INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

PHISHING MAIL USING INTIMIDATION AND THREATS

There is no need to panic or be in anyway concerned for your personal safety about the latest batch of "phishing" emails that are going out with "death threats" or extortion regarding your "alleged" online activity around pornography sites etc.

A simple Google search using the following term "I Was Paid To Kill You scam" gave me 43 million results, all of the first 100 or so pages reporting this mail as a scam. A further search, narrowing the results down to only South Africa and only from last week, resulted in a little over 100 000 results, all of which were reporting as a hoax.

A similar scam first surfaced in the USA in 2006. An email from a would-be assassin was sent to a number of users from a Russian e-mail address. The "assassin" apparently appointed by a close acquaintance of his target, offers the victim the opportunity to buy him or herself a new lease on life by paying between $50,000 and $150,000.

If you receive mail like this, you should never panic. If you look at the extortion mail there are clues that reveal that the mail is a hoax:

1. ***The subject line:*** *"I Was Paid To Kill You", "YOU SHOULD BE ASHAMED OF YOURSELF", "YOUR PRIVACY HAS BEEN COMPROMISED"*
   These are designed to cause anxiety, stress and panic.
2. ***Time limits:*** *"You have 48 Hours to pay…"*
   How can the scammer know that you have received the mail and when you have read the mail and keep track of time to see if "48-hours" has passed?
3. ***Engagement:*** *"Contact me back via e-mail…"*
   Never make contact with the scammers. This immediately alerts them that a "real person" read their mail and they will be able to concentrate their nefarious efforts on you.

If you ever receive emails like these, please report is to the Information Technology Cybersecurity Team using the following method:

Send the spam/phishing mail to help@sun.ac.za and sysadm@sun.ac.za.

Attach the phishing or suspicious mail on to the message if possible.
1. Start up a new mail addressed to sysadm@sun.ac.za (CC: help@sun.ac.za)
2. Use the Title "SPAM" (without quotes) in the Subject.
3. With this New Mail window open, drag the suspicious spam/phishing mail from your Inbox into the New Mail Window. It will attach the mail as an enclosure and a small icon with a light yellow envelope will appear in the attachments section of the New Mail.
4. Send the mail.

[Article by David Wiles]

Posted in:E-mail,Security | Tagged:Phishing,Report Phishing | With 0 comments