TIPS FOR BUSINESSES TO MINIMISE BUSINESS EMAIL COMPROMISES

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Kelly Lekaise | March 10, 2023

Cyber attacks are on the rise. An example of this is the recent judgement of Hawarden v Edward Nathan Sonnenbergs Inc ("**ENS Africa**"). In this matter, Judith Hawarden purchased immovable property and appointed ENS Africa as the conveyancer. Hawarden received an email from ENS Africa enclosing its bank account details in a PDF[1] to which she made the payment of R5 500 000. Unbeknown to the parties, the email had been intercepted and the banking details altered on the PDF. Hawarden then made payment using the altered banking details from a forged email address.

The evidence at trial established that the ENS Africa was aware of the risks of cyber attacks such as

email and PDF manipulation but failed to warn Hawarden. The court further established that ENS Africa had control over the way in which it conveyed its bank account details but chose to do so in an unprotected PDF attachment via email. The court held that ENS Africa chose this method even though were safer methods of communicating its bank details. The court found in favour of Hawarden and ordered ENS Africa to pay the amount of R5 500 000 to Hawarden. In light of this, here are several tips to avoid falling prey to such scams:

Check the email address.

- This one is particularly for the person making the payment. When a payment request is made via email, it is prudent to check that the email address has not been tempered with. In the Hawarden matter, the email address enclosing the payment details was from an "ensafirca "address, a misspelling of ensafrica. Being vigilant can help one spot such fraudulent tactics.
- Follow up an email payment requisition with an in-person confirmation or telephone call to the sender to confirm the contents of the email and the banking details.

Avoid sharing personal information.

- Hackers can use the smallest piece of information such as a name to gain access to company systems. For example, if a hacker calls to find out who is in charge of finances, and reception tells them it is John Doe, the hacker has sufficient information to create an email address using a name which can be used to target clients. Having a generic email address for finance related queries may mitigate this risk.

Create awareness.

- The Hawarden case highlights that a conveyancer owes their client a duty of care. Thus, it is important that organisations who use email for invoicing purposes, inform their clients to be vigilant, and facilitate a secure and safe way of processing payments from clients. Companies can bring to the attention of clients, through a banner on their email, the risk of email compromises. This can serve as a reminder to always call to verify the banking details of the sender. Where a large amount is involved, companies should have a direct conversation with client regarding email verification and confirmation of banking details.

Secure company systems

- Use email encryption, multi-factor authentication for email accounts, and send sensitive emails over a secure VPN.
- Update your email applications to the latest version. This is to ensure that your applications are equipped with the latest security updates on offer.
- Invest in antivirus software and firewalls. This is to ensure that your devices and networks are secured.

Cybersecurity insurance

- In the event of a cyberattack, your business might have to deal with the high costs of the cyber attack. Although your cyber insurance might not cover instances such as the above scenario, repairs and upgrades to hardware and software, data recovery, and other damages may be covered by your policy.

Cyberattacks are becoming more common and businesses should no longer just rely on emails to send banking details. It is therefore important for businesses to implement appropriate measures to minimise the risk of falling prey to cyber-attacks.

Contact us for more good, clear, precise advice.

---

[1] PDF stands for Portable Document Format.