We keep falling for phishing emails, and Google just revealed why

Here's what Google has learned by blocking 100 million phishing attacks on Gmail users—every day.

[Photos: Thomas Lefebvre/Unsplash; Clint Adair/Unsplash]

BY ROB PEGORARO
3 MINUTE READ

You should feel cranky about all the phishing emails you get. Because getting your brain in a grumpy gear will elevate the odds of your not getting fooled by the next phony invitation to log into your account.

At a briefing Wednesday evening at the Black Hat security conference in Las Vegas, Google security researcher Elie Bursztein and University of Florida security professor Daniela Oliveira shared that and other insights about the business of coaxing people into giving up their usernames and passwords.

The first thing to know about phishing: It's not as random and sloppy as it might seem. Said Bursztein: "Phishers have constantly refined."

The roughly 100 million phishing emails Google blocks every day fall into three main categories: highly targeted but low-volume spear phishing aimed at distinct individuals, “boutique phishing” that targets only a few dozen people, and automated bulk phishing directed at thousands or hundreds of thousands of people.

Those categories differ in duration. Google typically sees boutique campaigns wrap up in seven minutes, while bulk phishing operations average 13 hours.

Google also sees most phishing campaigns target its commercial mail service. Bursztein said Google-hosted corporate email accounts were 4.8 times more likely to receive phishing emails than plain old Gmail accounts.

Email services were the most commonly impersonated login page in those attempts, at 42%, followed by cloud services (25%), financial institutions (13%), online retail (5%), and delivery services (4%).

Bursztein noted that Google still can’t definitely identify many phishing emails—as improbable as that might seem, considering all the data it collects. That explains why Gmail shows an orange box above messages that look somewhat suspicious but aren’t necessarily attacks.

THIS IS YOUR BRAIN ON PHISHING ATTACKS

The presentation also covered the human factors that make phishing easier. As Oliveira explained, “When we are in a good mood, our deception-detection accuracy tends to decline.”

She cited research showing that increased levels of such feeling-good hormones as testosterone and estrogen, oxytocin, serotonin, and dopamine increase people’s risk-taking appetite. But a jump in cortisol levels associated with stress makes us warier.

Presumably, the soundtrack for your mail screening should not be Marvin Gaye’s “Let’s Get It On” but the J. Geils Band’s “Love Stinks.”

Oliveira outlined three common persuasive tactics in phishing invitations: appeals from a perceived authority (do you really want to ignore that urgent email from your boss?), offers of financial gain for acting on the message or warnings of financial loss for ignoring it, and appeals to the recipient’s emotions (“Won’t someone please think of the children?!”).

Bursztein and Oliveira’s advice to email users did not involve any recommendations to study web addresses in messages and on phishing landing pages. Instead, they emphasized two-step verification—but not just any form of 2FA.

Prior Google research showed that SMS verification, among the most common implementations of 2FA, can defeat larger-scale phishing but not the most targeted sort—while it worked against 96% of boutique phishing attempts, it only prevailed against 76% of spear-phishing attacks.

One key reason: Advanced phishing pages ask the target users to enter the code texted to their phone, then use that second credential to validate their account takeover before it expires. SIM-swap attacks to take over a phone account will also shatter this shield.

On-device prompts like those generated by Google’s Authenticator app are significantly stronger, thwarting 99% of boutique phishes and 90% of spear-phishing attempts. But the strongest protection comes from USB security keys, which in Google’s testing defeated 100% of all phishing attempts.

That’s because a USB key such as Yubico’s popular series needs to see the cryptographic key of the original site—a lookalike domain name or login page won’t fool its single-minded silicon.

But USB keys remain unsupported by many sites, won’t see support from Apple’s Safari until the macOS Catalina update ships later this year, and cost $20 and up. Bursztein and Oliveira brought a bunch to Vegas to give away to attendees at their talk, but everyone else will have to go out of their way to upgrade to that level of security.

09.14.19