Phishing emails: Here's why we are still getting caught out after all these years

Google explains why phishing scams are still depressingly effective.

By Steve Ranger | August 9, 2019 -- 13:58 GMT (06:58 PDT) | Topic: Security

September's Patch Tuesday was as bulky as all the Patch Tuesday releases have been in recent months.

Phishing emails (https://www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more/) were the first stage of some of the biggest hacks and data leaks of the last few years and groups behind such attacks are continuing to evolve new strategies.

In a talk at the Black Hat 2019 security conference, Google security researcher Elie Bursztein and University of Florida professor Daniela Oliveira detailed why these social engineering attacks remain effective, even though they have been around for decades.

Gmail blocks more than 100 million phishing emails every day, and Google said 68% of the phishing emails blocked by Gmail (https://security.googleblog.com/2019/08/understanding-why-phishing-attacks-are.html) each day are new variations.

It said many of the campaigns targeting Gmail end-users and enterprise customers only target a few dozen individuals. Enterprise users are nearly five times more likely to be targeted than standard Gmail users, while education users are twice as likely to be targeted than consumer users. Government users are three times more likely to be targeted, and non-profits are 3.8 times more likely to be hit with phishing than the average user.

While bulk phishing campaigns only last for 13 hours, more focused attacks are even more short lived; what Google terms as a 'boutique campaign' -- something aimed at just a few individuals in a company -- lasts just seven minutes. In half of all phishing campaigns, the email pretends to have come from the email provider, in a quarter it claims to be from a cloud services provider; after that it's most likely masquerading as a message from a financial services company or ecommerce site.

 The fraudsters and hackers are also up against pretty poor opposition: Google found that 45% of internet users don't understand what phishing is or the risk associated with it.

SEE: A winning strategy for cybersecurity (http://www.zdnet.com/topic/a-winning-strategy-for-cybersecurity/?ftag=CMG-01-10aaa1b) **(ZDNet special report) |** Download the report as a PDF

As phishing gangs are adept at using psychological tricks (like urgency and the fear of missing out) to trick people into clicking, users' failure to realise there is a threat associated with such emails is a significant problem. "This lack of awareness increases the risk of being phished and potentially hinders the adoption of two-step verification," Google warned.

MORE ON CYBERSECURITY

- **Trojan malware: The hidden cyber threat to your PC** (https://www.zdnet.com/article/trojan-malware-the-hidden-cyber-threat-to-your-pc/)

- **This malware will steal your Twitter and Facebook accounts** (https://www.cnet.com/news/this-malware-will-steal-your-twitter-and-facebook-accounts/?ftag=CMG-01-10aaa1b) **CNET**

- **Hackers are testing out this updated banking malware with added stealthy attacks** (https://www.zdnet.com/article/hackers-are-testing-out-this-updated-banking-malware-with-added-stealthy-attacks/)

- **Trojan malware is back and it's the biggest hacking threat to your business** (https://www.techrepublic.com/article/trojan-malware-is-back-and-its-the-biggest-hacking-threat-to-your-business/?ftag=CMG-01-10aaa1b) **TechRepublic**

- **How cybercriminals are still snaring victims using seven-year-old malware** (https://www.zdnet.com/article/how-cyber-criminals-are-still-snaring-victims-using-seven-year-old-malware/)

RELATED TOPICS: SECURITY TV   DATA MANAGEMENT   CXO   DATA CENTERS

SHOW COMMENTS

--- MORE RESOURCES ---

Dawn of the Terrorbit Era NETSCOUT Threat Landscape Report Powered by ATLAS Presented by ASERT

Research from NETSCOUT