INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

PROTECTING YOURSELF FROM SPEARPHISHING ATTACKS

For a large enterprise like Stellenbosch University phishing attacks are the most common cybercrime.

In the late 1990s and early 2000s, we were all inundated with spam emails, selling everything from fake pharmaceuticals to cheap perfumes. With spam, cybercriminals use a blanket approach sending emails to as many people as possible, hoping a few gullible customers will be funding further spam emails.

General "shotgun" phishing is still a problem today, but the past 18 months have seen a rise in a more sinister form of cyberattack, spearphishing, which is much more targeted to an individual or an enterprise's email system.

Spearphishing is similar to phishing, it's also a vector for identity theft where cybercriminals try to get users to hand over personal and sensitive information without their knowledge.

Cybercriminals view phishing attacks as a profitable and an easy way to gain access to an enterprise enabling them to launch more sophisticated attacks, for example, spearphishing attacks. Humans are, after all, the weakest link and thus the most effective target for criminals looking to infiltrate a network like the university.

Even though spearphishing is more focused than its less-sophisticated relative phishing, everyone can apply the following principles to protect yourself and the university against cybercriminal activity:

Use common sense when it comes to phishing attacks
Be sensible and smart while browsing online and checking your emails. Never click on links, download files or open attachments in email or social media, even if it appears to be from a known, trusted source. You should never click on links in an email to a website unless you are absolutely sure it's authentic. If you have any doubt, open a new browser window and type the address into the address bar. Always be wary of emails asking for confidential information – especially if it asks for personal details or banking information. The university and your bank will never request sensitive information via email. They do not need it. They have it all already.

Watch out for shortened links
Pay particularly close attention to shortened links, especially on social media. Cybercriminals often use Bit.ly, Tinyurl.com, Goo.gl or Tr.im to trick you into thinking you are clicking a legitimate link when in fact, you are being inadvertently directed to a fake site. Always place your mouse over a web link in an email (known as "hovering") to see if you're being sent to the right website.

Does the email look suspicious? Read it again
Many phishing emails are obvious. They will be filled with plenty of spelling mistakes, CAPITALISATION and exclamation marks. They will also have impersonal salutations – e.g. 'Dear Valued Customer' or 'Dear Sir/Madam' salutations – and will have implausible and generally suspicious content. Cybercriminals will often intentionally make mistakes in their emails bypass spam filters and improve responses.

Be wary of threats and urgent deadlines
Sometimes the university does need you to do something urgently, however, this is an exception rather the rule. For

example, you all have been getting reminders to reactivate your network account by the end of March. Threats and urgency, especially coming from what claims to be a legitimate company, are a giveaway sign of phishing. Some of these threats may include notices of a fine or advising you to take action to stop your account from being closed. Ignore the scare tactics and rather contact the company via phone.

Browse securely with HTTPS
You should always, where possible, use a secure website, indicated by https:// and a security "lock" icon in the browser's address bar, to browse. This is particularly important when submitting sensitive information online, such as credit card details.

Never use public, unsecured Wi-Fi, including MatiesWiFi, for banking, shopping or entering personal information online. Convenience should never be more important than safety. When in doubt, use your mobile's 3/4G or LTE connection.

[ARTICLE by David Wiles]

Posted in:Phishing,Security,Tips | Tagged:Phishing,Spear Phishing | With 0 comments