

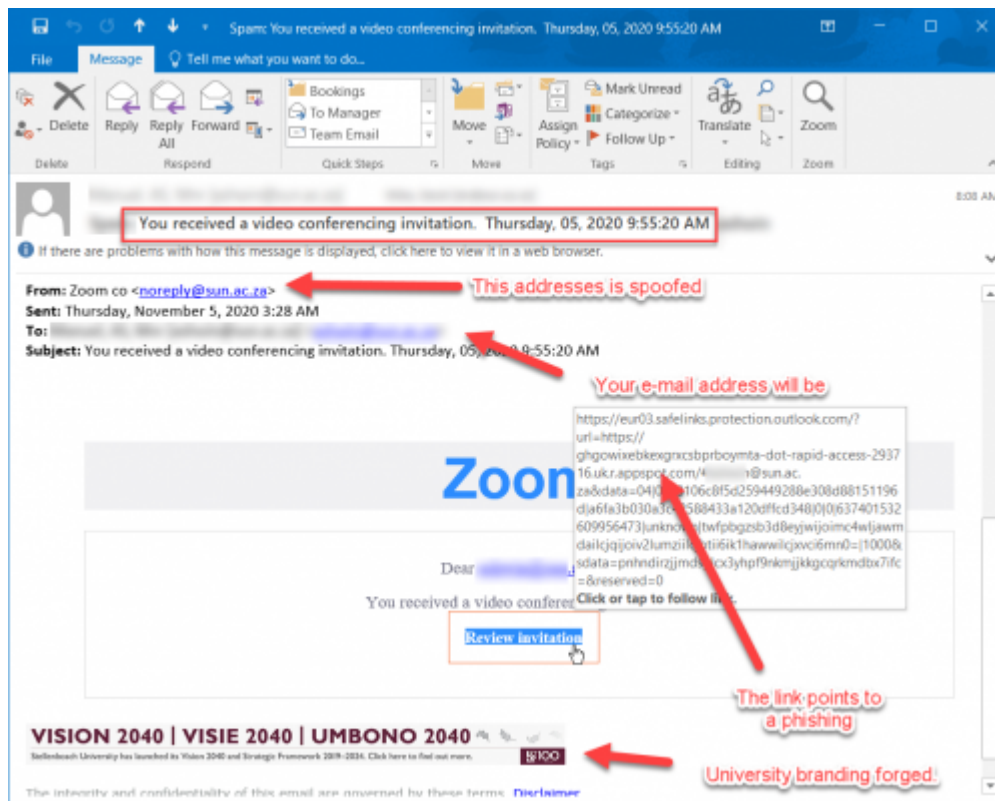
INFORMASIE TECHNOLOGIE

INFORMATION TECHNOLOGY

PHISHING ALERT: ZOOM INVITE

Please be on the lookout for a new tactic that phishing scammers are employing to get your personal details, passwords and to gain access to your university account.

These scammers are using "Zoom" video conference invitations to fool their intended victims and steal passwords and other personal details.



Above is one such example. Take note of the highlighted the warning signs that reveal the scam. This particular scam is "custom" programmed for specific university e-mail addresses and might target your address, as the e-mail addresses are embedded into the phishing web page and the e-mail itself.

If you do get such an e-mail please report it to IT Cyber Security as soon as possible on the [ICT Partner Portal](#).

If you have accidentally responded to the phisher and already provided them with your personal details, it is vitally important that you immediately change your password. Make sure the new password is completely different, and is a strong password that will not be easily guessed, as well as changing the passwords on your social media and private e-mail accounts, especially if you use the same passwords on these accounts.

After changing your password, also log a request on the ICT Partner Portal in order for your devices to be checked for malicious software.

[ARTICLE BY DAVID WILES]

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