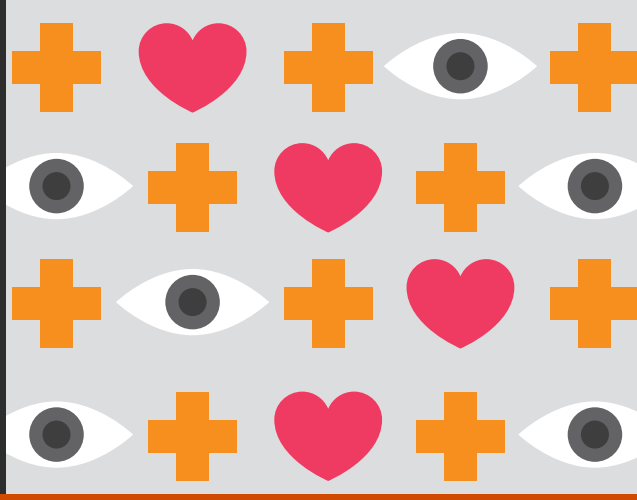
# Cybercrime Alert:

November 2019



## Appearances ARE deceiving!

## Business email compromise – The million Rand threat

### What you need to know?

- An increasing number of **South African** companies have fallen victim to business email compromise (BEC) in the last quarter. Attacks are affecting all sectors.
- We have however noted an increase in attacks on clients in the **mining sector** in the last quarter.
- Recent investigations indicate that cloud-based email platforms in particular are being targeted.
- According to the Ombudsman for Banking Services, between 2018 and 2019 over **R10m was lost** by businesses and individuals through BEC.
- Scams are being perpetrated using **fake emails** from senior executives of the company or phony vendor emails.
- **Damages** can include both **financial** and **reputational damages**.
- Strong controls related to people, process and technology can help protect company assets.

### What is business email compromise?

Business email compromise (BEC), also known as interception/impersonation fraud, can be defined as 'a criminal act where cyber attackers illegally access an email account and communicate as if they are the user' (Sabric, 2019).

Cyber criminals gain access to an individual's business email and impersonate people who use that account (executives, senior managers or supply chain partners) in order to intercept and redirect invoices and also change banking account details to their nominated account details. They can also in some cases trick staff into authorising fraudulent transfers.

The risk is further increased where document management systems can be accessed online using the user's email credentials. Attackers have been observed garnering further intelligence in order to shape their attack by trawling through debtor information on these portals.

### Modus operandi observed

Recently, we have observed attacks on email portals aimed at compromising email accounts. Previously attacks were carried out using fake email accounts to impersonate individuals. This trend has changed in that attackers compromise the legitimate email accounts of staff members. Below is the step-by-step process that we have observed in the last quarter of 2019:

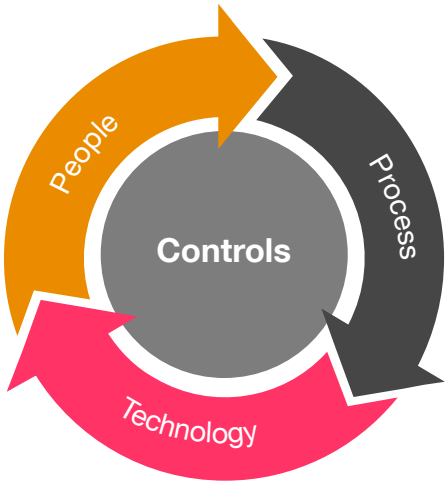
- Employees to be targeted are identified by the attackers.
- Attacks are launched against email platforms in order to compromise user credentials.
- Once targeted mailboxes are compromised, mailbox rulesets are altered to move incoming emails with specific criteria, i.e. a particular client's name or email address, to different folders and mark them as 'Read'.
- In some instances, where document management systems were available online, using similar credentials, attackers garnered further information regarding third parties to interact with. The focus was primarily on third parties with outstanding payments.
- Additional rules are created to redirect incoming emails to the fraudulent email addresses.
- Fake invoices are then generated by the fraudulent parties and attackers interact with clients or third parties using the compromised mailboxes in order to secure payment into their bank accounts.

pwc

Technological controls, process enhancements and the training of employees can protect against these scams

## Prevention is key!

Once funds have been transferred, recovering the stolen funds may be possible if detected early enough, often only with the help of law enforcement. Sound IT controls can help stop these scams in their tracks, such as:




- Cybersecurity awareness training for employees, in order to create awareness about social engineering attacks, strong passwords, safe online browsing, etc.

- Ensure that there is effective monitoring of alerts being generated from platforms;
- Further alerts should be created when rules are created on mailboxes;
- Implement two-factor authentication for external email and document management access;
- Ensure that IT staff receive training for new platforms deployed and understand the alerts being generated; and
- Enable account lockout for failed login attempts.

- Develop policies and procedures that include inherent checks and balances and multiple approvals for electronic transfers;
- Require the receiver of a payment request to confirm its validity;
- Any unplanned/urgent payment requests should be questioned; and
- Changes to beneficiary account details should be verified through legitimate channels.

## What to do if you suspect your organisation has been scammed

- Contact your local law enforcement agency immediately to report the matter.
- Contact both your financial institution and the receiving financial institution to request that they stop or reverse the transfer.
- Ensure that first responders obtain and store evidence in a digitally sound manner.
- Seek advice from counsel about any legal obligations or protective measures, such as insurance coverage for any loss. In parallel, evidence should be secured. This includes the fraudulent communications and logs which are critical to investigating these matters.
- Ensure that employees are aware of the scam, how it is being perpetrated, and that they could be a gateway for the scammer.
- Finally, enhance controls to minimise the risk of falling victim to these types of attacks.

**Sources:**

- South African Risk Information Centre (SABRIC) – https://www.sabric.co.za
- Ombudsman for Banking Services (OBS) – www.obssa.co.za

## How can PwC help?

To have a deeper discussion about how to protect against or investigate digital compromises, please contact the PwC Forensic Technology Solutions team:

**Junaid Amra:**
Mobile: +27 (0) 82 953 9325
Email: junaid.amra@pwc.com

**Solomon Bhala**
Mobile +27 (0) 65 970 6189
Email: solomon.bhala.za@pwc.com

**Trishee Jobraj**
Mobile: +27 (0) 82 370 9409
Email: trishee.jobraj@pwc.com

For more information visit our webpage: www.pwc.co.za