CYBERSECURITY AWARENESS MONTH: SOME STATISTICS AND COMMON SENSE ADVICE

*Posted on **May 11,2018** by **David Wiles***

onth is behind us. As a final signoff, we would like to share a few statistics ou spot phishing scams.

nced enough to be included in phishing attacks? According to Drew van e second most targeted country globally when it comes to phishing attacks.

o approximately R4.2 billion in 2013 alone and 5% of phishing attacks of "if" the university is going to be a target, but "when". Phishing attacks are ld also be yours as a user of the internet.

30% of South African internet users share at least three pieces of personal could be used to steal their identity.

no idea what their privacy settings were and who could see their personal Twitter etc.

using the same password or usernames on multiple sites, including social g to Ofcom's "Adults' Media Use and Attitudes Report 2013" report, 55% of the poll respondents used the same password for most, if not all, websites.

Here are 10 common-sense tips to help you spot and prevent becoming a victim of a phishing scam:

1. Learn to identify suspected phishing emails

- They duplicate the images and branding of a real company.
- They copy the name of a company or an employee of the company.
- They include sites that are visually similar or identical to a real business.
- They promote gifts or threaten the closure of an existing account.

2. Check the source of information from incoming email

Your bank, Information Technology, or cell phone provider will never ask you to send your passwords or personal information by mail. Never respond to these questions, and if you have the slightest doubt, call your bank, IT or your cell phone provider directly for clarification.

3. Never go to your bank's website by clicking on links in emails

Do not click on hyperlinks or attachments, as it will direct you to a fraudulent website. Type in the URL into your browser or use your own bookmarks or favourites if you want to go faster.

4. Beef up the security of your computer

Common sense and good judgement are as vital as keeping your computer protected with a good antivirus and anti-malware software to block this type of attack. In addition, you should always have the most recent update on your operating system and web browsers.

5. Enter your sensitive data on secure websites only

In order for a site to be 'safe', the address must begin with 'https://' and your browser should show a closed lock icon.

6. Periodically check your accounts

It never hurts to check your bank accounts periodically to be aware of any irregularities in your online transactions.

7. Phishing doesn’t only pertain to online banking

Most phishing attacks are against banks, but can also use any popular website to steal personal data such as eBay, Facebook, PayPal, etc. Even the university's e-HR site was targeted in 2017.

8. Phishing is international

Phishing knows no boundaries and can reach you in any language. In general, they are poorly written or translated so this may be another indicator that something is wrong. However, don't be convinced it's legitimate if it's in Afrikaans - phishers are getting clever and adapting.

9. Have the slightest doubt? Do not risk it.

The best way to prevent phishing is to consistently reject any email or news that asks you to provide confidential data. Delete these emails and call your bank to clarify any doubts.

10. Keep up to date and read about the evolution of malware

If you want to keep up to date with the latest malware attacks, recommendations or advice to avoid any danger on the network, subscribe to the Information Technology blog or follow them on Twitter. Put your local computer geek or the IT HelpDesk on the speed dial of your cell phone, and don't be embarrassed or too proud to ask questions from those who are knowledgeable on this topic.

Keep safe out there.

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