Why employees fall for scams and what companies can do about it

3 November 2020

Credit: CC0 Public Domain

Preventive countermeasures to phishing emails may actually increase the likelihood of employees falling for such scams, a new academic study reveals.

Protective controls, such as email proxy, anti-malware and anti-phishing technologies, can give employees a false sense of security, causing them to drop their vigilance because they incorrectly assume such measures intercept all phishing emails before they reach their inbox, a study co-organized by the University of Sussex Business School reveals.

Employees' sense of shame and fear of work colleagues' disapproval were more effective deterrents from accessing phishing scams, the academics determined.

To protect themselves from costly phishing scams, companies should put all staff through continuous security training and educational programs, experts at the University of Sussex Business School and the University of Auckland recommend.

Phishing scams are responsible for almost one in three data breaches and the cost of ransomware to businesses is estimated at over $8 billion globally.

Dr. Mona Rashidirad, lecturer in strategy and marketing at the University of Sussex Business School, said: "Security safeguards alone will not protect a company from phishing scams. Organizations and individuals substantially invest in security safeguards to protect the integrity, availability, and confidentiality of information assets. However, our study supports the findings of recent studies that these safeguards are not adequate to provide the ultimate protection of sensitive and confidential information.

"Protective and detective tools use machine learning, anomaly detection, text mining and profile matching to combat the threat of phishing emails but cyber criminals design these scams to bypass technological controls and exploit human cognitive biases.

"Technical countermeasures such as anti-phishing and spamming tools, email malware detection and data loss prevention still often require human intervention to analyze and distinguish between phishing and legitimate emails.

"To prevent phishing attacks, a well-designed continuous security training and educational program, incorporating phishing simulation exercises and embedded training for vulnerable employees, needs to be established and enforced in organizations."

Following a survey of employees, the researchers developed a theoretical model of factors that influence users in the clicking of phishing emails from a socio-technical perspective exploring employees' responses to or avoidance of the threat posed by the scam.

Applying theory of planned behavior (TPB), the

research team hypothesized that an employee's intention toward clicking on phishing emails is influenced most strongly by how their response would be perceived by managers and colleagues, the employee's self-assessment on how they can cope with the threat and their personal attitude toward compliance.

The researchers identified a range of individual, organizational and technological factors that could explain employees' failure to follow compliance with email security policy and liability to fall for phishing attacks.

This vulnerability to phishing scams did not vary significantly when considering an employee's age, gender or education, the study reveals.

Employees' clicking on phishing emails was often an irrational act triggered by habit and automatic behavior tendencies developed through a history of using email on a daily basis, the study said.

The authors determined that informing staff about procedural countermeasures, including information security standards, policies and guidelines, does increase security awareness among employees but is not sufficient by itself to invoke behavioral change in employees dealing with phishing emails.

Effective staff training should inform employees what security measures their employer already has in place but also what security risks remain that could be exploited by malicious attackers, the academics conclude.

Hamidreza Shahbaznezhad, senior data scientist in industry at the University of Auckland, said: "Although technical countermeasures such as anti-phishing and spamming tools, email malware detection and data loss prevention are deployed to mitigate the risk of phishing attacks, using these technologies to detect phishing attacks remains a challenging problem. This is not least because they often require human intervention to analyze and distinguish between phishing and legitimate emails."

Farzan Kolini, Ph.D. candidate at University of Auckland, said: "Preventive countermeasures such as anti-phishing tools and email proxy have a pivotal role in detecting phishing email, as phishing attacks have become more sophisticated to bypass privative security countermeasures. Hence, it is incumbent on employees to apply additional due-diligence to investigate any suspicious emails."

More information: Hamidreza Shahbaznezhad et al. Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter?, *Journal of Computer Information Systems* (2020). DOI: 10.1080/08874417.2020.1812134

Provided by University of Sussex

APA citation: Why employees fall for scams and what companies can do about it (2020, November 3) retrieved 17 October 2021 from https://techxplore.com/news/2020-11-employees-fall-scams-companies.html