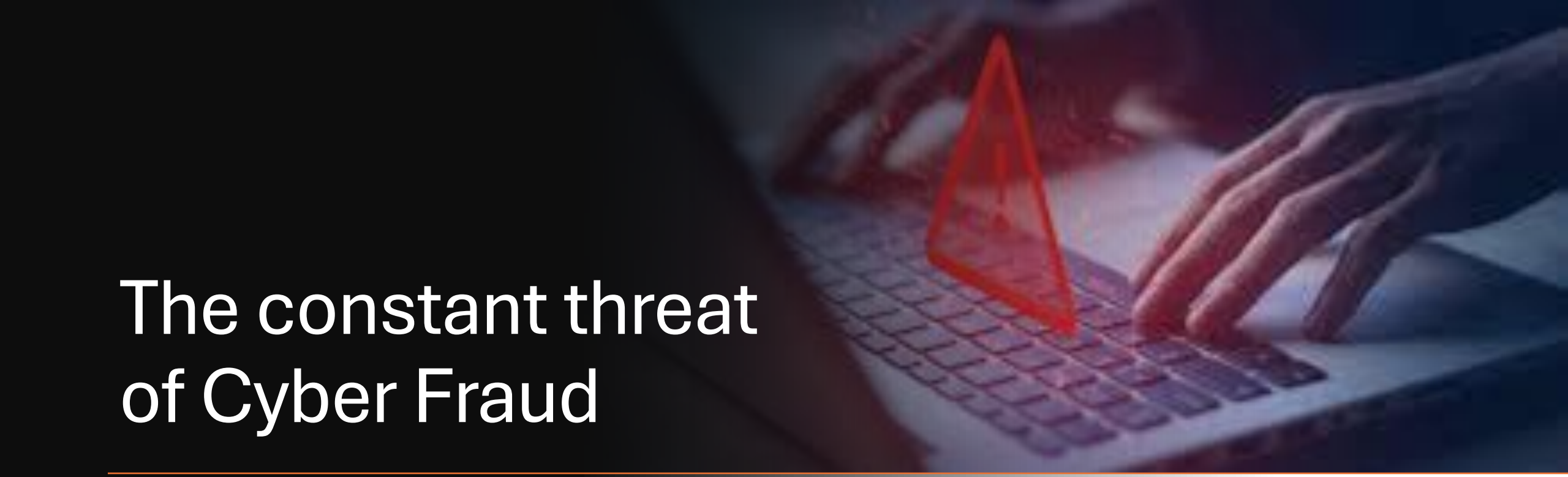


The constant threat of Cyber Fraud

September 2024

Bellingan Muller Hanekom Inc

John Havemann

Electronic Commerce and -Trade creates the opportunity for predatory Cyber Criminals to exploit members of society.

Historical Overview

Phishing:

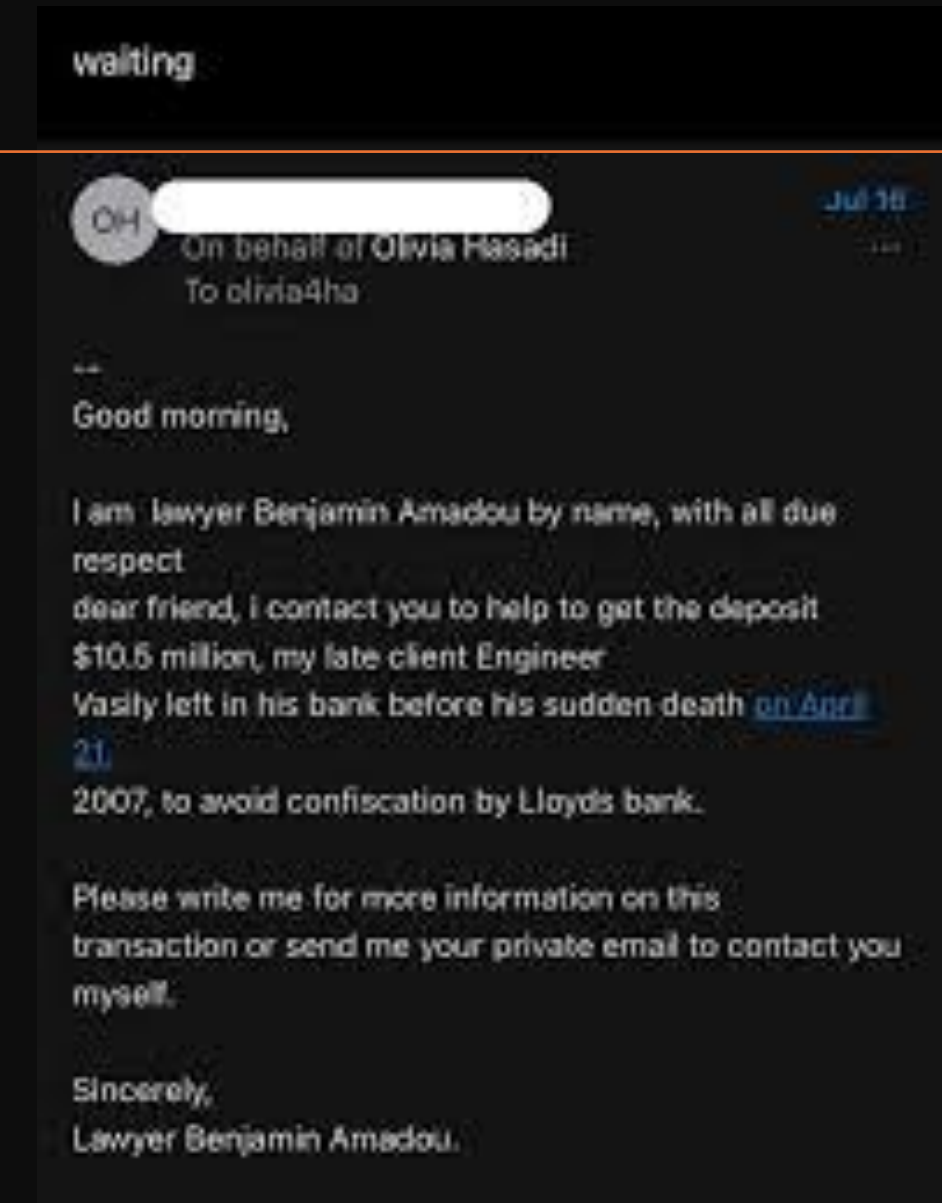
a) Phishing is the practice of sending fraudulent communications that appear to come from a legitimate and reputable source, usually through email and text messaging. The attacker's goal is to steal money, gain access to sensitive data and login information, or to install malware on the victim's device.

b) The classic approach is a third party requesting the payment of an amount to “release” funds held and/or frozen by a Reserve Bank or other government institution. The return on investment or motivation for the victim to oblige, would be to share in the spoils of the funds when they are released.

c) Common Narratives:

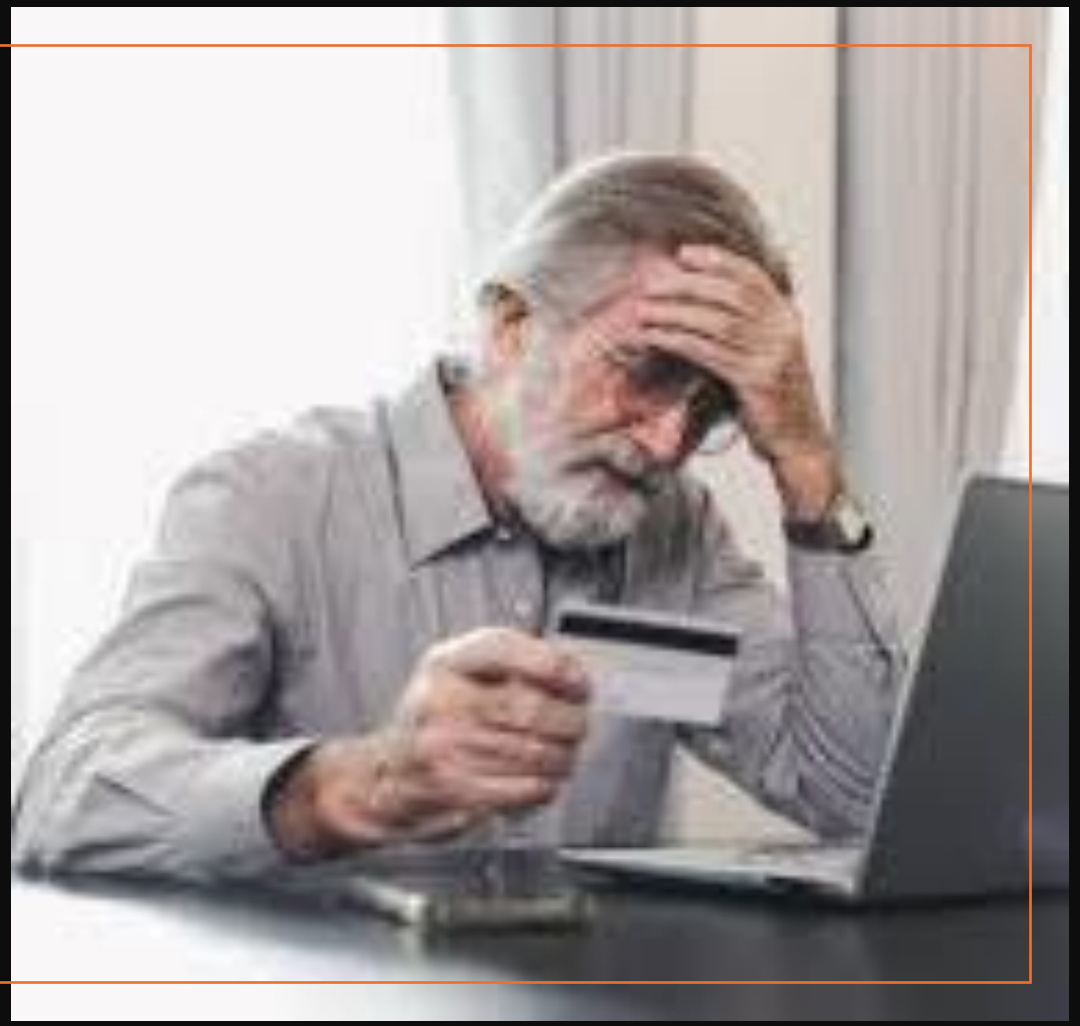
i. *“Surprise, you are the heir of a massive inheritance left to you by a family member you never knew existed”*

ii. *“I am a Prince of a war-torn country who inherited Millions. I am trying to move the Funds into South Africa, but the funds are being frozen by the SARB. It is going to cost R25 000 to release the funds. If you help, I will share the inheritance with you”*



What happens Next?

1. Funds are stolen.
2. Your computer is hacked, and sensitive information is now at the disposal of the attacker for future fraudulent activity.
3. Identity Theft.
4. Standard Insurance policies do not yet provide for private victims of cyber fraud.



Business Email Compromises (BEC)
Edward Nathan Sonnenbergs(ENS) v Hawarden

Background

- While purchasing a property for R6000 000,00, Hawarden experienced a business email compromise (BEC).
- An unrelated 3rd party (a Cyber Criminal) intercepted communications between Hawarden and ENS, who were appointed to tend to the Transfer of the property she had bought.
- The cyber criminal forged a letter from ENS and presented it to Hawarden for payment of the balance purchase price of R5 500 000,00.
- Hawarden complied and unknowingly deposited the funds into an unrelated account.
- The bank was unable to retrieve the funds as the money had been withdrawn.
- Hawarden issued Summons Against ENS for restoration.

Gauteng Division of the High Court, Johannesburg
Court *a quo* (Court of First Instance)

- JHB High Court found in favor of Hawarden
- Court held that the attorneys did not apply the necessary duty of care in educating the parties in respect of the risk, workings and implications of Cyber Fraud.

- Supreme Court of Appeal in Bloemfontein overturns the order.
- Factors taken into account:
  - ENS and Hawarden were not in an attorney-client relationship.
  - Estate Agent forewarned Hawarden on the risks of Cyber Fraud and Hawarden and she failed to verify the accounting details with ENS before making payment.
  - Hawarden's emails were breached.
  - Untenable for ENS to take further steps.
  - By finding in favor of the Plaintiff, the concern of imposing a legal duty on all other creditors that send banking details via email.
  - A further concern is that the legal duty would require entities to *"mitigate against risk outside of their realm of control"*.

Important Outtakes

1. It is clear that all relevant facts will be considered in determining liability in any given case and there is no clear formula for determining this of yet.
2. Prevention is the best outcome.
3. It is important for all parties to do as much as they can to educate their clients or other roll players on the risks of Cyber Fraud.
4. Usage of encrypted communications with multiple steps of authentication have already been implemented by most Financial Service Providers.
5. Registration as public pre-loaded beneficiaries for payment will also alleviate the risk of interception as creditors will alert clients that banking details are not exchanged electronically.