing what to look out for in phishing attacks. For instance, a 2013 document from the Securities and Exchange Commission warns that phishing emails may look like they come from legitimate sources, even copying a company or agency logo; the "from" line could contain the names of real people who work at the company; and URLs might look authentic. Additionally, phishing messages often include a sense of urgency or a threatened consequence if the recipient doesn't act quickly. A Federal Trade Commission article encourages people to be careful about opening attachments or clicking on links in emails, to look up websites and phone numbers through a web search rather than trusting those provided in the message and to call agencies directly to find out if the email is legit. But phishing shows no sign of slowing down. In the second quarter of this year, phishing attacks worldwide totaled 233,040, compared with 180,577 in the fourth quarter of 2017, according to a report by the Anti-Phishing Working Group, an international coalition working to standardize the response to cybercrime.