Breakthrough in cybersecurity is no phish story

March 29 2016, by Bert Gambini

Corporations, small businesses and public sector entities have tried unsuccessfully for years to educate consumers and employees on how to recognize phishing emails, those authentic-looking messages that encourage users to open a cloaked, though malicious, hyperlink or attachment that appears harmless.

In casual conversation, the problem sounds like a nuisance; on balance sheets, however, it's monstrous. The estimated financial tally from information loss, identity theft, service disruptions and additional security costs related to phishing exceeds $1 trillion. In fact, phishing accounts for more than one-third of the nearly 800 percent increase in cybercrimes since 2007, according to the Government Accountability Office.

The problem appears unstoppable, but a University at Buffalo cybersecurity expert may have finally hooked the phish that existing training methods have so far been unable to land.

Arun Vishwanath, an associate professor in the Department of Communication at UB, whose research specializes in how to stop online deception, has developed a groundbreaking comprehensive model that, he says, for the first time accounts for the multiple influences that contribute to the success of these attacks.

Vishwanath's model is a breakthrough in understanding why people fall for these schemes and could finally tilt phishing's dynamic from successful deception to effective detection.

The study, published in the latest issue of journal *Communication Research*, proposes and empirically tests a theory-based model that identifies specific user vulnerabilities that arise in a given user.

"When I talk to cybersecurity experts in companies or even in the U.S. government—and I've presented this to many of them—I'm told that the model provides a ready framework to understand why their employees fall prey to such attacks," says Vishwanath.

"This is so important."

The model encourages a new approach to training that is based on individual, predictive profiles of computer users, rather than relying on the current blanket training approach for everyone, a method that previous research has shown to be of limited effectiveness because people are often victimized hours after they've finished their training, according to Vishwanath.

"Using this model, organizations can come up with a dynamic security policy, one that takes into account employee cyber-behaviors and allows access to systems, software and devices based on these behaviors," he says. "It can also be used to develop a risk-index that assesses the overall risk threshold of individuals and groups."

Vishwanath's study, which is part of a larger research program to understand the people-problems of cybersecurity, tested the model by actually simulating different types of phishing attacks on real-world subjects.

"Calling people into a lab doesn't work for this kind of research because there is a heightened sense of awareness," he says. "Subjects in labs look at a screen and are asked if they believe they're looking at a phishing email. In reality, most people don't focus on emails and appear to be far less suspicious and far more susceptible than when they are in a lab.

"Methodologically, the premise I work with is that we have to play the role of the 'bad guys' in order to study how and why people are victimized."

The Suspicion, Cognition and Automaticity Model (SCAM) explains what contributes to the origin of suspicion by accounting for a user's email habits and two ways of processing information: heuristics, or thumb rules that lead to snap judgments about a message's content; and a deeper, systematic processing about an email's content.

"A fourth measure, cyber-risk beliefs, taps into the individual's perception about risks associated with online behaviors," he says.

Vishwanath's model accounts for these layers and the relationships among them with each measure providing a brush stroke that composes an overall portrait of the different reasons people fall victim to such attacks.

"These things matter," he says. "Once we understand why certain people fall for attacks we can target them with the appropriate training and education."

Current training is based on simply teaching people how to recognize a phish that only addresses one of the reasons why people fall for phishing. No wonder training has had limited overall effectiveness in stopping cyber breaches.

The point for Vishwanath is that most anti-phishing measures are trying to stop attacks under the assumption that they know why people fall prey to such attacks, rather than actually figuring out why the attacks are working.

With phishing losses mounting at alarming rates and the level of phishing sophistication evolving in step, Vishwanath says adopting the model is critical.

Millions of phishing attacks occur daily, many following recurring patterns, such as the emails that come now during tax seasons. These, too, have grown in rate and intensity. For instance, the number of malware-laden IRS phishing emails this month has already gone up by 400 percent.

The malware in these emails open back doors to computer networks that provide hackers with access to people's personal information. Some intrusions install key loggers that track what the person in typing or the sites they visit. And a new class of "ransomware" encrypts every file on a hard driver or server, holding the data hostage until users pay an untraceable ransom in bitcoin.

"If the Internet were the real world it would be the most dangerous city on earth," he says.

Provided by University at Buffalo

Citation: Breakthrough in cybersecurity is no phish story (2016, March 29) retrieved 4 May 2024 from https://techxplore.com/news/2016-03-breakthrough-cybersecurity-phish-story.html