# GONE PHISHIN'

A model developed by a UB researcher may help stem the tide of cyberattacks by exposing how and why people fall prey to phony emails.

## WHAT'S ON THE LINE

Whether through planting malware, capturing passwords or sabotaging systems, phishing emails—those deceptive messages with a link or attachment that's not what it seems—constitute a pernicious and pervasive cybersecurity threat. The nature of cybercrime makes its impact difficult to measure, but some have put the figure for financial theft, information loss, service disruptions and other costs at $1 trillion worldwide.

## TACKLING THE ISSUE

Though their consequences are widespread, successful phishing attacks are carried out one by one on individual users, whether in the home or in the workplace. Consequently, a common line of defense has been alerting people to the warning signs of deceptive emails. And yet, this approach has not been particularly effective, as even well-trained users frequently take the bait.

## REELING THEM IN

Groundbreaking research led Arun Vishwanath (PhD '01), an associate professor in the Department of Communication, to develop the Suspicion, Cognition and Automaticity Model, or SCAM, which analyzes a set of risky behaviors and beliefs previously overlooked by cybersecurity experts.

## THREE BIG CATCHES

What are people doing that allow breaches to occur, despite preventive training? The study uncovered several interrelated factors.

### 1 COMPLACENCY

An underlying belief that email is generally safe—even among those who know on a rational level that real threats exist—leads people to overlook red flags within messages.

### ACTING WITHOUT THINKING 2

People whose minds are on autopilot while browsing their inboxes have lower levels of suspicion—and higher levels of susceptibility.

### 3 ROTE EMAILING

The habitual use of email, in the form of regular, almost chronic checking, makes people less likely to proceed with caution and, again, to overlook red flags.

## BOTTOM LINE

Teaching people the warning signs of deceptive emails may be a positive first step, but it's not enough. Vishwanath stresses the need for a more individualized, multilayered approach to cybersecurity training, one that accounts for the complex cognitive and perceptual processes that put users at risk. This model, the first of its kind, can change the way people, businesses and other entities protect themselves against phishing attacks.

**ABOUT THE STUDY:** "Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility," which appeared in the journal Communication Research, was authored by Vishwanath with Brynne Harrison, a doctoral student at UB, and Yu Jie Ng (MA '14, BA '12), a doctoral student at Nanyang Technological University in Singapore. It is part of Vishwanath's continuing research into safeguarding individuals and organizations against cyberattacks by focusing on what he calls the weakest link in cybersecurity: internet users.