Recognize Common Email Scams and Hacks

YEO & YEO COMPUTER CONSULTING

Prioritizing Email Security

Not enough businesses put in place a proactive, preventative security strategy until they've been hacked. That's like waiting until you've been robbed to put locks on the door. There are lots of different types of email hacks. These are the most common ones we have either seen ourselves or heard about from our network of international IT security experts.

Email Forwarders: Hackers gain access to your email just once and create an email forwarder. Then, without your knowledge, all incoming email is forwarded to them. It's usually quite easy for them to spot patterns, such as invoices being sent to you regularly. From there, they can play a long game, gathering information and building up a profile of their target until an opportunity presents itself to steal some money.

Spoofed Emails: Hackers buy a domain name that's very similar to a real domain used by a supplier. Your supplier might use xyzcompany.com. And the hacker buys xyzcommpany.com. An extra character can often go unnoticed. Another trick would be to buy a domain with a different extension, such as a .net rather than a .com.

Follow-up Emails: Hackers send a malicious follow-up email immediately after a real email, and most people assume it's real.

Compromising a Supplier's Email: If hackers can compromise your supplier's email and intercept the outgoing invoices, they can get a range of customers to pay money to the wrong bank account. Flip that around, and imagine a hacker adjusted all of your invoices. So your customers were making payments, but not to your bank account.

Edited PDF: Many people think a PDF on an email is a safe document. But PDFs can be easily edited. We've heard of hackers intercepting invoice PDFs, editing them to change the bank account details, and then sending them to customers. This is a very clever hack because the person paying the invoice will typically have zero suspicion.

Social Engineering: Once a hacker is inside your email, they will gather information and look for opportunities. A golden chance for them is when the boss is on vacation. Because that's a break in normal patterns of behavior, they can leverage that.

We heard of one company where the boss's email was compromised, with an email forwarder set up. The hackers set up a Gmail account in the boss's name and emailed someone senior in the company. "My work email's not working, so I'm using my personal email," the message read. "Lovely sunshine here. I forgot to pay an invoice before I went – can you pay this quickly, please?" Inevitably, the staff didn't think twice.