Issued 11/19/18

Phishing Works!

Phishing works more frequently on those who understand what social engineering is then on those who live in blissful ignorance, or so a study of students at University of Maryland, Baltimore County suggests. Citing IBM data suggesting human error is a factor in 95 per cent of security incidents, researchers from the school's department of computer science and electrical engineering conducted a phishing test to assess the relationship between demographic factors and susceptibility to phishing. UMBC's boffins – Alejandra Diaz, Alan Sherman, and Anupam Joshi – conducted three types of phishing attacks earlier this year on separate groups of 450 students, covering a total of 1,350 individuals. Of these, 1,246 (92 per cent) opened a phishing email for least one of the experiments. About 59 per cent of these students clicked on a phishing link. And among the subset of students who responded to the post-attack survey (482), 70 per cent had clicked on a phishing link. As a point of comparison, when Michigan's Department of Information Technology conducted a security audit last year [link], it found among 5,000 randomly selected employees that 32 per cent opened the phishing message, 25 per cent clicked on the link in the message, and 19 per cent submitted their credentials through the phishing website loaded by the link. The first of these phishing messages was designed to look like a PayPal bill from a third-party merchant. The email attempted to trick the user into clicking on a link purporting to provide details for a supposedly placed order. The second presented itself as a message about Quadmania, a UMBC weekend festival. It said the recipient had

won a $100 Amazon prize and asked the recipient to click the provided link. The third claimed to be a message from the school's Division of Information Technology. It asked the user to verify his or her UMBC account credentials within 48 hours and made reference to the Quadmania phishing message to sound more credible. Overconfidence among the technically inclined has been detected elsewhere. At the Node Summit earlier this year, Guy Podjarny, CEO and cofounder of security biz Snyk, recounted an internal Salesforce phishing test that found developers were the second most likely employee group, after marketers, to fall for phishing tricks [link]. According to the Anti-Phishing Working Group (APWG), there were 233,040 phishing sites detected in Q2 2018, down from 263,538 in Q1 2018. The number of phishing reports submitted to the APWG was 264,483, about the same as the 262,704 reported in 1Q 2018.