# INFORMASIETEGNOLOGIE

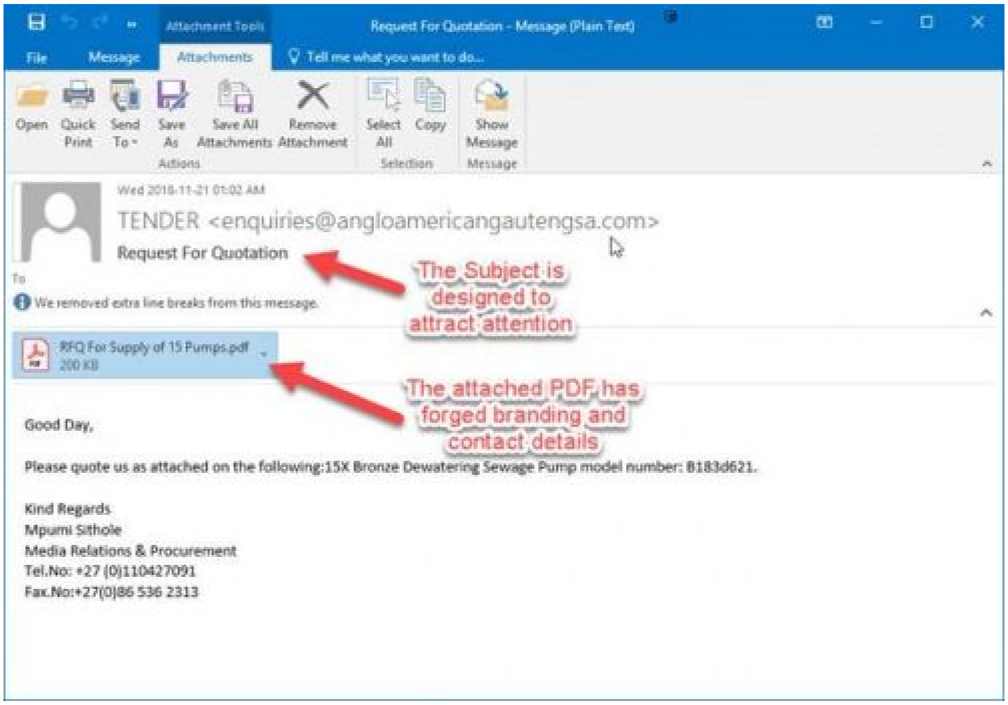
## INFORMATION TECHNOLOGY

## PHISHING SCAMS REQUESTING QUOTES AND NOTIFICATION ABOUT “NEW MESSAGE”

*Phishing attacks on the university continue with this week’s “flavour” being a return of the old “Request For Quotation” scam. With this scam you might receive an email from a large corporation arrives asking for you to provide a quotation, with an attached PDF that you are asked to fill in and send back to the sender.*

*Why would an academic department secretary be getting an RFQ to supply industrial supplies like sewage pumps? Scammers often only want to steal information from their victims, and in the case of the Faculty of Health Sciences, the scam RFQ could change to supply something like medical supplies or equipment.*

*Remember the email may look very convincing, with known company letterheads, VAT certificates etc.*



Wed 2018-11-21 01:02 AM

TENDER <enquiries@angloamericangautengsa.com>

Request For Quotation

The Subject is designed to attract attention

We removed extra line breaks from this message.

RFQ For Supply of 15 Pumps.pdf
200 KB

The attached PDF has forged branding and contact details

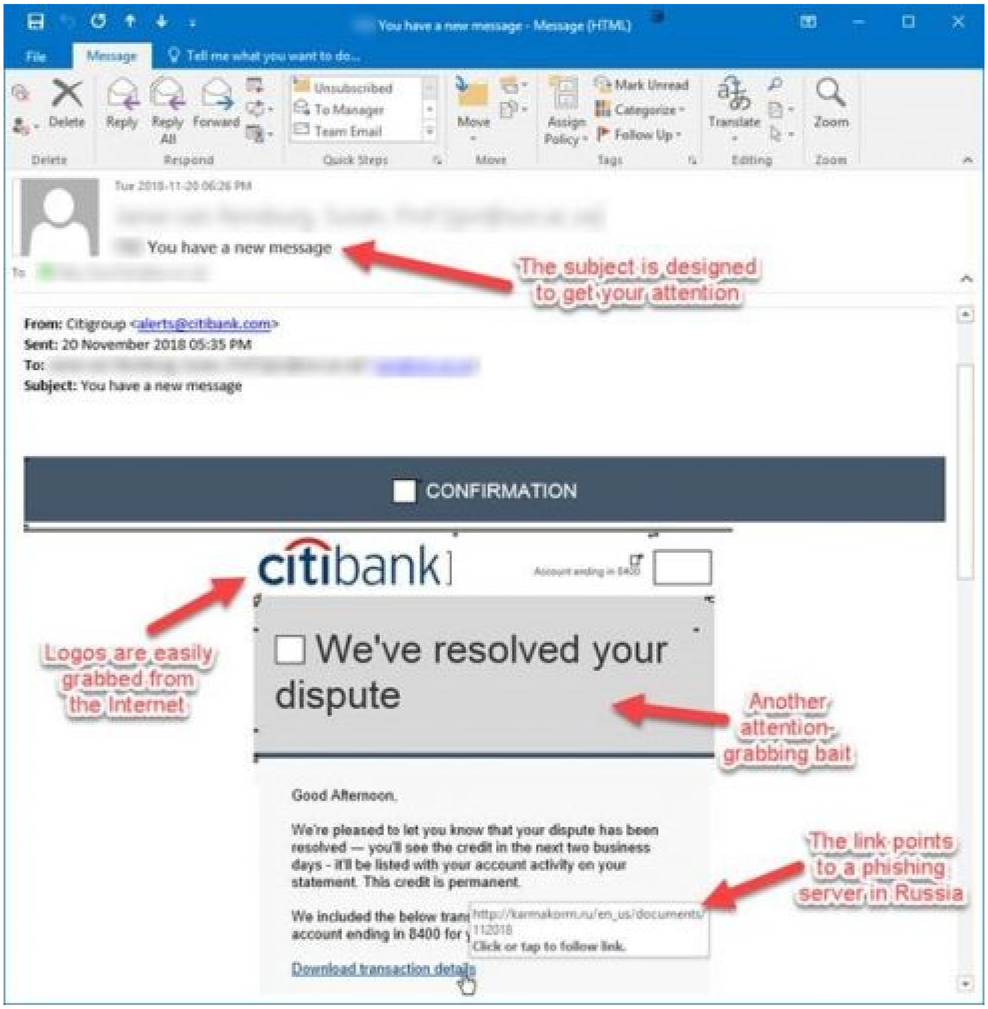
Good Day,

Please quote us as attached on the following:15X Bronze Dewatering Sewage Pump model number: B183d621.

Kind Regards
Mpumi Sithole
Media Relations & Procurement
Tel.No: +27 (0)110427091
Fax.No:+27(0)86 536 2313

*It is important not to respond to the sender or to open up the attachment. Often scammers just need a response so they can identify “live bait” and fine-tune their attack to a particular person.*

*Another phishing scam that appears to be coming back uses attention-getting subjects like “You have a new message” or “We’ve resolved your dispute” or “SARS refund pending” designed to get your attention. This particular one uses forged “Citibank” branding and informs you that a dispute has been resolved and you will be paid some money, but you are asked to open up a “document” to see the disputed transaction.*



Tue 2018-11-20 06:26 PM
[redacted]
[redacted] You have a new message
To [redacted]

The subject is designed to get your attention

**From:** Citigroup <alerts@citibank.com>
**Sent:** 20 November 2018 05:35 PM
**To:** [redacted]
**Subject:** You have a new message

□ CONFIRMATION

citibank

Account ending in 8400

□ We've resolved your dispute

Logos are easily grabbed from the Internet

Another attention-grabbing bait

Good Afternoon,

We're pleased to let you know that your dispute has been resolved — you'll see the credit in the next two business days - it'll be listed with your account activity on your statement. This credit is permanent.

We included the below tran[http://karmakom.ru/en_us/documents/112018
Click or tap to follow link.]
account ending in 8400 for y

Download transaction details

The link points to a phishing server in Russia

*The danger is in the document which will be download if you click on the link. In this particular case, it is a document with embedded macros that will install malware on your computer to steal personal information. Normally macros in Microsoft Word are disabled by default, but if you have enabled them for legitimate reasons then there would be a danger to your computer if you attempt to open the attached document.*

*These phishing scams are sent out to many university email addresses at the same time, so you are not personally being targeted by the phishers. These attacks will continue in various forms, because there are still individuals who fall for these scams, making phishing attacks very profitable.*

*If you do receive mail like this then please report it to IT Cyber Security. Once you have reported the spam or phishing mail, you can delete it immediately. You can do this in two ways:*

1. ***By reporting it on the ICT Partner Portal.** Go to https://servicedesk.sun.ac.za and select "**Report phishing, spam and malware**" right at the bottom of the list. Fill in your information and add the email as an attachment. Your request will automatically be logged on the system.*
2. ***By sending an email**.*
   *- Start up a new mail addressed to csirt@sun.ac.za.*
   *- Use the Title "SPAM" (without quotes) in the Subject.*
   *- 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.*
   *- Send the mail.*

*[Article by David Wiles]*

*Posted in:Phishing,Security | Tagged:Phishing,Report Phishing | With 0 comments*