Issued 3/7/18

Most Top US Higher Ed Institutions Fail to Protect Students from Phishing

88.8% of the root domains operated by top colleges and universities in the U.S. are putting their students, staff and other recipients at risk for phishing attacks that spoof the institution's domain, according to 250ok (https://250ok.com). Phishing and spoofing attacks against consumers are likely when companies do not have a published Sender Policy Framework (SPF) or Domain-based Message Authentication, Reporting and Conformance (DMARC) policy in place. SPF is an email validation system that detects spoofing attempts, or a third party disguising itself as a particular sender using a counterfeit email address. DMARC is considered the industry standard for email validation to prevent such attacks. The report, which analyzed 3,614 domains operated by the top accredited US colleges and universities by student enrollment, reveals the domains controlled by these institutions indexed lower in their adoption of a DMARC policy (11.2%) when compared to top US and EU retailers (15.8%). A 2017 study from the Anti-Phishing Working Group reported phishing attacks targeted an average of 443 brands per month in the first half of 2017, up from 413 per month during the same period in the previous year. These attacks are a threat to brand trust, as 91% of all cyber-attacks begin with a phishing email.