LEGAL PRACTITIONERS' LIABILITY COMMITTEE

Multi-factor authentication: a security must-have

Multi-factor authentication is one of the most effective ways you can prevent cyber-criminals from gaining access to your firm's systems and your clients' confidential information. Multi-factor authentication is readily available, easy to set up and gives you an extra layer of security if your password is stolen (including where it is fraudulently obtained by phishing and social engineering).

When you enter a username and password to access online accounts, that is classed as single-factor authentication. Your password is the only security credential (authenticating factor) that verifies you are who you say you are.

Single-factor authentication is unsafe. Usernames are often email addresses which may be publicly available or easily guessed and once cyber criminals have that, they can try to obtain your password by:

- experimenting with commonly used passwords or guessing a weak password
- sending you a phishing email which tricks you into clicking on a link and entering your password on a webpage
- taking advantage of a data breach on the relevant website or another website where you have used the same password.

Multi-factor authentication is a much safer option. It means using two or more authenticating factors, which can be two or more of the following:

- something you know – e.g. a password, personal identification number (PIN) or response to a question
- something you have – e.g. a mobile phone app, SMS code or physical token such a one-time PIN token
- something you are (physically) – e.g. a fingerprint or iris scan.

Cyber criminals continue to target software programs, as well as personal email and social media accounts which can be used for social engineering purposes. Multi-factor authentication is available on Office 365 as well as most popular email and social media platforms including LinkedIn, Facebook, Instagram, Gmail, Microsoft/Outlook Mail and iCloud. A search of the platform security and privacy settings will reveal simple steps to set it up. Options to use SMS alerts are an especially useful authentication factor because they also warn you if someone tries to log in to your account.

Multi-factor authentication should be the minimum security standard for all your online accounts and it's probably easier to turn on and use than you think.