Human Centred Cyber Security

Associate Professor Giovanni Russello and Senior Lecturer Danielle Lottridge, Computer Science, University of Auckland.

Phishing attacks are expected to cost the global economy US$20 billion in 2021 alone, and that number is only projected to go up. Within 10 years, global costs related to ransomware – often installed following successful phishing attacks – are projected to balloon to US$265 billion a year. We are hoping to change that.

Associate Professor Russello, the school head, is an expert in cybersecurity and online privacy, while Senior Lecturer Lottridge is an expert in human-computer interaction and user experience.

Until now, most work aimed at stopping phishing has focused on technological fixes or on what Russello calls “blame-the-user” approaches. The problem is, neither approach is doing enough.

Technological approaches have undeniably had an impact. Spam filters and similar tools stop about 90 percent of malicious emails. But that still leaves 10 percent. Given the sheer volume of phishing email (160 million of phishing emails per day!), most people are still confronting potentially dangerous emails on a daily or near-daily basis.

Current user-based interventions aren’t solving the problem either. Certainly, education can help people learn to recognise signs an email may be suspicious. However, 65 percent of companies that have been victims of phishing attacks had previously performed some form of training, says Russello.

The team wants to focus on something new: the individuals involved and the circumstances in which they receive phishing attacks.

Different email situations

It’s not hard to imagine situations when you might react differently to emails. On a good day, you might arrive at work well-rested and sip your coffee calmly as you read your several messages. Now imagine arriving frazzled on a Monday morning after an insomniac night and hairy commute only to find dozens, maybe hundreds of emails have piled up since your sick day on Friday. Oh, and you have a meeting shortly that may touch on the contents of some of those emails.

Currently, none of these factors make any difference to your email software, though you might be a lot more likely to hurriedly scan messages in the latter situation – and maybe click on a suspicious link.

The team envisions a system that would take a back seat in the relaxed scenario but “swoop in for extra support,” as Lottridge puts it, in the high-stress situation. The system they envision would also be personalised, because people might react to situations in different ways and need different kinds of support, whether it’s a reminder to slow down when they’re jumpy or auto-translation when they’re tired.

Though Russello and Lottridge have been examining this area for a few years, they consider themselves to be in the early stages of the project because it’s such a new area of research. Other researchers have examined aspects of users such as personality, culture and age, but these factors can’t be changed, while situations could be, says Lottridge.

Acknowledgements

Russello and Lottridge would like to acknowledge the rest of the team working on this project: Sijie Zhuo (PhD student), Associate Professor Yun Sing Koh, and Professor Robert Biddle from Computer Science, and Associate Professor Paul Corballis, Dr Jude Buckley (researcher) and Jacinda Murphy (PhD student).

Find out more: https://www.uniservices.co.nz/computer-scientists-investigating-new-ways-prevent-phishing