HSB

A Munich Re company

Technical bulletin

Phish bait

Three tips to help you avoid a hacker's hook

We all know to look out for suspicious emails. But phishing emails are becoming increasingly more sophisticated, tricking even the savviest amongst us. Here are three tips to avoid falling for cybercriminals' latest tricks.

1. Check the source

Before you open that email, take a moment to consider the source of the email and whether that person is likely to send you an attachment or link. Did the email come from someone with whom you regularly communicate? Check the email address, screen name, or phone number associated with the message. Hackers often mimic an email address that you would trust with one letter or number off from the original name or domain. For example, john_smith@company.com looks a lot like john_sm1th@company.co, but the subtle differences (there were two; did you spot them?) dictate whether you are receiving a business email or a malicious fake.

The address may even look exactly like a trusted contact but when you place your mouse pointer over the name, you can see that the address is different. A hacked email account can also be used to send malicious content, so be sure to evaluate the content of the message.

2. Check the content

Before you click on a link or download an attachment, take a look at it. Often, if you (carefully!) copy the link or type the name of the attachment into a search engine (not directly into your browser's web address field), you can find out whether or not the content is actively being used to spread malicious content (a virus, ransomware, etc.).

Ask yourself whether this is the type of content you usually receive from the sender. Are you expecting an attachment from the sender? Is the attachment or link the only content of the email? If you have the slightest doubt, either delete the message or give the sender a call. The amount of time used to verify the content is relatively short when compared to the time and expense incurred remediating a cyber-attack or data breach.

Hackers often make an urgent request to trick us into clicking on malicious links or files. Any urgent request sent via email should be verified in-person.

3. What if I clicked on the suspicious link or attachment?

Everyone makes mistakes and you wouldn't be the first person to click on a suspicious link or download a suspicious file. Even if nothing happens immediately, there is no guarantee that the threat has gone. Malware can lay dormant for weeks, months, or even years before activation. It may also be transmitting information in the background without your knowledge.

So, take action as soon as you realise you clicked on a suspicious link or file. Alert your IT security department immediately. If you are a smaller business, run a full virus scan and monitor your customer, company and financial data.

www.hsbeil.com HSBEI-2063-1020-1 Picture credits: Getty Images