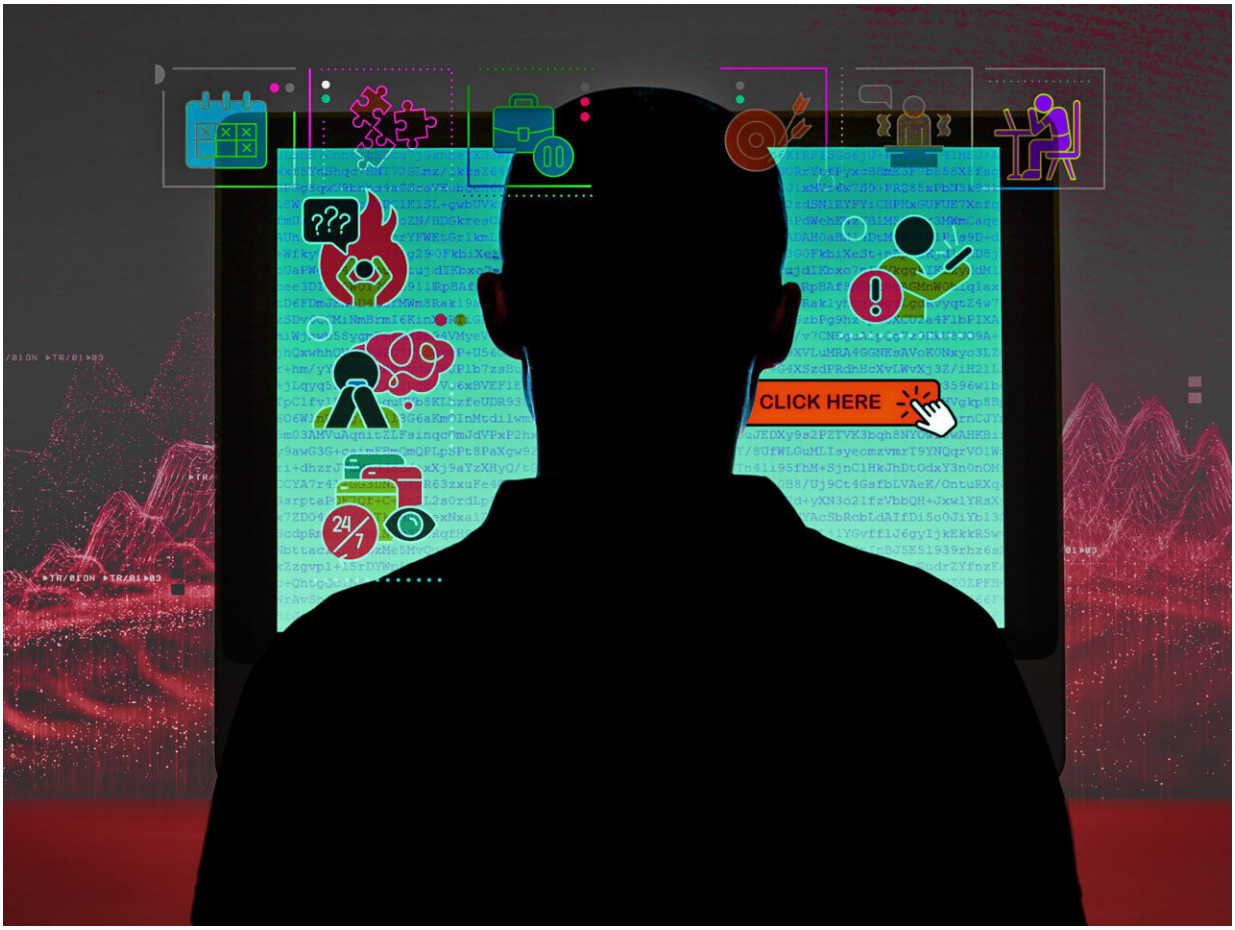
Stressed for a bit? Then don't click it, cybersecurity experts advise

July 5 2023



Workers who are feeling distressed are more likely to click on a phishing email, according to new human factors research at Pacific Northwest National Laboratory. Credit: Timothy Holland | Pacific Northwest National Laboratory

Workers feeling a specific form of stress are more likely than others to become the victims of a phishing attack, according to a study at the Department of Energy's Pacific Northwest National Laboratory.

While most—if not all—of us feel stress in the workplace, scientists identified a specific form of stress that indicates who is more vulnerable to clicking on bogus content that could lead to malware and other cyber ills. The work could help workers and their employers increase their cybersecurity defenses by recognizing the warning signs when someone is about to make a risky click.

The team's results from a study of 153 participants were published recently in the *Journal of Information Warfare*. The researchers noted that while the relatively small sample size limited their ability to tease out all of the relationships among more than two dozen variables they studied, the relationship between stress and response to the simulated phishing email was statistically significant.

The costs of phishing attacks are enormous. An analysis sponsored by Proofpoint and conducted by the Ponemon Institute estimates that large U.S. businesses lost, on average, $14.8 million apiece to fraudsters via phishing in 2021 alone.

Defenses include not just better technology but also improved awareness by would-be victims.

"The first step to defend ourselves is understanding the complex constellation of variables that make a person susceptible to phishing," says PNNL psychologist Corey Fallon, a corresponding author of the study. "We need to tease out those factors that make people more or less likely to click on a dubious message."

In their study, Fallon and colleagues found that people who reported a

high level of work-related distress were significantly more likely to follow a phony phishing email's link. Every one-point increase in self-reported distress increased the likelihood of responding to the simulated phishing email by 15 percent.

The scientists describe distress as a feeling of tension when someone on the job feels they're in a difficult situation and unable to tackle the task at hand. Distress might stem from feeling their workload is too high, or they might be questioning whether they have adequate training or time to accomplish their work.

Fancy phish to explore phishing psychology

The 153 participants had agreed to take part in a study, but they were unaware that the phishing email sent a few weeks later was part of the planned study into human factors research.

As far as phishes go, this was a fancy phish. There was no mention of a large sum of money from an African prince, for example, and there were no outright spelling mistakes or gross grammatical errors.

"These were well-crafted emails deliberately designed to trick people and tailored to the organization," said Jessica Baweja, a psychologist and an author of the study. "It was much harder to detect than the average phish."

Each participant received one of four different versions of a message about an alleged new dress code to be implemented at their organization. The team tested three common phishing tactics separately and together. Here's what they found:

- Urgency. 49 percent of recipients clicked on the links. Sample text: "This policy will go into effect 3 days from the receipt of

this notice...acknowledge the changes immediately."
- Threat. 47 percent clicked. "…comply with this change in dress code or you may be subject to disciplinary action."
- Authority. 38 percent clicked. "Per the Office of General Counsel…"
- The three tactics together: 31 percent clicked.

While the team had expected that more tactics used together would result in more people clicking on the message, that wasn't the case.

"It's possible that the more tactics that were used, the more obvious it was a phishing message," said author Dustin Arendt, a data scientist. "The tactics must be compelling, but there's a middle ground. If too many tactics are used, it may be obvious that you're being manipulated."

In day-to-day operations, PNNL tests its staff with fake phishing emails periodically. Typically around just 1 percent of recipients will click. Far more employees spot the phish early on and provide crowd-sourced alerting to the Laboratory's cybersecurity experts, said Joseph Higbee, PNNL's chief information security officer. When a real phishing email is detected, the Laboratory purges the system of all instances of the email immediately. The information is frequently shared with other DOE laboratories.

Human-machine teaming to reduce cybersecurity risk

How can companies and employees use this data to reduce the risk?

"One option is to help people recognize when they are feeling distressed," said Fallon, "so they can be extra aware and cautious when they're especially vulnerable."

In the future, one option might be human-machine teaming. If an

algorithm notes a change in a work pattern that might indicate fatigue or inattention, a smart machine assistant could suggest a break from email. Automated alerts are becoming more common, for instance, when a driver drifts unexpectedly and the car issues a warning about fatigue. The researchers noted that the potential benefits of input from a machine assistant would need to be weighed against employee privacy concerns.

"It can be hard to see email as a threat," said Baweja. "Our ancient brains aren't wired to equate email with scary things. You're working through emails all day and it's routine; there's little reason to think they could harm you or our organization.

"Organizations need to be thinking about how to encourage people to make good choices. People overestimate their ability to detect phishing emails," she added.

PNNL researchers are continuing the work, but with a twist. Instead of asking what makes people more vulnerable to phishing, they will conduct a small study of people who resisted the bait, to learn more about their traits and state of mind as they monitor their email.

The work is part of a broader program in human-machine teaming and human factors research at PNNL, which recently hosted a Symposium on Human Factors.

More information: Phishing in the Wild: An Ecologically Valid Study of the Phishing Tactics and Human Factors that Predict Susceptibility to a Phishing Attack, *Journal of Information Warfare* (2023). www.jinfowar.com/journal/volum … lity-phishing-attack

Provided by Pacific Northwest National Laboratory