INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

TAX SEASON = CYBER SCAMS

Only people with an unusual desire for pain and discomfort look forward to a trip to the dentist. The same goes for tax.

Criminals know this and prey on our vulnerability. Every year at this time, e-mails like the one below end up in SU staff inboxes. It informs you that the taxman owes you money and all you have to do to receive it, is to click on a link.

This is a scam, and you should never respond or go to the site or open up the attached file, as this could compromise your banking security.

1. *SARS has your banking details on record and keeps it in secure and encrypted form. They do not need you to confirm or enter your banking details.*
2. *SARS will always either SMS or send you a registered letter in the post to inform you of tax returns. They will never contact you by unsecured e-mail.*
3. *They also have enough data to address the mail to you PERSONALLY and not via some vague “Dear Taxpayer” or "Good Day" salutation.*
4. *There is no EFiling@sars.gov.za address.*
5. *The attached file is usually a html (webpage) file and will connect you to a server controlled by the criminals. This server downloads a Trojan virus to your computer that will install software, malware and do all sorts of nasty things to your computer and data. Another tactic is to present you with a “login page” where you enter your banking account details, your PIN code etc.*
6. *Unless you have added your university e-mail address as the primary contact address on the SARS system, you should never receive mail on your university account.*

This phishing scam will allow the criminals to log into and take control of your bank account via the internet.

They can create themselves as beneficiaries, transfer your money to their account, and then delete the evidence pointing to their account.

These scam e-mails will never stop. It is always difficult to block them too because scammers change their addresses, details and methods on a daily basis. So it is always best to dump these mails in the junk mail folder, blacklist the sending domain and delete the mail immediately.

Why do these criminals continue to send their mail? Because they catch people regularly. In 2012 R14+ million was stolen from South Africans alone using phishing tactics such as this one.

Also read more on this on the mybroadband website.

EXAMPLE OF E-MAIL:

From: *SARS eFiling [mailto:eFiling@sars.gov.za]*
Sent: *Saturday, 27 June 2015 10:14*
Subject: *Your account has been credited with R3,167.14*

Your account has been credited with R3,167.14

Please click below to accept and verify payment.

Accept Payment

During this process, there will be verifications. If you don't receive codes on time, come back to finish verification when received

SARS eFiling

[ARTICLE BY DAVID WILES]

Posted in:Security | Tagged:Malware,Phishing,Sars,SARS E-mail | With 0 comments