Tech companies not doing enough to protect users from phishing scams

July 30 2019

Credit: CC0 Public Domain

Technology companies could be doing much more to protect individuals and organisations from the threats posed by phishing, according to research by the University of Plymouth.

However, users also need to make themselves more aware of the dangers to ensure potential scammers do not obtain access to personal or sensitive information.

Academics from Plymouth's Centre for Security, Communications and Network (CSCAN) Research assessed the effectiveness of phishing filters employed by various email service providers.

They sent two sets of messages to victim accounts, using email content obtained from archives of reported phishing attacks, with the first as plain text with links removed and the second having links retained and pointing to their original destination.

They then examined which mailbox it reached within email accounts as well as whether they were explicitly labelled in any way to denote them as suspicious or malicious.

In the significant majority of cases (75% without links and 64% with links) the potential phishing messages made it into inboxes and were not in any way labelled to highlight them as spam or suspicious. Moreover, only 6% of messages were explicitly labelled as malicious.

Professor Steven Furnell, leader of CSCAN, worked on the study with MSc student Kieran Millet and Associate Professor of Cyber Security Dr. Maria Papadaki.

He said: "The poor performance of most providers implies they either do not employ filtering based on language content, or that it is inadequate to protect users. Given users' tendency to perform poorly at identifying malicious messages this is a worrying outcome. The results suggest an opportunity to improve phishing detection in general, but the technology as it stands cannot be relied upon to provide anything other than a small contribution in this context."

The number of phishing incidents has risen dramatically since they were first recorded in 2003. In fact, global software giant Kaspersky Lab reported that its anti-phishing system was triggered 482,465,211 times in 2018, almost double the number for 2017.

It is also a significant problem for businesses, with 80% telling the Cyber Security Breaches Survey 2019 that they have encountered 'Fraudulent emails or being directed to fraudulent websites' - placing this category well ahead of malware and ransomware.

Phishing is designed to trick victims into divulging sensitive information, such as identity and financial-related data, and the threat can actually take several forms:

- Bulk-phishing—where the approach is not specially targeted or tailored toward the recipient;
- Spear-phishing—where the message is targeted at specific individuals or companies and tailored accordingly;
- Clone-phishing—where the scammers take a legitimate email containing an attachment or link, and replace it with a malicious version;
- Whaling—in these cases the phishing is specifically targeted towards high value or senior individuals.

Professor Furnell, who has previously led various projects relating to user-facing security, added: "Phishing has now been a problem for over a decade and a half. Unfortunately, just like malware, it's proven to be the cyber security equivalent of an unwanted genie that we can't put back in the bottle. Despite many efforts to educate users and provide safeguards, people are still falling victim. Our study shows the technology can identify things that we would ideally want users to be able to spot for themselves—but while there is a net, it clearly has big holes."

More information: Steven Furnell et al, Fifteen years of phishing: can technology save us?, *Computer Fraud & Security* (2019). DOI: 10.1016/S1361-3723(19)30074-0

Provided by University of Plymouth