BIZCOMMUNITY

One question can keep you safe from phishing scams

Phishing is the most widely used and successful cybercrime attack. Some estimates claim that over three billion phishing emails are sent every year. It's a cheap, simple and very effective tactic because it targets people.

"I don't like the saying that people are the weakest link in security," says Gerhard Swart, chief technology officer at cybersecurity company, Performanta.

"Instead, we should say that people are the best target. If a computer is properly secured, it takes a lot of technical effort and know-how to fool that machine into installing bad software or something to that degree. But because of the trust we give humans, which need to use those computers, they can be manipulated into making those mistakes. And because the computer they use trusts them, humans can unintentionally subvert security. Humans enjoy a terrific amount of security privilege, that's why cybercrime often targets people."

Qualified, but still a liar - consequences of CV misrepresentation
Jacques van Wyk and Andre van Heerden 10 Oct 2023

Cybercriminals try to provoke us into sudden and spontaneous actions that we will regret later, but by then, the damage is done.

This is the purpose of phishing emails: they appeal to our base emotions and make us reactive. The promise of lotto winnings or an unexpected delivery, banking instructions from an angry customer, or even an odd letter from your child's school - criminals will stoop low to hijack our attention and get us to interact with a dangerous attachment or link.

Is it legit?

But phishing attacks are not automatic; they require a person to interact with that bad attachment or link, hoping we don't consider our actions. Hence phishing messages lure us with great reward or urgency. The simplest countermeasure is to pause and ask: "Is it legit?"

"Are you waiting for a package? Did you expect that client to suddenly change their banking details? Has an unknown aunt really died and left a fortune to you? No, most likely not. Let's take a common example: an email claiming your Netflix subscription has failed. But did you get a notice from the bank? Has your Netflix stopped working? It takes a few seconds to check. Phishing attacks hope you don't until it's too late," says Swart.

When we take a few seconds to question the legitimacy of an email, we thwart phishing. Look at an email and ask yourself: "Is this legit?" If there is any doubt, don't click on anything. Report the incident to your IT department or service provider and delete the email. Phishing emails could even arrive from a trusted person whose account was hijacked.

Legitimacy must pass several tests:

- Are you expecting this correspondence?
- Does the correspondence sound like that person?
- Does the correspondence inform, not demand immediate action?
- Can you verify the message independently (such as calling the sender)?

If it fails on any of these points, the email (or SMS or instant message) is not legit. There are other signs as well because criminals keep evolving their tactics. But taking a moment to pause and evaluate the message will almost always stop their attempt.

Keep your business and people secure. Start by encouraging them to adopt this single habit - when responding to a message, pause and ask: "Is it legit?"