I-RiskSpot
Risk Management Monthly Newsletter
Brought to you by the Bar Council Risk Management Committee

STAYING SAFE ONLINE

HOW TO CREATE A SECURE PASSWORD

- Your password should be difficult for anyone to guess;
- Don't use personal information as your password eg your birthday;
- Don't use the same password for different online accounts;
- Create long and unique passwords — use a mix of lower and uppercase letters, random numbers, and special characters/symbols;
- Always sign out / opt out for the "Remember Password" option;
- Avoid entering your passwords when connected to unsecured Wi-Fi or when using devices you do not own;
- Pay attention to your password strength when creating your password; and
- Change your passwords regularly and do not share the details with others.

HOW TO SPOT FAKE/PHISHING EMAILS

- The email contains inconsistencies about the email addresses, links, and domain names;
- The email is from a completely different address or free webmail address;
- The email uses a non-specific greeting like "Dear Sir/Madam" or "Dear Customer" instead of your name;
- The email demands urgent action, threatening a negative consequence or loss of opportunity if not responded to;
- The email claims to be from a prominent organisation but the website link appears fake;
- The email requests your personal information, such as login username, password or bank details;
- The email contains spelling and grammatical errors;
- The email contains an image of the text rather than in text format / pasted onto the body of the email; and
- The email contains suspicious attachments with unfamiliar extensions or those commonly associated with malware eg .zip, .exe, .scr, etc.

OTHER METHODS TO STAYING SAFE ONLINE

- Use a reliable antivirus and keep your security software updated;
- Consider wiping out data on a gadget remotely if it is lost;
- Turn on your firewall;
- Make sure website links are secure and trusted before keying in any banking information;
- Ensure email settings have the requisite security settings, ie encryption of emails;
- Protect your accounts using two-factor authentication, ie requiring a second verification step to log in to your accounts;
- Protect your data by backing it up to an external hard drive or in the cloud;
- Lock your smartphone and tablet devices;
- Don't click on unsolicited pop-ups, unknown emails or unfamiliar links;
- Don't disclose information unless you're certain of its intended purpose;
- Don't store credit card details online;
- Don't reply to spammers;
- Don't post personal details on social media;
- Disable Bluetooth and Wi-fi when not in use;
- When throwing away old computers or mobile devices, make sure the drives are fully wiped and the machine is given a factory reset; and
- Don't respond to requests to change the personal email address associated with your online account.

For enquiries on PII and risk management, please contact:
Bar Council Professional Indemnity Insurance & Risk Management Department
Tel: 03-2050 2001
Email: pirm@malaysianbar.org.my
Website:www.praktis.com.my

Issued by Mohamad Ezri Abdul Wahab and Arthur Wang
Co-Chairpersons, Bar Council Risk Management Committee
October 2022