Under cyber attack: UH researchers look at how to catch a 'phisher'

May 16 2017

As cybersecurity experts scramble to stop another wave of ransomware and malware scams that have infected computers around the world, computer science experts at the University of Houston are "phishing" for reasons why these types of attacks are so successful. The research findings, presented last month at the ACM Asia Conference on Computer and Communications Security, are being used to develop the next generation of email filters to better identify and defend against this type of cyber attack.

Computer science professors Rakesh Verma, Arjun Mukherjee, Omprakash Gnawali and doctoral student Shahryar Baki used publicly available emails from Hillary Clinton and Sarah Palin as they looked at the characteristics of phishing emails and traits of the email users to determine what factors contribute to successful attacks. The team used natural language generation— a process used to replicate human language patterns—to create fake phishing emails from real emails. It's a tactic used by hackers to execute "masquerade attacks," where they pretend to be authorized users of a system by replicating the writing styles of the compromised account.

Using the Clinton and Palin emails, the research team created fake emails and planted certain signals, such as fake names, repetitive sentences and "incoherent flow". Study participants were then given eight Clinton emails and eight Palin emails—four were real, four were fake. Volunteers were asked to identify which emails were real and explain their reasoning. The study took into account the reading levels of the Clinton and Palin emails as well as the personality traits, confidence levels and demographics of the 34 volunteers who participated.

The results of the study showed that:

- Participants could not detect the real emails with any degree of confidence. They had a 52 percent overall accuracy rate.
- Using more complex grammar resulted in fooling 74 percent of participants.
- 17 percent of participants could not identify any of the signals that were inserted in the impersonated emails.
- Younger participants did better in detecting real emails.
- Only 50 percent of the participants mentioned the fake names.
- Only six participants could show the full header of an email.
- Education, experience with emails usage and gender did not make a difference in the ability to detect the deceptive emails.

"Our study offers ideas on how to improve IT training," Verma said. "You can also generate these emails and then subject the phishing detectors to those kind of emails as a way to improve the detectors' ability to identify new attacks."

In the case of the recent Google Docs attack, Verma says people fell for the scam because they trust Google. When users opened the given URL, they were sent to a permissions page and hackers got control of their emails, contacts and potentially their personal information. Google stopped the scam, removed the fake pages and disabled offending accounts. Verma said a real Google Docs application will generally not ask for permission to access your contacts or read your emails.

The "WannaCry" ransomware attack that has hit banks, hospitals and government agencies around the globe is also spread through email phishing and can be spread through the Google Doc-type "worm" as well.

What all email users need to know in order to protect themselves:

- Look closely at the sender of the email and the full header that has information about how the email was routed.
- Look at the body of the email for any fake, broken links that can be identified by hovering a mouse over them.
- Think about the context of the email and how long it has been since you have had contact with the sender.

"There will be copycat attacks in the future and we have to watch out for that," said Verma.

Provided by University of Houston

Citation: Under cyber attack: UH researchers look at how to catch a 'phisher' (2017, May 16) retrieved 24 July 2024 from https://phys.org/news/2017-05-cyber-uh-phisher.html