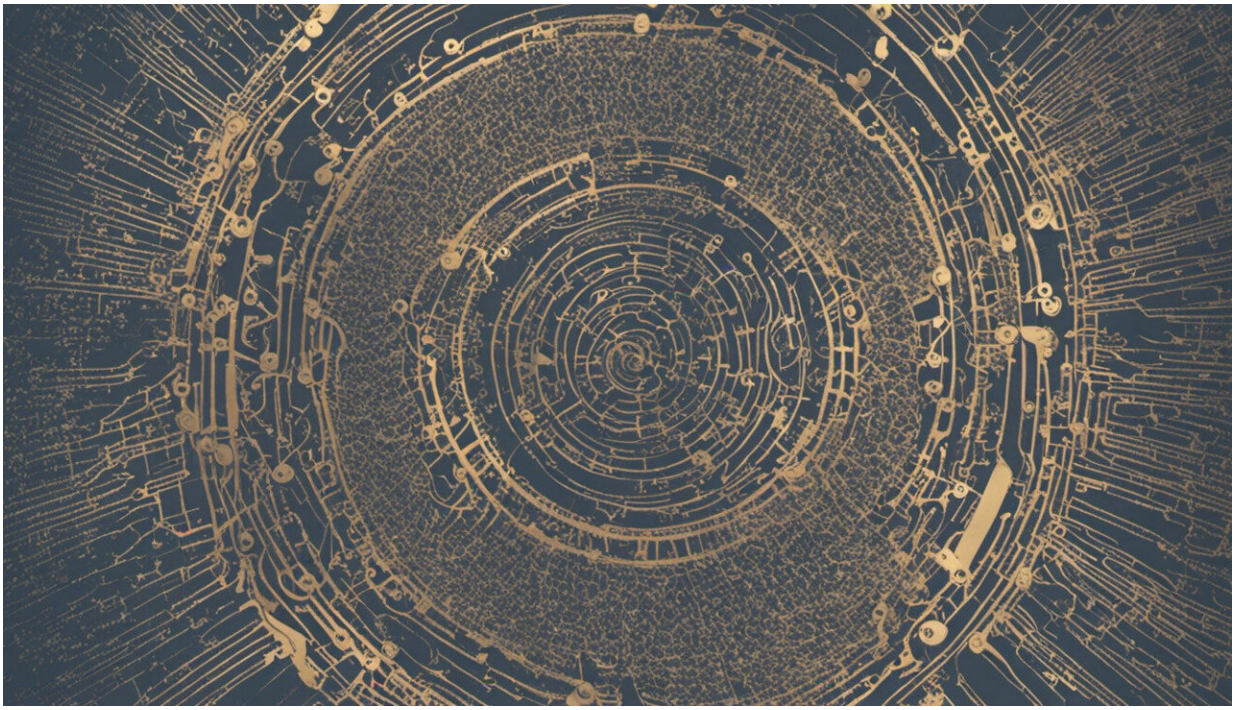
# Cybersecurity's weakest link is humans

May 5 2016, by Arun Vishwanath, The State University Of New York



Credit: AI-generated image (disclaimer)

There is a common thread that connects the hack into the sluicegate controllers of the Bowman Avenue dam in Rye, New York; the breach that compromised 20 million federal employee records at the Office of Personnel Management; and the recent spate of "ransomware" attacks that in three months this year have already cost us over US$200 million: they were all due to successful "spearphishing" attacks.

Generic – or what is now considered "old school" – phishing attacks typically took the form of the infamous "Nigerian prince" type emails, trying to trick recipients into responding with some personal financial information. "Spearphishing" attacks are similar but far more vicious. They seek to persuade victims to click on a hyperlink or an attachment that usually deploys software (called "malware") allowing attackers access to the user's computer or even to an entire corporate network. Sometimes attacks like this also come through text messages, social media messages or infected thumb drives.

The sobering reality is there isn't much we can do to stop these types of attacks. This is partly because spearphishing involves a practice called social engineering, in which attacks are highly personalized, making it particularly hard for victims to detect the deception. Existing technical defenses, like antivirus software and network security monitoring, are designed to protect against attacks from outside the computer or network. Once attackers gain entry through spearphishing, they assume the role of trusted insiders, legitimate users against whom protective software is useless.

This makes all of us Internet users the sole guardians of our computers and organizational networks – and the weakest links in cyberspace security.

## The real target is humans

Stopping spearphishing requires us to build better defenses around people. This, in turn, requires an understanding of why people fall victim to these sorts of attacks. My team's recent research into the psychology of people who use computers developed a way to understand exactly how spearphishing attacks take advantage of the weaknesses in people's online behaviors. It's called the Suspicion, Cognition, Automaticity Model (SCAM).

We built SCAM using simulated spearphishing attacks – conducted after securing permission from university research supervision groups who regulate experiments on human subjects to ensure nothing inappropriate is happening – on people who volunteered to participate in our tests.

We found two primary reasons people are victimized. One factor appears to be that people naturally seek what is called "cognitive efficiency" – maximal information for minimal brain effort. As a result, they take mental shortcuts that are triggered by logos, brand names or even simple phrases such as "Sent from my iPhone" that phishers often include in their messages. People see those triggers – such as their bank's logo – and assume a message is more likely to be legitimate. As a result, they don't properly scrutinize those elements of the phisher's request, such as the typos in the message, its intent, or the message's header information, that could help reveal the deception.

Compounding this problem are people's beliefs that online actions are inherently safe. Sensing (wrongly) that they are at low risk causes them to put relatively little effort into closely reviewing the message in the first place.

Our research shows that news coverage that has mostly focused on malware attacks on computers has caused many people to mistakenly believe that mobile operating systems are somehow more secure. Many others wrongly believe that Adobe's PDF is safer than a Microsoft Word document, thinking that their inability to edit a PDF translates to its inability to be infected with malware. Still others erroneously think Google's free Wi-Fi, which is available in some popular coffee shops, is inherently more secure than other free Wi-Fi services. Those kinds of misunderstandings make users more cavalier about opening certain file formats, and more careless while using certain devices or networks – all of which significantly enhances their risk of infection.

## Habits weaken security

Another often-ignored factor involves the habitual ways people use technology. Many individuals use email, social media and texting so often that they eventually do so largely without thinking. Ask people who drive the same route each day how many stop lights they saw or stopped at along the way and they often cannot recall. Likewise, when media use becomes routine, people become less and less conscious of which emails they opened and what links or attachments they clicked on, ultimately becoming barely aware at all. It can happen to anyone, even the director of the FBI.

When technology use becomes a habit rather than a conscious act, people are more likely to check and even respond to messages while walking, talking or, worse yet, driving. Just as this lack of mindfulness leads to accidents, it also leads to people opening phishing emails and clicking on malicious hyperlinks and attachments without thinking.

Currently, the only real way to prevent spearphishing is to train users, typically by simulating phishing attacks and going over the results afterward, highlighting attack elements a user missed. Some organizations punish employees who repeatedly fail these tests. This method, though, is akin to sending bad drivers out into a hazard-filled roadway, demanding they avoid every obstacle and ticketing them when they don't. It is much better to actually figure out where their skills are lacking and teach them how to drive properly.

## Identifying the problems

That is where our model comes in. It provides a framework for pinpointing why individuals fall victim to different types of cyberattacks. At its most basic level, the model lets companies measure

each employee's susceptibility to spearphishing attacks and identify individuals and workgroups who are most at risk.

When used in conjunction with simulated phishing attack tests, our model lets organizations identify how an employee is likely to fall prey to a cyberattack and determine how to reduce that person's specific risks. For example, if an individual doesn't focus on email and checks it while doing other things, he could be taught to change that habit and pay closer attention. If another person wrongly believed she was safe online, she could be taught otherwise. If other people were taking mental shortcuts triggered by logos, the company could help them work to change that behavior.

Finally, our method can help companies pinpoint the "super detectors" – people who consistently detect the deception in simulated attacks. We can identify the specific aspects of their thinking or behaviors that aid them in their detection and urge others to adopt those approaches. For instance, perhaps good detectors examine email messages' header information, which can reveal the sender's actual identity. Others earmark certain times of their day to respond to important emails, giving them more time to examine emails in detail. Identifying those and other security-enhancing habits can help develop best-practice guidelines for other employees.

Yes, people are the weakest links in cybersecurity. But they don't have to be. With smarter, individualized training, we could convert many of these weak links into strong detectors – and in doing so, significantly strengthen cybersecurity.

**More information:** A. Vishwanath et al. Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility, *Communication Research* (2016). DOI: 10.1177/0093650215627483

*This article was originally published on The Conversation. Read the original article.*

Source: The Conversation