We believe we're less likely than others are to fall for online scams

May 6 2020

Credit: CC0 Public Domain

We believe we are less likely than others are to fall for phishing scams, thereby underestimating our own exposure to risk, a new cybersecurity study has found. The research also reports that this occurs, in part, because we overlook data, or "base rate information," that could help us

recognize risk when assessing our own behavior yet use it to predict that of others.

Together, the results suggest that those who are not informed of the risk that, for instance, work-from-home situations pose to online security may be more likely to jeopardize the safety of themselves and those they work for.

COVID-19 has had a devastating impact on the physical and mental health of people around the globe. Now, with so many more working online during the pandemic, the virus threatens to wreak havoc on the world's "cyber health," the researchers note.

"This study shows people 'self-enhance' when assessing risk, believing they are less likely than others to engage in actions that pose a threat to their cyber security—a perception that, in fact, may make us more susceptible to online attacks because it creates a false sense of security," says Emily Balcetis, an associate professor in New York University's Department of Psychology, who authored the study, which appears in the journal *Comprehensive Results in Social Psychology*.

"This effect is partially explained by differences in how we use base rate information, or actual data on how many people are actually victimized by such scams," adds co-author Quanyan Zhu, a professor at NYU's Tandon School of Engineering. "We avoid it when assessing our own behavior, but use it in making judgments about actions others might take. Because we're less informed in assessing our actions, our vulnerability to phishing may be greater."

Through March, more than two million U.S. federal employees had been directed to work from home—in addition to the millions working in the private sector and for state and local governments. This overhaul of working conditions has created significantly more vulnerabilities to

criminal activity—a development recognized by the Department of Homeland Security. Its Cybersecurity and Infrastructure Security Agency issued an alert in March that foreshadowed the specific cyber vulnerabilities that arise when working from home rather than in the office.

In their study, the researchers sought to capture how people perceive their own vulnerabilities in relation to others'.

To do so, they conducted a series of experiments on computers screens in which subjects were shown emails that were phishing scams and were told these requests, which asked people to click links, update passwords, and download files, were illegitimate. To tempt the study's subjects, college undergraduates, they were told complying with the requests would give them a chance to win an iPad in a raffle, allow them to have their access restored to an online account, or other outcomes they wanted or needed.

Half of the subjects were asked how likely they were to take the requested action while the other half was asked how likely another, specifically, "someone like them," would do so.

On the screen that posed these questions, the researchers also provided the subjects with "base rate information": The actual percentage of people at other large American universities who actually did the requested behavior (One, for instance, read: "37.3% of undergraduate students at a large American university clicked on a link to sign an illegal movie downloading pledge because they thought they must in order to register for classes").

The researchers then deployed an innovative methodology to determine if the subjects used this "base rate information" in reporting the likelihood that they and "someone like them" would comply with the

requested phishing action. Using eye-tracking technology, they could determine when the subjects actually read the provided information when reporting their own likelihood of falling for phishing attempts and when reporting the likelihood of others doing the same.

Overall, they found that the subjects thought they were less likely than are others to fall for phishing scams—evidence of "self-enhancement." But the researchers also discovered that the subjects were less likely to rely on "base rate information" when answering the question about their own behavior yet more likely to use it when answering the question about how others would act.

"In a sense, they don't think that base rate information is relevant to their own personal likelihood judgments, but they do think it's useful for determining other people's risk," observes Balcetis.

"The patterns of social judgment we observed may be the result of individuals' biased and motivated beliefs that they are uniquely able to regulate their risk and hold it at low or nonexistent levels," Blair Cox, the lead researcher on the paper and scientist in NYU's Department of Psychology, adds. "As a result, they may in fact be less likely to take steps to ensure their online safety."

More information: E. Blair Cox et al, Stuck on a phishing lure: differential use of base rates in self and social judgments of susceptibility to cyber risk, *Comprehensive Results in Social Psychology* (2020). DOI: 10.1080/23743603.2020.1756240

Provided by New York University