HIGH COURT HACKING JUDGMENT SHIFTS THE ODDS IN GOGO DLAMINI'S FAVOUR

Category: Privacy Law and POPIA,Privacy Law, Infosec, and POPIA,Technology Law
written by Lucien Pierce | March 10, 2023

Introduction

A Johannesburg High Court judgment, in an acrimonious cybercrime-related dispute between Africa's largest law firm and a retired senior citizen, has tipped the scales in favour of the proverbial "Gogo Dlamini." For those who do not know, in South Africa Gogo (meaning Granny) Dlamini is the proverbial less powerful individual who has to face up to those who have immense power and resources.

In this case, a retiree – Ms. Judith Hawarden – approached law firm – Edward Nathan Sonnenbergs (ENSafrica) – to act as her conveyancer for a house she wanted to buy. Unfortunately, Ms. Hawarden's email account was hacked. This allowed the hackers to intercept emails from ENSafrica. Some of these emails had ENSafrica's banking details in a type of document called a PDF. PDF documents, especially if they are unprotected, are easy to manipulate. This type of crime is called a business email compromise or BEC.

This is exactly what the criminals did: they took a PDF document, changed ENSafrica's banking details and inserted their own. Ms. Hawarden then paid R5.5 million into what she believed was ENSafrica's bank account. She then discovered what had happened but, by then, the hackers had withdrawn all the money. After a complex and very technical court case, the judge ruled that ENSafrica could have and should have done much more to improve its own internal information technology security and processes. The court also said that it had a responsibility towards Ms. Hawarden and should have done more to protect her interests.

Why Is This Judgment So Important?

It is significant because if global, highly secure technology companies can fall prey to hackers, what about you, me or Gogo Dlamini? As an example, both Google and Facebook lost over US$100 million to a fraudster using a similar technique. All the cyber-fraudster did was create fake, but convincing, email addresses that were similar to Facebook's and Google's real supplier and then sent false

invoices with the fraudster's banking details. Google and Facebook fell for it.

If Google and Facebook fell for it, what chance do you, me or Gogo Dlamini have? It has become relatively common for large organisations to blame their customers for hacking incidents where the customer or client loses money. The customer is typically accused of not having kept passwords or PINs secure or of having fallen for phishing emails which gave hackers access to the customer's email accounts.

Who Are The Targets Of Hackers?

There are many avenues for hackers and criminals to target unsuspecting victims. These hackers often rely on information they have obtained elsewhere. They are patient and stealthy and use this information to convince their victim to let their guard down. There's an old saying: the most effective lie is always the closest to the truth. The cyber-fraudsters will create a story that is very believable and often based on a true set of circumstances that the victim may have experienced.

Consider these scenarios: hackers may get access to police records on stolen vehicles. If they are able to confirm that a stolen vehicle is insured, they know there is a possibility of the vehicle theft victim getting an insurance pay-out. If they are able to get access to the vehicle theft victim's email account (something that is quite common), they are in a strong position. If the insurer sends the victim a loss/claim agreement, the hackers are able to intercept it change the banking details on the agreement and other documents and send it back to the insurer. The insurer then pays out the claim into the hackers account. There are many variations to this: a lawyer paying out an inheritance; a pension fund paying out a lump sum at retirement; a financial services provider paying out a long term investment. In each of these instances, the organisation is likely to push the blame for the loss onto the individual saying: "You allowed your email account to be hacked" or "You must have given your one-time password (OTP) to the perpetrator".

Conclusion

As anyone knows, taking on a large well-resourced organisation that has a good litigation budget, is a huge challenge. It can be both mentally and financially taxing: some victims just accept the knock and walk away. But, with Ms Hawarden's success, South Africa's courts have stepped in to protect you, me and Gogo Dlamini. The court accepted that "*individuals in society are generally not well placed to respond to the ever-evolving threat of cyber-crime.*" The court recognised that where someone is in a better position to prevent something from going wrong, that person should bear responsibility. It said, "*where one of two innocent parties has to suffer a loss arising from the misconduct of a third party it is for the public advantage that the loss should fall…on that one of the two who could most easily have prevented the happening or the recurrence of the mischief*."

Any insurer, financial service provider, accounting or law firm, in fact almost any organisation that relies on paying or receiving funds, should be urgently considering how it interacts with those who it pays to or receives money from. Even though each case will be decided on its own facts, you, me and Gogo Dlamini are in an immensely stronger position to take on big organisations if they do not do their part to help us avoid becoming victims of this type of cybercrime.

Contact us for more good, clear, precise advice.