REGULATORY

You don't want to be counted as a victim!

5 June 2019 *6 min read*

By Ahmore Burger-Smidt, Director, Head of Data Privacy Practice, Werksmans Advisory Services (Pty) Ltd

HOW DO THEY PHISH? DATA BREACHES AND DATA SECURITY

The loss of personal information and identity theft is indeed an area of great concern to business and also data subjects. This has been the status for years irrespective of the introduction of the Protection of Personal Information Act, 2013 ("**POPIA**") and the increased debate around cyber security and data breaches.

It was reported by Kaspersky Lab on 5 May 2019, that South Africa is experiencing a major increase in cyberattacks. It is estimated that approximately 13 842 attempted cyberattacks take place daily. This means that there are 9 cyberattack attempts in South Africa every second. This impacts organisations. The question is how.

Businesses cannot but operate electronically, storing information on databases in the cloud. Without email, they will come to a standstill. Personal information is collated at a frightening speed and data subjects often do not question why they need to disclose their information. More and more employees blur the line between their personal and work lives, which means that companies receive electronic communication not only for purposes of the business, but also emails of a personal nature. Employees also shop online from their desks and even more, join social media sites.

The ease and convenience of electronic communication and data storage has changed the way we do business. However, data subjects are placing their trust and financial security in the hands of businesses each time they submit and make available their personal information. Cybercriminals and hackers can access online communication without difficulty, this creates vulnerabilities in that cybercriminals can infiltrate company databases and illegally gain access to personal information.

The POPIA stipulates that a responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking **appropriate, reasonable technical and organisational measures. These appropriate, reasonable technical and organisational measures must be in place to prevent:**

- loss of, damage to or unauthorised destruction of personal information; and
- unlawful access to or processing of personal information.

Furthermore, in order to be deemed complaint with POPIA, a company being a responsible party, must take reasonable measures to:

- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Undoubtedly, the number of technical security measures that organisations deploy is increasing. As technical security measures are enhanced, attackers are focusing more on the weakest link in the chain and that weak link is the human factor.

Phishing is a method whereby malicious e-mails are sent by cybercriminals with the intent to gain a first point of entry into the organisation's network. Through Phishing **sensitive information is obtained** such as usernames, passwords and credit card details (indirectly money).

One might wonder why Phishing is so successful today. The reality is that employees are experiencing an "**infobesity**" through the number of emails they receive, making them less cautious to detect Phishing attempts. In addition, many employees are simply not sufficiently skeptical when it comes to receiving requests to do things like transfer funds, open attachments, or provide sensitive information.

Phishing is not always easy to identify. The following reflect forms of Phishing – and the list is long.

Source: www.phishing.org

In addition to the table above, there are also Botnets, i.e. networks of malware infected computers that give cybercriminals control of thousands of computers at once. They help to hide the cybercriminal's identity and are controlled remotely by cybercriminals, usually for financial gain or to launch attacks on websites or networks. Botnets may infect and use laptops, desktops, servers, routers, smartphones or any other network equipment to conduct malicious activity. Worse still, all computers connected to the Internet are susceptible to malware infections.

Organisations of all sizes, geographic locations and industries can fall victim to cybercrime. Facebook is clearly an apt example.

New legislation and regulations aim to hold organisations and their executives more accountable with regard to the protection of information assets and IT infrastructure. The General Data Protection Regulation ("**GDPR**") came into force on 25 May 2018 and fines of up to €20 million or four percent of annual global revenue can be imposed in terms of the GDPR. On 21 January 2019, a select panel of the French data protection authority, CNIL, which has the power to impose sanctions, fined Google €50 million following its failure to comply with the obligations provided for in the GDPR. POPIA has been partly enacted and once fully operational the Information Regulator will have access to significant powers to deal with data breaches, including imposing administrative fines.

Whether by accident or intent, many employees are often the root cause of successful cyberattacks. Employees do not understand that security is everyone's responsibility. Executives should realise that they need to hold all employees accountable for cybersecurity today.

However, employees need the tools and incentives to help them to define and address risks. New ways of work – remote access and remote work – highlights the urgent need for employee training. Training employees to think and act with security in mind cannot be ignored.

Cyberattacks and data fraud or theft are now two of the top five risks CEOs are most likely to face according to the latest World Economic Forum report on global risks.

If the lifeblood of the 4th Industrial Revolution and Digital Economy is data, digital trust constitutes the heart. Digital security dictates the level of confidence data subjects have and the extent to which they trust businesses, people, processes and technology to hold their personal information private and secure.

There is an inherent distrust amongst data subjects in the security of the Internet and IT systems.[1]

The rapid growth of personal information loss is a worrying trend. POPIA aims to hold organisations and their executives accountable for the protection of personal information and for the responsible use of customer data. In future, data breaches could add significantly to the financial impact of cyberattacks as regulators start to impose fines. The cost of business disruption, including diminished employee productivity and business process failures that happen after a cyberattack, continues to rise at a steady rate. The loss of trust will rise at an exponential rate.

Educating employees to recognise and respond to Phishing attacks is the best step towards a more secure organisation. This constitutes one of the required steps in establishing a data security defence strategy. Clearly an appropriate, reasonable technical and organisational measure as required by POPIA and an appropriate action to hold onto the trust of clients and customers, the data subjects.

[1] United Nations, Cybersecurity and Fake News to Dominate List of Concerns at Internet Governance Forum, October 2018

Ahmore Burger-Smidt

Head of Regulatory

View Profile