Phishing success linked to incentives and sticking to an effective strategy

February 21 2018

Credit: CC0 Public Domain

Not all phishing campaigns work, but when an attacker perseveres with a strategy that does it is the key to their success. That's the finding of a new study focusing on the attacker, a largely ignored but crucial aspect

of phishing. In addition to identifying successful strategies, it also reveals that attackers are motivated by quicker and larger rewards—with creative individuals putting more effort into constructing these malicious emails. Insights from the study, published today in open-access journal *Frontiers in Psychology*, can be used to develop tools and training procedures to detect phishing emails.

"We find specific phishing strategies, such as the use of authoritative tone, expressing shared interest and sending notifications, are more likely to succeed," says Dr. Prashanth Rajivan, lead author of the study and based at Carnegie Mellon University, Pennsylvania, USA.

Phishing is a common form of cyber-attack. Criminals impersonate a trustworthy third party to persuade people to visit fraudulent web sites or download malicious attachments, with the intent of compromising their security. While research has largely focused on the victims of these crimes, this new study looks at a critical aspect of phishing: the attacker's behavior and strategies.

"We created a game-like experiment to assess how well different strategies work, and to understand how incentives and success rates, or an individual's creativity, can affect motivation," explains Dr. Rajivan.

In the experiment, human participants play the role of a phishing attacker and accumulate points, over a number turns, for successfully deceiving other people who are the 'end-user' performing an email management task. The game was carefully constructed to train and reward people into producing phishing emails that employ different strategies and topics.

Strategies that were less likely to succeed included 'offering deals,' 'selling illegal materials' and 'using a positive tone.'

"People may be less receptive to strategies associated with scams that worked a decade ago," explains Dr. Rajivan. "More successful strategies today would be 'sending notifications,' 'use of authoritative tone,' 'taking advantage of trust by impersonating a friend or expressing shared interest,' and 'communicating failure'."

The repeated design of the game allowed the researchers to assess the attacker's tactics over time. This revealed that perseverance with a successful strategy, rather than switching from one to another, can yield better results. The researchers attribute this to the attackers improving the email text at each turn.

Incentives had a direct influence on motivation, with delayed rewards resulting in lesser effort. The easier and sooner high rewards were gained, the more effort an attacker applied to designing persuasive emails, as did individuals who scored high in a 'creativity' test. There was no evidence to suggest, however, that creativity could be used as a predictor of phishing success.

"There has been a resurgence in phishing attacks in recent years and the regular, non-expert users of the Internet are usually the victims of these crimes. We need to improve current security practices to change the incentive structure for the attacker. If the rewards are greater than the costs, attackers will continue to exert more effort into phishing campaigns," says Dr. Rajivan. "We think that attackers with higher creativity may be capable of changing and adapting emails to evade detection, even though their creativity cannot determine how much success they achieve in getting the end-user to respond."

He continues, "Our novel experimental design could be used to crowdsource people to play our game, which would give us lots of information on phishing success rates and how these emails can be adapted, thereby improving detection software. In addition, we could use

it as a training tool to help people think like hackers to better detect phishing emails."

More information: *Frontiers in Psychology* (2018). DOI: 10.3389/fpsyg.2018.00135 , www.frontiersin.org/articles/1 … psyg.2018.00135/full

Provided by Frontiers