NATIONAL OFFICE
Thornhill Office Park
Building 20
94 Bekker Road
Vorna Valley, Midrand
Tel: 010 001 8500

LEGAL PRACTICE COUNCIL

Notice

30 July 2020

LPC warns practitioners of a fraudulent email purporting to be from the LPC Free State provincial office

The Legal Practice Council would like to warn all legal practitioners about a fraudulent email that purports to be from an employee at the Free State provincial office of the Legal Practice Council.

Legal practitioners are advised to please ignore any email from the sender ilzem@lpc.org.za followed by operation@spcosg.com or any other suspicious indication that the e-mail does not originate from the LPC. Practitioners are warned not to click on the link in this or any other mail that comes from a suspicious source. Indications in the mail that should give rise to suspicions are the fact none of our emails are ever sent in conjunction with other email addresses. Kindly note that the LPC sends emails with its signature only.

Legal practitioners are again warned of business e-mails frauds and alerted to the common cyber-attack known as phishing.

"Phishing" is the most common type of cyber-attack that affects organisations like ours. Phishing attacks can take many forms, but they all share a common goal – getting one to share sensitive information such as login credentials, credit card information, or bank account details. Although we maintain controls to help protect our networks and computers from cyber threats, we rely on you to be our last line of defence. We outline below a few different types of phishing attacks to watch out for:

- Spear Phishing: Spear phishing is a more sophisticated phishing attack that includes customised information that makes the attacker seem like a legitimate source. They may use your name and phone number and refer to LPC in the e-mail to trick you into thinking they have a connection to you, making you more likely to click on a link or attachment that is contained in the e-mail.

- Whaling: Whaling is a popular ploy aimed at getting someone to transfer money or send sensitive information to an attacker via email by impersonating a real company official, and particularly a senior executive. Using a fake domain that appears similar to ours, the mails would look like normal emails from a high-level official of the Council, typically the chairperson or Executive Officer, and ask for sensitive information (including usernames and passwords).

- Shared Document Phishing: You may receive an e-mail that appears to come from a file-sharing site like SharePoint alerting you that a document has been shared with you. The link provided in these e-mails will take you to a fake login page that mimics the real login page and your account credentials will be stolen if entered.

<u>What You Can Do</u>

To avoid these phishing schemes, please observe the following email best practices:

- Do not click on links or attachments from senders that you do not recognise. Be especially wary of .zip or other compressed or executable file types.
- Do not provide sensitive personal information (like usernames and passwords) over email.
- Watch for email senders that use suspicious or misleading domain names.
- Inspect URLs carefully to make sure they are legitimate and not imposter sites.

- Do not try to open any shared document that you are not expecting to receive.
- Be especially cautious when opening attachments or clicking on links if you receive an email containing a warning banner indicating that it originated from an external source.

Issued by the Legal Practice Council