# Be vigilant against email scams

With the lockdown leading to business being run almost exclusively on email, fraudsters are increasingly using email-based scams to catch unsuspecting businesses off-guard.

Image by antonynjoro from Pixabay

“One of the most common email scams that businesses fall victim to is Business Email Compromise (BEC). Business Email Compromise is a global phenomenon and a form of cybercrime which uses email fraud/email phishing to target businesses, individuals and governments. At its core, the scam leverages digital technology combined with social engineering techniques,” says Nadiah Maharaj, chief risk officer at FNB Business.

The scam can be carried out in multiple ways:

- It is common for fraudsters to use malware to compromise (gain unauthorized access) to a business’ email account and to then send emails to that business’s clients (debtors) advising them of a change in the business’ banking details.

- A business can also receive an e-mail informing them that their supplier has changed their bank account details. The correspondence will include the details of the new account. The business is then requested to make future payments into the new account. The details are, of course, fraudulent with the consequence that monies are paid to the fraudster and not the legitimate supplier.

- Fraudsters can also phone the victims informing them of the change of details and that an email will follow. The telephone call will be used by the fraudster so that they can extract more information to make their communications more believable (also known as social engineering).
- Criminals would typically target specific employee roles within an organisation, by sending a spoofed email with instructions that purport to be from a senior party normally the CEO or similar, to affect urgent payments.

## Steps to keep protected

Business can take the following steps to ensure that they don't fall victim to this type of fraud:

- Make sure your PC/Laptop is current with OS updates and anti-virus/malware software.
- If you are contacted by a 'supplier', ask to speak to your known contacts and do not take instructions from staff at the supplier who are not known to you. Ensure that any request to change banking details is properly confirmed with that known contact and using contact details you have sourced yourself.
- Beware of supposed confirmatory e-mails from almost identical e-mail addresses, such as .com instead of .co.za, or addresses that differ from the genuine one by perhaps one letter that can be easily missed example an "I" instead of "J".
- Make use of the "Account Owner Verification" tab on Online Banking to test that the name of the account accords with the account number provided.
- Urgent and unplanned payment instructions should be treated with caution. Sensitise staff to this modus operandi and instruct them to scrutinise invoices for irregularities prior to any payment and escalate suspicions.
- Ensure that your company's private information is not disclosed to third parties who are not entitled to receive it, or third parties whose identities cannot be rightfully verified.
- Don't use public computers or unsecured network connections to check e-mail; there's virtually no way to know if they are infected with malware accidentally or have key logging spyware installed intentionally.

Businesses who have fallen victim to this type of fraud, should contact their bank immediately to be assisted to stop any payments if possible, as a matter of urgency.

The fraud should also be reported to the South African Police Services (SAPS). Banks will provide the SAPS with the relevant information, upon receipt of a duly served subpoena. If the fraudster has benefited from the fraud, business can further consider civil recovery and also check with their insurer if it is an insurable loss.

"This National Cybersecurity Awareness Month, we urge all business owners to educate themselves about cybercrime and commit to staying alert and vigilant" concludes Maharaj.