

# INFORMASIE TECHNOLOGIE

## 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.

**How to Spot a Phish**  
Finding the phish 101 with Professor Troy

**Lesson 1: Watch out for emotions**

- Greed**: Phishing emails often target a financial reward or some kind of perk. If you click a link or enter your login information, an email offers you something that seems too good to be true, it probably is.
- Urgency**: If an email provides a strict deadline for performing an action — be suspicious. Phishing emails will try to fluster recipients by creating a sense of urgency.
- Curiosity**: People are naturally curious, and phishers take advantage of this by sending emails that promise to show us something exciting or forbidden.
- Fear**: Scaring recipients is a common tactic in phishing emails. Emails that threaten you with negative consequences or punishment should be treated with suspicion.

**Lesson 2: Examine these items closely**

- Email Signatures**: A signature block that is overly generic or doesn't follow company protocols could indicate that something is wrong.
- Sender Address**: If the address doesn't match the sender name, be suspicious of the entire email.
- Email Tone**: We know how our co-workers and friends talk, so if an email sounds strange, it's probably worth a second look.

**Lesson 3: Beware of these elements**

- Attachments**: When an attachment comes from someone you don't know or if you weren't expecting the file, make sure it's legitimate before opening it.
- Log-in Pages**: Spoof phishers will often forge login pages to look exactly like the real thing in order to steal your credentials.
- Links**: Put your mouse pointer over the link and see if what pops up matches what's in the email. If they don't match, don't click.

**If you see something, say something!**  
Report suspected phishing emails to the information security team.

**PHISHME**  
The PhishMe name and logo are trademarks of PhishMe, Inc. in the United States and other countries.  
Copyright © 2015, PhishMe, Inc. All rights reserved.

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

...rious errors.

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

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

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

...installs malware. When opened, it will run and install a small program on your PC and information.

...accounts 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](mailto: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](http://www.computerhope.com)]

Posted in: [E-mail](#), [Security](#), [Tips](#) | Tagged: [Hacking](#), [Phishing](#), [Spam](#) | With 0 comments