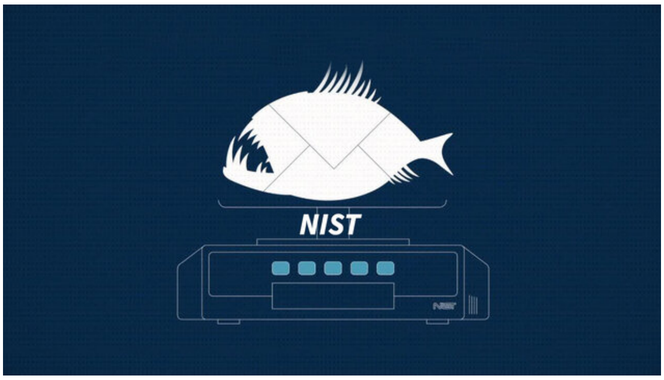
New tool helps IT staff see why users click on fraudulent emails

17 September 2020, by Alex Boss



A new tool called the Phish Scale can help organizations better train their employees to avoid phishing attacks. Credit: National Institute of Standards and Technology

Researchers at the National Institute of Standards and Technology (NIST) have developed a new tool called the Phish Scale that could help organizations better train their employees to avoid a particularly dangerous form of cyberattack known as phishing.

By 2021, global cybercrime damages will cost $6 trillion annually, up from $3 trillion in 2015, according to estimates from the 2020 Official Annual Cybercrime Report by Cybersecurity Ventures.

One of the more prevalent types of cybercrime is phishing, a practice where hackers send emails that appear to be from an acquaintance or trustworthy institution. A phishing email (or phish) can tempt users with a variety of scenarios, from the promise of free gift cards to urgent alerts from upper management. If users click on links in a phishing email, the links can take them to websites that could deposit dangerous malware into the organization's computers.

Many organizations have phishing training programs in which employees receive fake phishing emails generated by the employees' own organization to teach them to be vigilant and to recognize the characteristics of actual phishing emails. Chief information security officers (CISOs), who often oversee these phishing awareness programs, then look at the click rates, or how often users click on the emails, to determine if their phishing training is working. Higher click rates are generally seen as bad because it means users failed to notice the email was a phish, while low click rates are often seen as good.

However, numbers alone don't tell the whole story. "The Phish Scale is intended to help provide a deeper understanding of whether a particular phishing email is harder or easier for a particular target audience to detect," said NIST researcher Michelle Steves. The tool can help explain why click rates are high or low.

The Phish Scale uses a rating system that is based on the message content in a phishing email. This can consist of cues that should tip users off about the legitimacy of the email and the premise of the scenario for the target audience, meaning whichever tactics the email uses would be effective for that audience. These groups can vary widely, including universities, business institutions, hospitals and government agencies.

The new method uses five elements that are rated on a 5-point scale that relate to the scenario's premise. The overall score is then used by the phishing trainer to help analyze their data and rank the phishing exercise as low, medium or high difficulty.

The significance of the Phish Scale is to give CISOs a better understanding of their click-rate data instead of relying on the numbers alone. A low click rate for a particular phishing email can have several causes: The phishing training emails are too easy or do not provide relevant context to the user, or the phishing email is similar to a previous exercise. Data like this can create a false sense of security if click rates are analyzed on their own without understanding the phishing email's difficulty.

By using the Phish Scale to analyze click rates and collecting feedback from users on why they clicked on certain phishing emails, CISOs can better understand their phishing training programs, especially if they are optimized for the intended target audience.

The Phish Scale is the culmination of years of research, and the data used for it comes from an "operational" setting, very much the opposite of a laboratory experiment with controlled variables. "As soon as you put people into a laboratory setting, they know," said Steves. "They're outside of their regular context, their regular work setting, and their regular work responsibilities. That is artificial already. Our data did not come from there."

This type of operational data is both beneficial and in short supply in the research field. "We were very fortunate that we were able to publish that data and contribute to the literature in that way," said NIST researcher Kristen Greene.

As for next steps, Greene and Steves say they need even more data. All of the data used for the Phish Scale came from NIST. The next step is to expand the pool and acquire data from other organizations, including nongovernmental ones, and to make sure the Phish Scale performs as it should over time and in different operational settings. "We know that the phishing threat landscape continues to change," said Greene. "Does the Phish Scale hold up against all the new phishing attacks? How can we improve it with new data?" NIST researcher Shaneé Dawkins and her colleagues are now working to make those improvements and revisions.

In the meantime, the Phish Scale provides a new method for computer security professionals to better understand their organization's phishing click rates, and ultimately improve training so their users are better prepared against real phishing scenarios.

Information on the Phish Scale is published in a research article appearing in the current issue of the Journal of Cybersecurity. For additional background information about the development of the Phish Scale, see the team's body of research.

More information: Michelle Steves et al. Categorizing human phishing difficulty: a Phish Scale, *Journal of Cybersecurity* (2020). DOI: 10.1093/cybsec/tyaa009

Provided by National Institute of Standards and Technology

APA citation: New tool helps IT staff see why users click on fraudulent emails (2020, September 17) retrieved 28 November 2020 from https://techxplore.com/news/2020-09-tool-staff-users-click-fraudulent.html