Focusing on user habits key to preventing email phishing

November 11 2015, by Bert Gambini

The cumulative number of successful phishing cyberattacks has risen sharply over the last decade, and in 2014 that figure surged past the total U.S. population.

To date, about 400 million breaches have yielded hackers some kind of personal information, according to Arun Vishwanath, an associate professor in the Department of Communication at the University at Buffalo and an expert in cyber deception.

"That means everyone in the country may have been breached," says Vishwanath. "Everyone. Including me and you."

Spear phishing is the biggest threat to cyber security at every level, he says. These are the tightly targeted, malware-carrying attacks that send links or attachments in what often appear to be genuine-looking email messages. Users launch the malware - intrusive software that initiates device-compromising background programs - when they click the link or open the attachment.

Businesses in the public and private sectors teach people to recognize phishing, but those efforts often fail or don't work for very long because the training ignores users' habits and instead focuses exclusively on how users process information, says Vishwanath, whose latest research on email habits and phishing outcomes is published in the *Journal of Computer-Mediated Communication*.

"The findings point to a joint operation of habits and information processing, something that most social scientists have ignored," says Vishwanath. "We can't just focus on one aspect of that use, yet that's what we're doing and it explains why phishing is successful."

Information processing is about analyzing and reacting to an environment or situation. It's contextual, like trying to determine the contents of an unmarked bottle. Habits emerge from a different learning process and exist as a separate phenomenon from information processing, says Vishwanath.

Hackers ironically hit the same mark that the training designed to stop them misses. Phishing is successful because the perpetrators take advantage of people who are habitual in the way they respond.

And security levels don't play a role. Spear phishing is a people problem,

and it works 17-35 percent of the time - even after people have been trained.

But Vishwanath says his research suggests that the training, which teaches people to recognize suspicious emails, is based on the presumption that the phishing problem can be accounted for by information processing.

"The training and education designed to stop phishing is all about asking what's in the bottle," he says. "It's contextual.

"In actual practice, many activities are habitual, or a combination habit and information processing."

That people's routines are ignored in training accounts for why they so quickly resume those routines - sometimes, mere hours after being trained.

"None of our interventions deal with habits, he says. "Right now our training is analogous to teaching people how to drive by making them have an accident and telling them they've done so. It never explains why they've had an accident."

The issue is not a lack of awareness. Email systems, especially when accessed on mobile devices, are built to create and foster habits. They encourage users to repeatedly check for messages, establishing routines that Vishwanath says turns their devices into a casino game, with users opening emails like reckless gamblers habitually pulling the arms of slot machines without thinking of the long-term consequences.

"Routines are powerful and hard to stop," he says.

Even sophisticated email systems that flag suspicious messages don't

help because users become desensitized to the warnings and quickly resume their habits.

"Altering the types of warnings issued would reflect the role of routines and make the messages more salient, but we're not doing that."

Vishwanath says the key is about making the distinction between habits and information processing, and training users to break existing patterns and rhythms.

"This is cyber hygiene," he says. "It's improving the baseline."

Provided by University at Buffalo