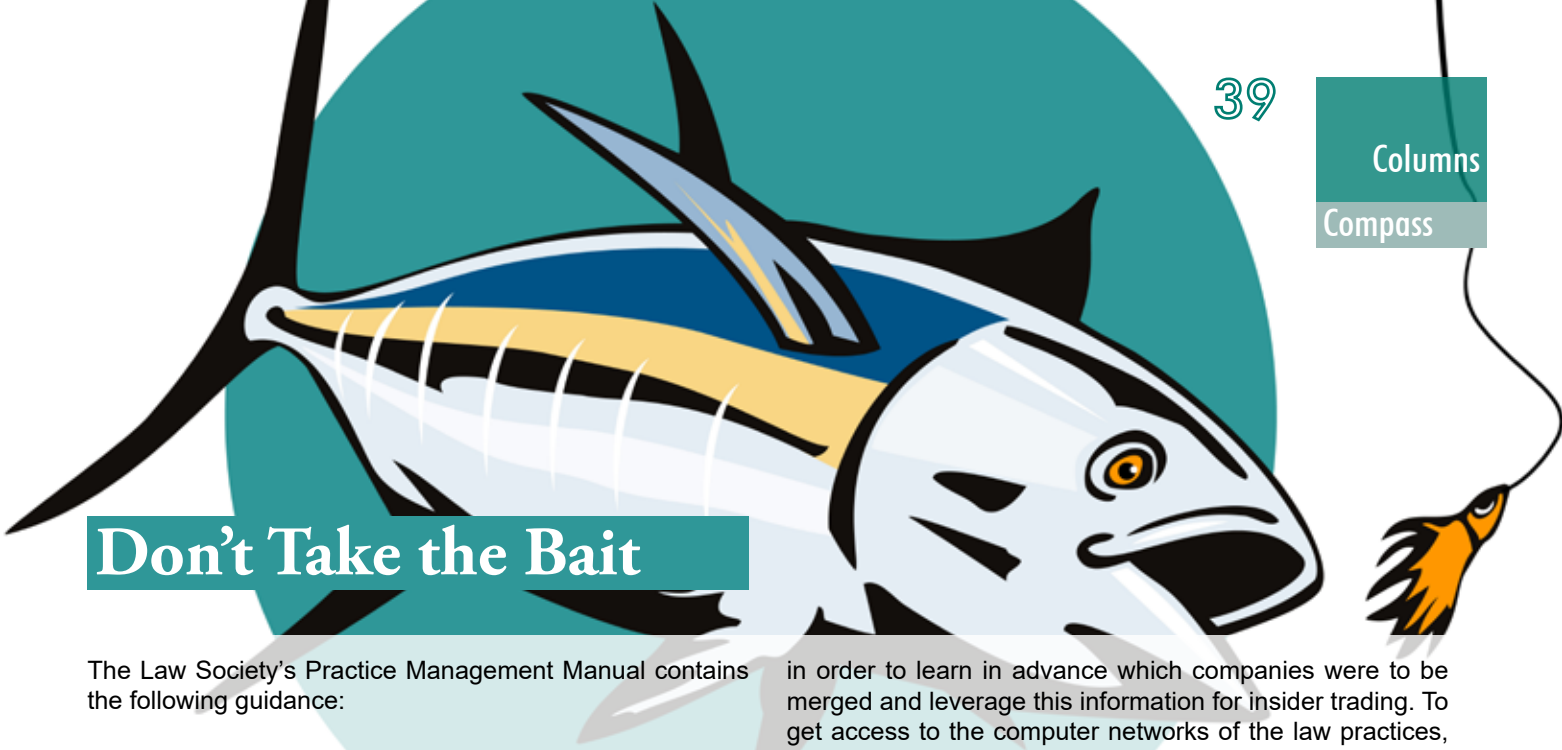

Don't Take the Bait

The Law Society's Practice Management Manual contains the following guidance:

> Stay Alert to Security Risks
>
> To keep the Practice's IT Systems virus-free, exercise caution when opening e-mail messages from unidentified parties. Do not open any email attachment unless you recognise the sender AND you are expecting an attachment from the sender. Delete suspicious emails from your mailbox or alert the IT Department who will undertake the appropriate course of action in respect of the same.

The guidance is a reminder that the human element is likely to be the weakest link in a law practice's IT security system. It is this weakness that phishing seeks to exploit. Phishing is "a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly." (Merriam-Webster)

Scammers use numerous phishing tactics. It may vary from a simple e-mail asking for information to complex spear-phishing attacks which appear to be from a reputable source. Spear-phishing usually targets a specific organisation or individual. These attacks may result in a loss of data or it may allow criminals to install malware in the law practice's computer system.

Phishing first surfaced in the United States sometime in the mid-1990s. The term "phishing" is a homophone of fishing. It was coined as an analogy to fishing where lures or baits are used to 'fish' for passwords and information. Some of the earliest hackers were known as phreaks, hence the use of "ph" in place of the letter "f" in the spelling of the term.

In 2016, there were numerous reports of law practices in other countries being targeted by scammers. In the United States, New York based threat intelligence firm, Flashpoint, warned that a broker named "Oleras" was attempting to hire hackers to break into law pratices' computer systems in order to learn in advance which companies were to be merged and leverage this information for insider trading. To get access to the computer networks of the law practices, the broker suggested spear-phishing attacks on employees whose names, email addresses and social media account information were provided.

The following are some phishing tactics that have been employed in the past:

- Lawyers in some states in the United States received phishing e-mails which purported to be about disciplinary investigations by the state bar regulator. Some lawyers in Nevada received emails referencing discipline complaint notification in the subject line, while others said the recipient had not paid his or her bar dues. California bar members also received emails about an alleged disciplinary matter, and the communications appeared to be signed by the bar president. Other states affected were Florida, Georgia and Alabama. (Source: *American Bar Association Journal*)

- A large number of associates at a law firm received an e-mail from a Hotmail account or similar, which included the name of the firm's managing partner – to give the appearance that it had been sent from his personal account. The e-mail, purporting to be from the partner, said that he was having difficulty accessing the firm's e-mail that morning, but that he needed them to look at an attached document asap. The document contained a bug designed to harvest information from the law firm's systems. (Source: *Are lawyers an easy target for hackers? The Law Society Gazette (England & Wales)*)

- *The bogus applicant*
  One tactic used to persuade a target to install malware on to their system has been the use of fake job applicants. This can involve an e-mailed job application, with an attachment that purports to be a CV or application form but that is actually a disguised malware program. This is usually detectable by antivirus systems, but is a route

that has seen successful use in several cases as the attachment's existence makes sense in the context of a job application e-mail. As this type of e-mail is one that firms will expect to receive from people that they do not know, it is more likely to be opened.

- A more novel approach on record involved an "applicant" arriving late for an interview, wet from rain, and holding a collapsing folder full of soaked documents that were no longer readable. The aim was to enlist sympathy from reception staff and to persuade them to allow the "applicant" to print out fresh copies of their CV and portfolio, which the "applicant" had saved on a datastick. Once the datastick was inserted it installed malware to the firms systems. (Source: Spiders in the web: The risks of online crime to legal business. Solicitors Regulation Authority)

- *Commercial espionage by "spear phishing"*
  In 2011, a Toronto law firm working on a proposed acquisition of a Chinese company was targeted by data thieves. Lawyers working on the deal received e-mails that appeared to be from a partner in the firm who was involved in the transaction. The e-mails were actually a targeted phishing operation, and contained an attachment which installed a computer program on to the firm's IT systems. This program was used to record data and information and allow the third party to access it. The attack involved three other Toronto law firms, and was eventually traced to computers in China. Commercial espionage was the presumed motive for the attack. (Source: Spiders in the web: The risks of online crime to legal business. Solicitors Regulation Authority)

Phishing tactics will continue to evolve. Scammers have the persistence and determination, and they are driven by an optimism that their "fishing" expeditions with countless lures will result in at least some recipients taking the bait.

Awareness and vigilance are critical. Intuitively, you should be able to spot most scams. However, as seen in the tactics that have been employed in the past, it may be difficult in some instances to distinguish legitimate e-mails from phishing e-mails. If unsure, it may be best to err on the side of caution and delete the e-mail, do not open an attachment, or check with the purported sender of the e-mail.

Knowledge Management Department
The Law Society of Singapore