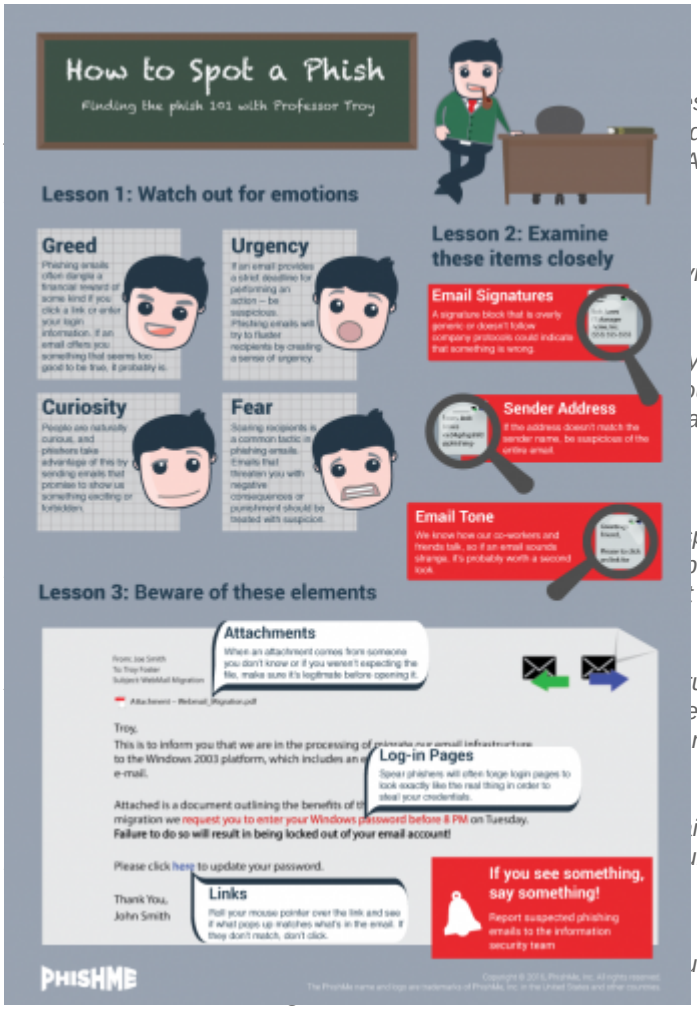
INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

HOW TO RECOGNISE A PHISHING E-MAIL

We can't warn you against every phishing e-mail– there's a new variation every day. You are the only person who can protect yourself from phishing scams and identity theft. The only way to do this is to learn to recognise a harmful e-mail by paying attention and keeping an eye out for a few tell-tale signs.



sses and often the person sending them has no idea who dress is supposedly coming from, it's fake. For example, if Also, see a list of types of companies generally used in

ious errors.

you as "ABSA customer" or "Dear user", etc. If the unt, they would mention your account details or name in a client by name and won't ask you for your information.

pecific deadline, creating a sense of urgency and berly. For example, demanding that you log in and will be closed.

ue URL you are visiting, often these e-mails will show a e link and look at the display address. Is this the website not, it's clearly a phishing e-mail.

ins malware. When opened, it will run and install a small r PC and information.

unts being hacked, out-of-date accounts, or account

• Credit cards expiring or being stolen, a duplicate credit card, credit card transactions, etc.
• Confirming orders, requesting that you log in to confirm recent orders or transactions before a delivery can be made.
• Winning a prize or getting something for free. Both Woolworths and Pick 'n Pay's have been used in fake campaigns to lure people into providing personal details.

Company names phishers generally use

• Any major bank. ABSA and Standard Bank are both popular choices in South Africa.

• Insurance companies, for example, Outsurance.
• Internet service providers
• Apple or Microsoft claiming your account has been suspended.
• E-mail providers, e.g. Gmail or Yahoo
• SARS. Especially at this time of year. (We've had a few of these.)
• DHL or any delivery company claiming they have a package for you.
• Your company's medical aid, for example, Discovery
• Your company's IT department
• Casinos and lotteries
• Online dating websites
• Popular websites such as Amazon, Facebook, MySpace, PayPal, eBay, Microsoft, Apple, Hotmail, YouTube, etc.

A few tips to keep you safe

*• **Never follow links in an e-mail you're uncertain of.** Rather visit the page by typing the address of the company in your browser. For example, instead of clicking on the "ABSA URL" in the e-mail, type http://www.absa.co.za in your web browser and log in at their official website.*
*• **Never send personal information by e-mail.** If a company is asking for your personal account information or claiming your account is invalid, visit the website and log in to the account as you normally would. If everything seems in order and there aren't any urgent notifications from your bank, you should be fine.*
*• If you are still not sure about the status of your account or are concerned about your personal information, **contact the company directly**, either through an e-mail address provided on their website, over the phone or visit your local branch.*
*• **Delete the e-mail** and don't click on links or fill in any information.*
*• If you've already divulged your information, immediately **change your password or PIN** and contact the institution to inform them of the breach.*
*• To **report spam or phishing e-mails** send an e-mail to sysadm@sun.ac.za with the subject SPAM with the suspect e-mail attached. IT system administrators will then be able to block the e-mail to protect other users.*

[SOURCE: www.computerhope.com]

Posted in:E-mail,Security,Tips | Tagged:Hacking,Phishing,Spam | With 0 comments