28 AUGUST 2019

DISPUTE RESOLUTION
CORPORATE INVESTIGATIONS
ALERT

IN THIS **ISSUE**

Do not take the bait! There might be a cybercriminal on the other end of the line

Many South Africans can attest to receiving an email containing a seemingly plausible story promising instant riches and involving large amounts of money, which the sender promises to send only if he or she receives help with some initial costs.

Electricity supply cannot be restored by way of a *mandament van spolie*

Spoliation refers to the unlawful deprivation of a party's right of possession. The remedy for such deprivation is a spoliation order or, by another name, the *mandament van spolie*. When it comes to the dispossession of a party's right of possession of movable or immovable property, South Africa's law on spoliation orders is long settled.

CDH
CLIFFE DEKKER HOFMEYR

CLICK HERE

For more insight into our expertise and services

Do not take the bait! There might be a cybercriminal on the other end of the line

Phishing has remained a persistent problem because of the human element: people are inadequately prepared or trained to identify and prevent against becoming victims of phishing scams.

Many South Africans can attest to receiving an email containing a seemingly plausible story promising instant riches and involving large amounts of money, which the sender promises to send only if he or she receives help with some initial costs.

This is the familiar tale of the notorious 419 scams of which most people are aware. Cybercrime has, however, evolved over the years with the significant emergence of malware attacks, ransomware attacks, hacking, spamming and phishing.

Spamming and phishing are two very common forms of cybercrimes mainly because email is still the most common way to perpetrate a cyber-attack. Significant reliance on email communication has also made both individuals and organisations vulnerable. 91% of cybercrime attacks are initiated via email, whilst 88% of South African organisations have experienced a phishing attack in the last 12 months. This is according to the Mimecast State of Email Security 2019 Report. Phishing has, however, remained a persistent problem because of the human element: people are inadequately prepared or trained to identify and prevent against becoming victims of phishing scams.

Phishing is a type of social engineered cybercrime which tricks people into divulging their personal information.

Phishing occurs when an email is sent to a person by a cybercriminal who is pretending to be a legitimate source. The goal is to mislead the email recipient into believing that the message contains information that he or she requires. There are different types of phishing attacks and it can occur in one of the following ways:

- Bulk-phishing: where the attack is not specifically targeted or tailored toward one recipient;
- Spear-phishing: where the attack is targeted at specific individuals or companies and tailored accordingly;
- Clone-phishing: where the cybercriminal takes a legitimate email containing an attachment or link, and replaces it with the incorrect details; and
- Whaling: when the phishing attack is specifically targeted towards high-value individuals in senior positions in companies.

There are also variations of phishing attacks such as smishing, which is a form of phishing where a cybercriminal sends malicious SMS text and social media messages to obtain valuable information. Smishing is becoming a popular cybercrime as people tend to open text messages more often than emails. Phishing can also occur in the form of a telephone call or voice message purporting to be from a reputable institution such as a bank. This is called vishing.

Do not take the bait! There might be a cybercriminal on the other end of the line...*continued*

Cybercriminals are intimately familiar with how corporate email users interact with the internet and they are constantly evolving their techniques to trick users in order to obtain information.

Despite the cliché names given to these malicious attacks, phishing should not be trivialised. Cybercriminals are no longer just targeting individuals, but organisations are also being affected with elaborate attacks to access company data, intellectual property, senior executive's e-mails or any other sensitive information. Phishing can result in the loss of sensitive data which can ultimately affect a business's revenue or brand. Individuals and organisations need to be aware of these various types of phishing attacks. The cardinal rule when it comes to preventing cyber-attacks is to be sensitised to cyber risks.

Red flags which could indicate a phishing attempt include emails or text messages that suggest urgency or a limited time to respond, spelling errors or bad grammar, an unusual sender or an unexpected message. Individuals should also be weary of being asked to provide personal details such as a banking password over the telephone or email as well as avoid installing or updating mobile apps from links received in a text message.

In order to not take the bait, if an email or text message which resembles the features that are described above is received, the best response would be to delete the email or text message and/or contact available technical support. Most importantly, where there is doubt about the authenticity of the message, it would be prudent to independently contact the purported sender to verify the contents thereof by using a known contact number. The contact details contained in the email or message should not be used as cybercriminals have in many cases resorted to providing 'fake' contact numbers so they can deal with the queries should the victim try to verify the information, thus making the entire scenario appear to be legitimate.

Cybercriminals are intimately familiar with how corporate email users interact with the internet and they are constantly evolving their techniques to trick users in order to obtain information. This is why individuals in their private capacity and individuals in their capacity as employees need adequate cyber security awareness training. Lack of adequate cybersecurity measures also contributes to the risk of a phishing attack or another cyber attack on organisations and individuals. Organisations need to devote resources to implement effective cybersecurity measures and risk management controls. These measures should include

Do not take the bait! There might be a cybercriminal on the other end of the line...*continued*

The cost of preventative measures outweighs the cost of falling victim to a cyber-attack.

keeping system software updated, implementing endpoint protection, using secure internet connections as well as securing web browsing and emails. These measures are also available for individuals for personal computers and for mobile phones. In addition to technical measures, organisations and individuals may also consider obtaining cyber liability insurance. Cyber liability coverage can help to cover the costs related to the effects and consequences of a cyberattack. The cost of preventative measures outweighs the cost of falling victim to a cyber-attack.

Individuals and organisation need to take a proactive approach to protect against the loss of personal and business data. Both groups must invest time and resources to adequately address the fact that cybercriminals continue to exploit the human element. This can be done by receiving training on how to not only to recognize a phishing attack, but to also respond appropriately to such threats. As the old adage goes, prevention is better than cure. In the case of cybercrime, prevention is also the first line of defence against falling victim to cyberattacks.

Zaakir Mohamed and Refiwe Makhema

CDH
CLIFFE DEKKER HOFMEYR

Electricity supply cannot be restored by way of a *mandament van spolie*

The Court was called upon to decide whether Masinda was entitled to a spoliation order after Eskom had disconnected the supply of electricity to Masinda's immovable property.

Spoliation refers to the unlawful deprivation of a party's right of possession. The remedy for such deprivation is a spoliation order or, by another name, the *mandament van spolie*. When it comes to the dispossession of a party's right of possession of movable or immovable property, South Africa's law on spoliation orders is long settled. It has been established in recent judgments that the remedy can also be extended to certain incorporeal rights, which relate to intangible property. In this regard our courts have recently had to grapple with the following question: Can a party that owns or is in possession of an immovable property rely on a spoliation order when another party disconnects the supply of electricity or water?

In *Eskom Holdings SOC Limited v Masinda* [2019] ZASCA 98 the Supreme Court of Appeal (SCA) dealt with this issue. The Court was called upon to decide whether Masinda was entitled to a spoliation order after Eskom had disconnected the supply of electricity to Masinda's immovable property. In this case Masinda obtained a final order from the High Court directing Eskom to reconnect the electricity supply to her property.

Eskom appealed the final order to the SCA contending that the connection made from its grid to Masinda's property was illegal and a danger to the public and, for this reason, it had acted lawfully in disconnecting the supply. In response, Masinda argued that, as in spoliation proceedings, the legality or otherwise of an applicant's possession is not an issue to be decided - the supply had to be reconnected before any dispute as to its legality could be determined.

The SCA undertook an examination of the principles applicable to the *mandament* and held that although the remedy originally protected only physical or immovable property, this protection was extended in *Telkom v Xsinet* [2003] ZASCA 35 to quasi-possession of certain incorporeal rights such as rights of use or those of servitude. The Court emphasised that not all incorporeal rights may be the subject of spoliation.

The Court also cited *Impala Water Users Association v Lourens NO & Others* 2008 (2) SA 495 (SCA) which stands as authority that the mere existence of a terminated water supply is insufficient in itself to constitute an incident of possession of the property (the water supply) and that more than a personal right/contractual right is required for the afforded protection under the *mandament*.

The SCA held that in order to justify a spoliation order in the case of an incorporeal right, the right must be of such a nature that it vests in the person in possession of the property (water, electricity, right of way, as the case may be) as an incident of their possession such as rights bestowed by servitudes, registration or statute.

CDH
CLIFFE DEKKER HOFMEYR

Electricity supply cannot be restored by way of a *mandament van spolie*...continued

The SCA emphasised that rights that flow from a contractual nexus between parties are insufficient as they are purely personal, and, in such a case, this would reduce a spoliation order to an order of specific performance in the proceedings.

The SCA emphasised that rights that flow from a contractual nexus between parties are insufficient as they are purely personal, and, in such a case, this would reduce a spoliation order to an order of specific performance in the proceedings.

In applying these principles to *Masinda*, the Court considered the nature of the Masinda's right to the electricity, which was purchased through the prepaid system, finding that her right to receive the prepaid electricity was a personal right flowing from the sale and that it did not flow from the possession of the property. The Court stated that Masinda relied solely on the existence of the electrical supply to justify the spoliation order, which was insufficient to establish her right to a spoliation order. Eskom's appeal was upheld with costs and the order of the High Court was set aside.

Litigants seeking to restore possession of a personal right which flows from a contract should compel specific performance as a remedy in order to resolve the contractual dispute.

Mongezi Mpahlwa and Johanna Lubuma

OUR TEAM

For more information about our Dispute Resolution practice and services, please contact:

Tim Fletcher
National Practice Head
Director
T +27 (0)11 562 1061
E tim.fletcher@cdhlegal.com

Thabile Fuhrmann
Chairperson
Director
T +27 (0)11 562 1331
E thabile.fuhrmann@cdhlegal.com

Timothy Baker
Director
T +27 (0)21 481 6308
E timothy.baker@cdhlegal.com

Eugene Bester
Director
T +27 (0)11 562 1173
E eugene.bester@cdhlegal.com

Lionel Egypt
Director
T +27 (0)21 481 6400
E lionel.egypt@cdhlegal.com

Jackwell Feris
Director
T +27 (0)11 562 1825
E jackwell.feris@cdhlegal.com

Anja Hofmeyr
Director
T +27 (0)11 562 1129
E anja.hofmeyr@cdhlegal.com

Julian Jones
Director
T +27 (0)11 562 1189
E julian.jones@cdhlegal.com

Tobie Jordaan
Director
T +27 (0)11 562 1356
E tobie.jordaan@cdhlegal.com

Corné Lewis
Director
T +27 (0)11 562 1042
E corne.lewis@cdhlegal.com

Richard Marcus
Director
T +27 (0)21 481 6396
E richard.marcus@cdhlegal.com

Burton Meyer
Director
T +27 (0)11 562 1056
E burton.meyer@cdhlegal.com

Zaakir Mohamed
Director
T +27 (0)11 562 1094
E zaakir.mohamed@cdhlegal.com

Rishaban Moodley
Director
T +27 (0)11 562 1666
E rishaban.moodley@cdhlegal.com

Mongezi Mpahlwa
Director
T +27 (0)11 562 1476
E mongezi.mpahlwa@cdhlegal.com

Kgosi Nkaiseng
Director
T +27 (0)11 562 1864
E kgosi.nkaiseng@cdhlegal.com

Byron O'Connor
Director
T +27 (0)11 562 1140
E byron.oconnor@cdhlegal.com

Ashley Pillay
Director
T +27 (0)21 481 6348
E ashley.pillay@cdhlegal.com

Lucinde Rhoodie
Director
T +27 (0)21 405 6080
E lucinde.rhoodie@cdhlegal.com

Belinda Scriba
Director
T +27 (0)21 405 6139
E belinda.scriba@cdhlegal.com

Tim Smit
Director
T +27 (0)11 562 1085
E tim.smit@cdhlegal.com

Willie van Wyk
Director
T +27 (0)11 562 1057
E willie.vanwyk@cdhlegal.com

Joe Whittle
Director
T +27 (0)11 562 1138
E joe.whittle@cdhlegal.com

Roy Barendse
Executive Consultant
T +27 (0)21 405 6177
E roy.barendse@cdhlegal.com

Pieter Conradie
Executive Consultant
T +27 (0)11 562 1071
E pieter.conradie@cdhlegal.com

Willem Janse van Rensburg
Executive Consultant
T +27 (0)11 562 1110
E willem.jansevanrensburg@cdhlegal.com

Nick Muller
Executive Consultant
T +27 (0)21 481 6385
E nick.muller@cdhlegal.com

Jonathan Witts-Hewinson
Executive Consultant
T +27 (0)11 562 1146
E witts@cdhlegal.com

JOHANNESBURG
1 Protea Place, Sandton, Johannesburg, 2196. Private Bag X40, Benmore, 2010, South Africa. Dx 154 Randburg and Dx 42 Johannesburg.
T +27 (0)11 562 1000 F +27 (0)11 562 1111 E jhb@cdhlegal.com

CAPE TOWN
11 Buitengracht Street, Cape Town, 8001. PO Box 695, Cape Town, 8000, South Africa. Dx 5 Cape Town.
T +27 (0)21 481 6300 F +27 (0)21 481 6388 E ctn@cdhlegal.com

STELLENBOSCH
14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.
T +27 (0)21 481 6400 E cdhstellenbosch@cdhlegal.com

CLIFFE DEKKER HOFMEYR