

INFORMASIE TECHNOLOGIE

INFORMATION TECHNOLOGY

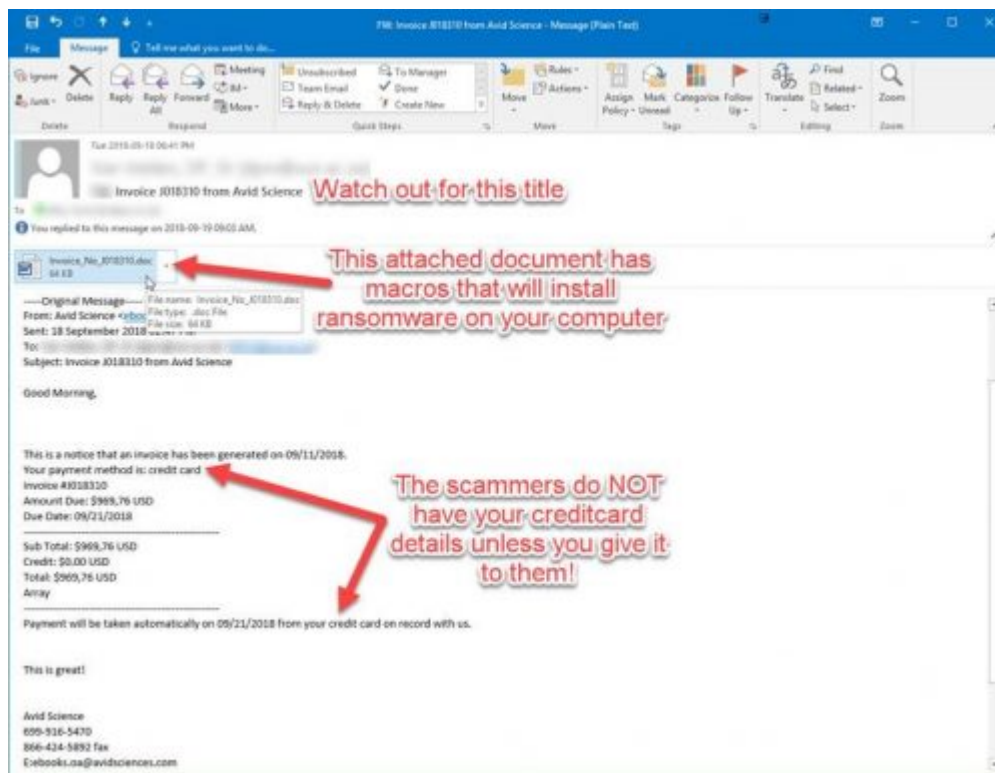
WARNING: PHISHING SCAMS WITH FAKE INVOICES

The nature of the university as an academic institution means that goods like books and academic journals are purchased by staff.

Phishing scammers will often exploit these purchases by either spoofing the e-mail addresses of well-known publishers or sending "invoices" that are infected with malware to fool people into divulging personal details like passwords and bank account details, or more seriously, infecting their victim's computers with ransomware which encrypts the contents of the hard drive and demands a ransom to unlock access to the encrypted files.

Last week several colleagues reported that they were getting invoices from a journal publisher for books they allegedly purchased. An invoice for books purchased is usually attached.

Here is an example of the phishing scam:



Please keep an eye open for this threat over the next few days. We have been reading reports of a drastic increase in the incidents of ransomware infections targeting large institutions like universities. Keep on your toes, these criminals will never stop trying, because they catch their victims from the university so easily. Don't become a victim. Fight them by reporting these scams to the IT CyberSecurity Team, and by spreading the news to your colleagues and classmates.

If you have received mail that looks like this please immediately report it to the Information Technology Security Team

using the following method: (especially if it comes from a university address) Once you have reported it, delete it or put it in your Junk Mail folder.

1. Start up a new mail addressed to csirt@sun.ac.za, cc sysadm@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](#), [Phishing](#), [Security](#) | Tagged: [Phishing](#) | With 0 comments