Cyber Attacks – Email Correspondence Risks

2 October 2019
K Erasmus
https://www.tech4law.co.za/tech-advisor/security-d91/cyber-attacks-email-correspondence-risks/

How much of the following sounds familiar:

An email from a potential new client, asking for legal advise based on the attached document, whether it be a summons, offer to purchase or other legal notice or document, entering your password to view the document or open an email with attachment and subject line “Proof of Payment” without thinking which client is due to send a P.O.P. An email from your client’s Gmail, Yahoo or Hotmail account, but with one altered letter, advising that payments are to be made into a new account as sent from futurelawfaculty@gmail.com , while your clients email address is futureslawfaculty@gmail.com. Would you pick up on the missing letter? Likewise would you pay funds from your trust account electronically to the account provided by an employee of the Legal Practitioners Development Fund upon receiving a call advising that a deposit had erroneously been paid into your trust account , requesting that the money be transferred back. (Legal Practitioners Indemnity Insurnace Fund NPC, Accessed 2019) (Legal PRactitioners Indemnity Insurnace Fund NPC, Accessed 2019)

All the above instances are well know scams aimed at legal firms and professionals as reported in the Legal Practitioners Development Fund Website in an attempt to make more legal practitioners aware of the potential cyber-attacks and threats in South Africa, a dark reality of the digital times in which we practice.

In South Africa there is on average 13,842 cyber attacks daily, which translates into 570 attacks per hour, with South Africa itself being listed as the second most targeted country in the world in so far as cyberattacks are concerned. (Allen, 2019) (Pillay, 2019) Worrisome statistics given the confidential information and data legal practitioners deal with on a daily basis (Eloff, 2017)and the fact that the Attorneys Insurance Indemnity Fund does not provide cover for cyber attacks and financial loss that may be incurred as a result of same. (Allen, 2019) (Pillay, 2019)

Given the highly confidential and sometimes sensitive nature of information entrusted to a legal practitioner, there is an ethical duty on legal practitioners to protect all sources of information by appropriate safeguards and procedures, whether dealing with paper or electronic sources of information. Failing which may lead to professional negligence and reputational damage

Given the highly sophisticated methods used by hackers today, Law Firms will be wise to heed to the warning bell and take note of The Law Society of South Africa’s 2018 Guideline on

Information Security For South African Law Firms. The guidelines, which aim merely to provide a general framework, provide that law firms must establish credible Information Security Management Systems (ISMS) by specifically focusing on technology, processes and people, the three components present in the processing of information. (Jooste, 2019)

A credible ISMS requires a legal practitioner to use available technologies and software programmes to enhance information security such as anti-virus software, intrusion detection devices and automatic back up applications. Additionally a proper ISMS requires that law firms provide clear processes that manage and control the generation, processing, communication and retention of information and that meets the goals of confidentiality, integrity and availability. Lastly a credible ISMS requires that the importance of securing and safeguarding client confidential information must be understood as a legal obligation, part of the legal duty underpinning client -legal privilege. (Heyink, 2018)

As expressed by Judge King, highlighted by the LSSA 2018 Guideline on Information Security, we are whether we like it or not members of the information age and accordingly there rests a duty on legal practitioners to ensure the proper governance of the information on which our practices depend. (Heyink, 2018)

To illustrate the importance of Cybersecurity and the ease with which a system can be compromised, Futures Law Faculty, together with IEIT Holdings, Cyberlogic, Cog3nt and Nuventiv, have invited a Cybersecurity Expert , Prof Cobus Jooste and 16 year old international ethical hacker, Marcus Weinberger, to discuss cybersecurity and demonstrate how you can ensure the cybersafety and security of your and your company's personal data on 24 October 2019, 5PM at Inner City Ideas Cartel.

For more information see – www.futureslawfaculty.co.za or to buy tickets - https://www.quicket.co.za/events/77143-hacking-cybersecurity/#/

Author

Kristi Erasmus

Head of Futures Law Faculty

info@futureslawfaculty.co.za / kristi@ilpdr.co.za

www.futureslawfaculty.co.za