SECURITY | **LEER EN ESPAÑOL**

Hackers want you to be happy. People in a good mood are easier to trick, research says

A study from the University of Florida looks at the psychology of phishing emails and when you're most likely to click on that link.

BY ALFRED NG 🐦 | AUGUST 7, 2019 5:05 PM PDT

f 𝕏 F ⑂ 💬 0

The study, presented by researchers from Google and the University of Florida, found that hackers used psychological tricks to get people to click on malicious links.

Angela Lang/CNET

Being in a bad mood can have its benefits. Like keeping you safe from hackers.

Ebner, presented the research at the Black Hat cybersecurity conference in Las Vegas on Wednesday. Oliveira was joined by Elie Burszstein, who leads Google's anti-abuse research team.

Phishing attacks are an online scourge in which hackers pose as legitimate institutions in the hopes of getting personal information, such as passwords. Phishing, which usually occurs via email, is the leading cause of data breaches, according to an annual report by Verizon. Google blocks about 100 million phishing emails every day, Burszstein said.

Phishing campaigns change quickly. Some morph in as little as seven minutes, he said.

"Attackers keep changing and updating their designs to make them more efficient," Burszstein said. "They quickly adapt and keep the number of targeted users low. This makes it really hard to detect."

Phishing has become so sophisticated that most people are susceptible to attack unless they have multi-factor authentication enabled. Though phishing attacks are easily detectable, they're also effective. As Amazon chief technology officer Werner Vogels said at the Amazon Web Services Summit, "there's always that idiot that will click the link."

Oliveira's study suggests that you aren't an idiot if you click on a phishing link. You're just human.

Over the course of the three-week experiment, 158 participants, who were told they were participating in research about how people use the internet, would get a phishing email once a day. Researchers would track whether they clicked it. The emails were based on real phishing campaigns that Google had detected.

Phishing emails are crafted to exploit human nature. They rely on people making quick decisions without thinking, almost as if clicking on the link were a reflex and not a cognitive decision, she found.

"We are susceptible to phishing because it tricks the way our brain makes decisions," Oliveira said.

When it comes to decision-making, our brains can work in two ways, the researcher said, referencing the dual process theory. Your brain works automatically for daily activities, like brushing your teeth. Big decisions, like buying a house, take a lot of deliberation and thought.

Clicking on email links falls into the former camp, and hackers rely on that fast decision-making to phish victims, she noted.

The tech giant plans an awareness campaign.

Luckily, we all have psychological protection that works in the background. Oliveira said that people with high levels of stress are better at detecting deception like phishing emails, and more skeptical of online scams. It's why some phishing campaigns use psychological triggers to get people in a good mood, she said.

"Nobody is telling anybody to be in a bad mood and stressed out all the time," Oliveira said. "Just keep in mind that when you are in a good mood, your guard is down."

BLACK HAT DEFCON

READING · Hackers want you to be happy. People in a good mood are easier to trick, research says

AUG 11 · DARPA's $10 million voting machine couldn't be hacked at Defcon (for the wrong reasons)

AUG 10 · That 4G hotspot could be a hotbed for hackers

AUG 10 · Those robocall blocker apps are hanging up on your privacy

AUG 9 · What a security researcher learned from monitoring traffic at Defcon

· SEE ALL ›