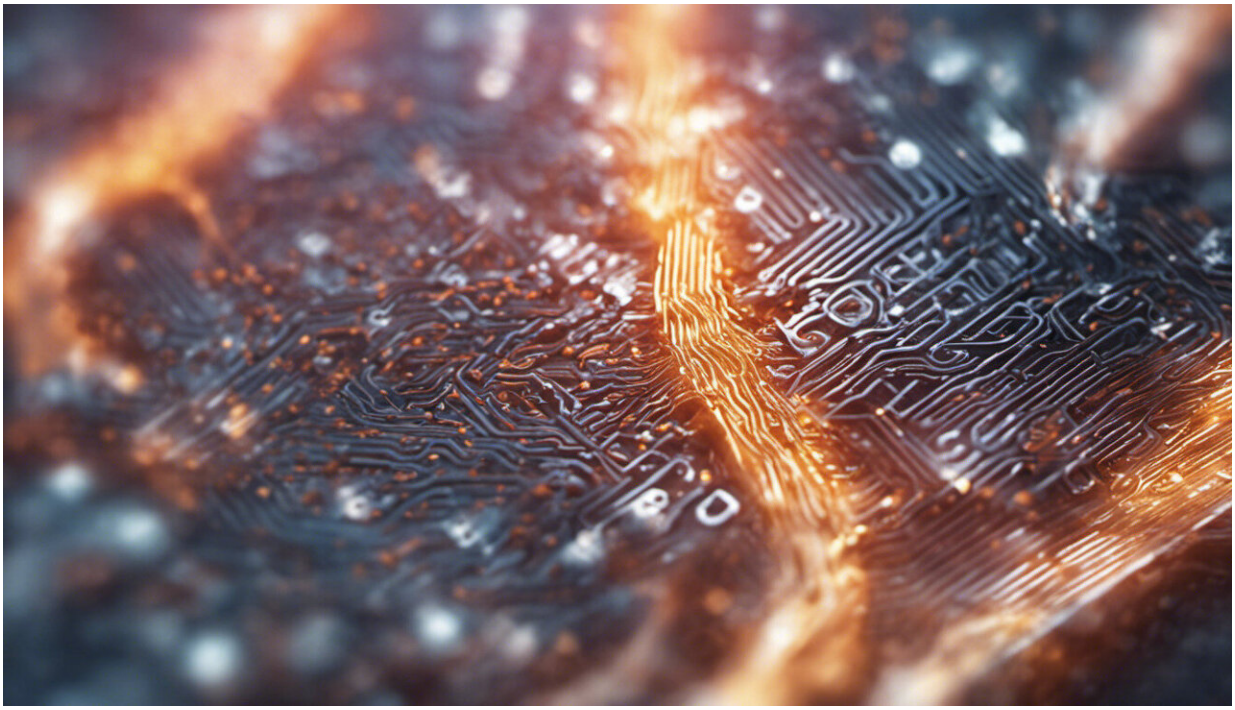
Email scams are getting more personal. They even fool cybersecurity experts

July 12 2022, by Gareth Norris, Max Eiza and Oliver Buckley



Credit: AI-generated image (disclaimer)

We all like to think we're immune to scams. We scoff at emails from an unknown sender offering us £2 million, in exchange for our bank details. But the game has changed and con artists have developed new, chilling tactics. They are taking the personal approach and scouring the internet for all the details they can find about us.

Scammers are getting so good at it that even cybersecurity experts are taken in.

One of us (Oliver Buckley) recalls that in 2018 he received an email from the pro-vice chancellor of his university. "This is it, I thought. I'm finally getting recognition from the people at the top. Something wasn't right, though. Why was the pro-vice chancellor using his Gmail address? I asked how I could meet. He needed me to buy £800 worth of iTunes gift cards for him, and all I needed to do was scratch off the back and send him the code. Not wanting to let him down, I offered to pop down to his PA's office and lend him the £5 note I had in my wallet. But I never heard back from him."

The infamous "prince of Nigeria" emails are falling out of fashion. Instead, scammers are scouring social media, especially business-related ones like LinkedIn, to target people with tailored messages. The strength of a relationship between two people can be measured by inspecting their posts and comments to each other. In the first quarter of 2022, LinkedIn accounted for 52% of all phishing scams globally.

Human tendencies

Psychologists who research obedience to authority know we are more likely to respond to requests from people higher up in our social and professional hierarchies. And fraudsters know it too.

Scammers don't need to spend much time researching corporate structures. "I'm at the conference and my phone ran out of credit. Can you ask XXX to send me report XXX?" runs a typical scam message.

Data from Google Safe Browsing shows there are now nearly 75 times as many phishing sites as there are malware sites on the internet. Almost 20% of all employees are likely to click on phishing email links, and, of

those, a staggering 68% go on to enter their credentials on a phishing website.

Globally, email spam cons cost businesses nearly US$20 billion (£17 billion) every year. Business consultant and tax auditor BDO's research found that six out of ten mid-sized business in the U.K. were victims of fraud in 2020, suffering average losses of £245,000.

Targets are normally chosen based on their rank, age or social status. Sometimes, spamming is part of a coordinated cyber attack against a specific organization so targets are selected if they work or have connections to this organization.

Fraudsters are using spam bots to engage with victims who respond to the initial hook email. The bot uses recent information from LinkedIn and other social media platforms to gain the victim's trust and lure them into giving valuable information or transferring money. This started over the last two to three years with the addition of chatbots to websites to increase interactions with customers. Recent examples include the Royal Mail chatbot scam, DHL Express, and Facebook Messenger. Unfortunately for the public, many companies offer free and paid services to build a chatbot.

And more technical solutions are available for scammers these days to conceal their identities such as using anonymous communication channels or fake IP addresses.

Social media is making it easier for scammers to craft believable emails called spear phishing. The data we share every day gives fraudsters clues about our lives they can use against us. It could be something as simple as somewhere you recently visited or a website you use. Unlike general phishing (large numbers of spam emails) this nuanced approach exploits our tendency to attach significance to information that has some

connection or for us. When we check our full inbox, we often pick out something that strikes a chord. This is referred to in psychology as the illusory correlation: seeing things as related when they aren't.

How to protect yourself

Even if you're tempted to bait email scammers, don't. Even confirming your email address is in use can make you a target for future scams. There is also a more human element to these scams compared with the blanket bombing approach scammers have favored for the last two decades. It's eerily intimate.

One simple way to avoid being tricked is to double-check the sender's details and email headers. Think about the information that might be out there about you, not just about what you receive and who from. If you have another means of contacting that person, do so.

We should all be careful with our data. The rule of thumb is if you don't want someone to know it, then don't put it online.

The more advanced technology gets, the easier it is to take a human approach. Video call technology and messaging apps bring you closer to your friends and family. But it's giving people who would do you harm a window into your life. So we have to use our human defenses: gut instinct. If something doesn't feel right, pay attention.

Provided by The Conversation

Citation: Email scams are getting more personal. They even fool cybersecurity experts (2022,

July 12) retrieved 19 May 2024 from https://techxplore.com/news/2022-07-email-scams-personal-cybersecurity-experts.html