HOME CYBER DEFENSE
ARE YOU SAFE FROM CYBER CRIME?
ALERT

Issued 6/7/17

Humans, Not Computers, are the Biggest Problem in Cybersecurity

Criminals are now relying more on manipulating human behavior to inflict cyberattacks, rather than actually hacking into software, according to research results released Tuesday. Cybersecurity firm Proofpoint's research has shown business email compromise (BEC) attacks, where company employees are tricked into making fraudulent payments to the attackers, has spiked from 1% of malware emails in 2015 to 42% by the end of 2016. Proofpoint Australia managing director Tim Bentley said that even though the phenomenon is relatively new, criminals have already evolved the technique to get around corporate defenses. "For example, we have found locally that the BEC approach is transitioning from an actor purporting to be a CEO or CFO and requesting a wire transfer to an actor purporting to be a businesses' existing supplier and requesting a wire transfer for an invoice payment," he told Business Insider. "It can take several months before the business even realizes it has been wiring money to a fraudulent account."

Social media fraud is also an attack method that's gaining traction, having increased 150% last year. These involve criminals imitating social media accounts of well-known brands and picking on consumers that start interacting with it. Email cyberattacks are continuing to be popular with attackers, the research found, because they garner instant responses. In fact, 25% of clicks on malicious links happen within 10 minutes of the email being sent, with 50% clicking within the hour. And nearly 90% of the clicks occur within the first 24 hours. Proofpoint stated that Thursdays are the worst days for email attacks, with 38% more malware messages sent on that day than any other weekday. Perhaps not surprisingly, business hours is when clicks on malicious links peak, with the median time-to-click getting under an hour when people are at work.