proofpoint

April 22, 2015

New Proofpoint Research: How Attackers Exploit People to Circumvent Cyber-Security

Second Annual Human Factor Report Details Cybercriminals' Shifting Social Engineering Tactics to Focus on Corporate Targets

SUNNYVALE, Calif., April 22, 2015 (GLOBE NEWSWIRE) -- Proofpoint, Inc., (Nasdaq:PFPT), a leading next-generation security and compliance company, today released the results of its annual study that details the ways attackers exploit end-users' psychology to circumvent IT security. The Human Factor Report 2015 reveals that last year was the year attackers "went corporate" by changing their tactics to focus on businesses rather than consumers, exploiting middle management overload of information sharing, and trading off attack volume for sophistication. The Proofpoint findings reiterate how human behavior, not simply system or software vulnerabilities, has significant implications on enterprise security—and what defenses are necessary in a world where everyone clicks.

As noted by Nick Hayes, Christopher McClean and Claire O'Malley, in the December 17, 2014 Forrester Research report *Reinvent Security Awareness To Engage The Human Firewall (access requires subscription)*, "The human element is one of the most critical aspects of your security program, yet it's often the most neglected…However, this is the problem…Security technologies that are critical to protecting your environment are often rendered useless due to easily avoidable human factors." Yet many organizations still rely solely on legacy gateway-only technologies for protection, rather than utilizing a layered defense strategy of blocking technologies, targeted attack protection and detection technologies, and threat response technologies, focused on people rather than infrastructure.

Key findings from The Human Factor Report 2015 include:

- **Every organization clicks.** On average, users click one of every 25 malicious messages delivered. No organization observed was able to eliminate clicking on malicious links.
- **Middle management is a bigger target.** Representing a marked change from 2013 when managers were less frequently targeted by malicious emails, in 2014 managers effectively doubled their click rates compared to the previous year. Additionally, managers and staff clicked on links in malicious messages two times more frequently than executives.
- **Sales, Finance and Procurement are the worst offenders.** Sales, Finance and Procurement (Supply Chain) were the worst offenders when it came to clicking links in malicious messages, clicking on links in malicious messages 50-80 percent more frequently than the average departmental click rate.
- **Clicks happen fast**. Organizations no longer have weeks or even days to find and stop malicious emails because attackers are luring two-out-of-three end users into clicking on the first day, and by the end of the first week, 96 percent of all clicks have occurred. In 2013, only 39 percent of emails were clicked in the first 24 hours; however, in 2014 that number increased to 66 percent.
- **Attacks are occurring mostly during business hours.** The majority of malicious messages are delivered during business hours, peaking on Tuesday and Thursday mornings. Tuesday is the most active day for clicking, with 17 percent more clicks than the other weekdays.
- **Users learn, but attackers adapt faster than users can learn.** The use of social media invitation lures, which were the most popular and effective email lures in 2013, decreased 94 percent in 2014. Email lures that employ attachments rather than URLs, such as message notification and corporate financial alerts, increased significantly as a vector. During select days in 2014, Proofpoint saw a 1,000 percent increase in messages with malicious attachments over the normal volume. The most popular email lures in 2014 included: e-fax and voicemails notifications, and corporate and personal financial alerts.

"The Human Factor research validates the critical value of threat information—and provides insight into how, when and where attacks are taking place," said Kevin Epstein, Proofpoint's vice president of Advanced Security & Governance. "The only effective defense is a layered defense, a defense that acknowledges and plans for the fact that some threats will penetrate the perimeter. Someone always clicks, which means that threats will reach users. Proofpoint's approach is effective because our systems can determine who those users are, where they are, and what's happening in real time—and actively protect organizations with real-time automated threat response."

Proofpoint's Human Factor Report is based on data gathered from its suite of advanced threat protection products that are live within customer environments. To receive a copy of Proofpoint's Human Factor Report, please visit www.proofpoint.com/humanfactor.

About Proofpoint, Inc.

Proofpoint Inc. (Nasdaq:PFPT) is a leading next-generation security and compliance company that provides cloud-based solutions for comprehensive threat protection, incident response, secure communications, social media security, compliance, archiving and governance. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system. Proofpoint protects against phishing, malware and spam, while safeguarding privacy, encrypting sensitive information, and archiving and governing messages and critical enterprise information. More information is available at www.proofpoint.com.

CONTACT: MEDIA CONTACT:

Patricia Hogan

Proofpoint, Inc.

408-763-3863

phogan@proofpoint.com

Source: Proofpoint, Inc.