Phishing tricksters nab the warm fuzzies, smiles

11 August 2019, by Nancy Cohen

Credit: CC0 Public Domain

Phishing is the most common form of cyberattack and still growing. Yet, in a survey of Internet users, it was found that 45 percent of those surveyed did not understand what phishing was or the risk associated with it.

Alfred Ng in CNET is one of many tech watchers who do not take phishing lightly. "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."

Recent research from University of Florida shows that those who fall victim to phishing attacks are not necessarily idiots or fools or anything else you want to sling to remind the world you are more clever than they.

A University of Florida study finds that people in a good mood were easier to trick. Alfred Ng, CNET: "Being in a bad mood can have its benefits. Like keeping you safe from hackers."

University of Florida Professor Daniela Oliveira, who led the study along with Dr. Natalie Ebner, presented research at the Black Hat cybersecurity conference in Las Vegas recently. Oliveira was joined by Elie Burszstein, who leads Google's anti-abuse research team. Bursztein's team invents ways to protect users against Internet threats.

His slide show brought home the present phishing scene, where baiters are quite expert in preying on human emotions and also quite nimble in stirring up new traps for engagement.

Phishing is evolving and it is well crafted.

Researchers studied the psychology around phishing emails; hackers take advantage of human nature to tempt people into clicking on malicious links.

"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," Ng wrote.

Phishing victims are in the toothbrush camp during times when they feel like clicking.

So, you would need to curb your enthusiasm to single out victims as fools. Ng reported that "Oliveira's study suggests that you aren't an idiot if you click on a phishing link. You're just human."

Patrick O'Neill in *MIT Technology Review* likewise noted what Oliveira said at the Black Hat cybersecurity conference in Las Vegas. "We are all susceptible to phishing because phishing tricks the way our brain makes decisions."

There are forces at play here that make people behave according to "emotional intelligence, cognitive motivation, mood, hormones, and even

the victim's personality."

O'Neill explained further. "Mood plays a role: people who are feeling happy and not stressed are less likely to detect deception in front of them. Cortisol, a stress hormone, increases vigilance and makes detecting a deception more likely. Serotonin and dopamine, hormones associated with positive feelings, can lead to risky and unpredictable behavior that make people more vulnerable."

Deceptive cues make messages more appealing. These include persuasion; gain-loss framing; and emotional salience.

Bursztein's site carried a slide presentation, "Deconstructing the Phishing Campaigns that Target Gmail Users," Elie Bursztein, Daniela Oliveira.

Gmail, with over 1.4 billion active users, has a unique opportunity to get to know phishing tactics firsthand. What makes phishing an attack vector that is so hard to mitigate, however? Answer: Phishers quickly adapt their campaigns and they keep the number of targeted users low.

How fast do phishing campaigns change? CNET quoted Bursztein as saying some morphed in as little as seven minutes. "Attackers keep changing and updating their designs to make them more efficient," he added. Consider that some 68 percent of phishing emails blocked by Gmail are different every day.

What can be done about phishing, then? Building awareness of the traps and pitfalls cannot hurt but a number of observers uphold 2FA as a genuine protective measure and O'Neill spelled out the reward. Even if your password were stolen, the thieves would need something more to break in.

O'Neill liked the idea of two-factor authentication for each of a person's important logins (email, online banking, social media, shopping sites, etc.

"When it's enabled, the system asks you for something in addition to a password when you log in, such as a code sent to your phone via text message, a code from an authenticator app, or a physical security key on a USB stick (the most secure method of all, according to recent research). That way, if you've inadvertently given your password to a hacker in a phishing scam, they still won't be able to log in to your account. Last year, Google said that fewer than 10% of its users had two-factor authentication enabled on their accounts."

The *MIT Technology Review* article carried a link to a list of websites and whether or not they support 2FA.

APA citation: Phishing tricksters nab the warm fuzzies, smiles (2019, August 11) retrieved 17 January 2022 from https://techxplore.com/news/2019-08-phishing-tricksters-nab-fuzzies.html