How this 26-year-old Amazon employee saved $120,000 in less than 4 years

Netflix vs Apple: Here's which stock would have made you richer if you invested...

Tech entr
built $35M

WORK

Checking your email when you're grouchy could make you less likely to fall for phishing scams

Published Tue, Aug 27 2019 • 9:39 AM EDT

Jennifer Liu

@criene | Twenty20

you to click through to some important company update. You click, before noticing that something was just so slightly off in the sender's address.

Now you have to watch a 20-minute training video about email security in the workplace.

It happens to the best of employees. But security researchers have a few tips to safeguard yourself — and your data — from phishing campaigns. And as it turns out, scanning your inbox while in a bad mood could help you avoid falling for such a scam.

Here's why:

Why phishing is so successful

Phishing is the practice of sending fake emails from a supposedly reputable source with the intent of getting the user to divulge sensitive information like passwords and credit card numbers. And like all forms of technology, it's grown more sophisticated over the years. Psychology has begun to play a larger role.

"We are all susceptible to phishing because phishing tricks the way our brains make decisions, especially in regard to deception detection," Daniela Oliveira, a professor at the University of Florida, tells CNBC Make It. Oliveira, along with professor Natalie Ebner, researches interdisciplinary computer security and what makes certain segments of users more susceptible to cybersecurity threats. "The conclusion is that our ability to detect deception is influenced by interindividual differences in cognitive motivation, socioemotional functioning and neurobiology."

Essentially, phishers hope to trick the part of your brain that reacts quickly. It does so by targeting, as Oliveira and Ebner put it in their 2017 study on phishing, principles of influence. For example, phishers may try to mimic a person of authority (like your boss) knowing humans tend to comply with requests made by figures of authority. Or

Your mood can impact how secure your inbox is

Phishers may have strategies to get your attention, but your own personality — and possibly mood — can play a role in how vulnerable you are to either falling for or resisting a scam.

For example, Oliveira says that people with higher levels of emotional intelligence tend to understand emotions better, both their own and others', making them better able to detect deception. People who scored lower in agreeableness as a personality trait were also better at spotting a scam.

Even so, there's a possibility that your day-to-day disposition can also play a role your gullibility.

"A positive mood tends to produce a more optimistic interpretation of social situations, which might reduce our levels of suspicion," Oliveira says. A negative mood, on the other hand, might trigger the part of the brain that processes information slower and more deliberately (as in, not the instant reaction phishers are hoping for).

And as for neurobiology, hormones can influence our risk-taking behavior. "Individuals with high levels of steroid hormones — testosterone or estrogen — tend to take greater risks, which might leave them more vulnerable to deception," Oliveira says. "Oxytocin, also called the social hormone, has been shown to decrease deception detection accuracy. Increased levels of dopamine in the brain bring forth impulsive and risk-taking behaviors under uncertainty, which leaves them more vulnerable to deception.

"On the other hand, increased levels of cortisol, the stress hormone, is associated with decreased risk-taking behavior," she adds. "Nobody here is saying that being in a bad mood or stressed out is good, but it all seems to reinforce the idea that you need to be more vigilant when in a good mood or when relaxed."

You might be thinking, "But I can spot an email scam a mile away — there are typos everywhere!" That's no longer always the case, especially as phishers become more targeted in their methods. So in addition to having a heightened awareness of potential cybersecurity threats, other tools can help keep your information safe.

Citing Oliveira and Ebner's research, Google security researcher Elie Bursztein recommends using two-factor authentication to protect your data. Looking into the 100 million phishing emails Google blocks every day, two methods stand out: Opt in to receive a text with a security code to log into accounts, or use an authentication app like Google Authenticator, LastPass or 1Password.

This awareness is crucial whether you're logged into your own or your work email. According to the data, Google-hosted corporate accounts were 4.8 times more likely to receive phishing emails than personal Gmail accounts. And scammers take many shapes — phishers are most likely to impersonate email providers (42%), cloud services (25%), financial institutions (13%), e-commerce (5%) and delivery companies (3.9%).

Like this story? Subscribe to CNBC Make It on YouTube!

1:07
Don't miss: This map shows where in the US cyber crime costs people the most
This former FBI agent shares her best tips to avoid scams

Trending Now

1 **19% of Americans are considered 'upper class'—here's how much they earn**

2 **I raised 2 successful CEOs and a doctor—here's one of the biggest mistakes I see parents making**

4 How a former NBA No. 1 draft pick blew a $61 million fortune and now owes six figures

5 8 US cities that will pay you thousands to move there

Stay in the loop

Get Make It newsletters delivered to your inbox

SIGN UP

About Us

Learn more about the world of CNBC Make It

LEARN MORE

Follow Us