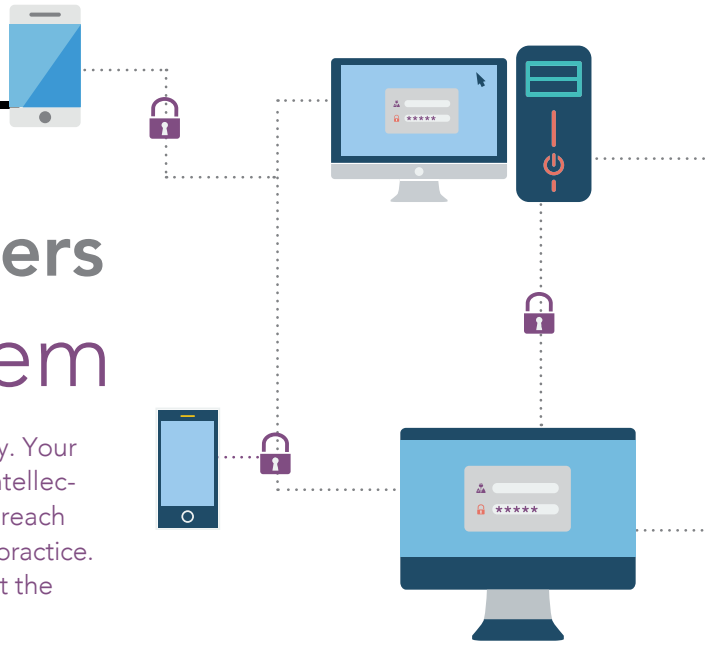


New lawyer cyber dangers and how to avoid them

Like the local bank, your practice holds valuable information and money. Your computer systems may contain client information, trade secrets, and intellectual property. Your trust accounts have large sums of money. A cyber breach or trust account theft will harm your clients and potentially cripple your practice. Security guards, specialized safes, and sophisticated procedures protect the local bank. What safeguards have you put in place for your practice?

Perceived to be less sophisticated than banks and big companies, lawyers make easy targets for tech-savvy criminals. The payoff, which can include emptying trust accounts and taking advantage of confidential information, is big for hackers. Young lawyers can be especially vulnerable given their lack of experience.

Bad cheque frauds

Bad cheque fraud occurs when a fraudster, posing as a legitimate client, retains a lawyer on a contrived legal matter. The fraudster may ask for help with collecting a business debt, facilitating a loan, enforcing an agreement against an ex-spouse, or collecting a fee for trademark or copyright infringement. Whatever the legal issue, a common red flag is that the matter must be resolved quickly and with little effort. A cheque arrives from the opposing party, and the lawyer deposits the cheque. The client demands the funds from the cheque be released immediately. The lawyer releases the funds before the cheque clears. The fraudster vanishes into thin air, and the lawyer discovers, too late, that the bad cheque bounced.

These deceptions are sophisticated. Fraudsters use realistic looking fake identification. They will have all the usual supporting documents a real file will have. They will seek to add you on LinkedIn and may appear in your social network as "friends" of people you know. We have even seen fake websites created to support these frauds. Organized crime is behind these frauds and more money and effort is invested into duping you than ever before.

Spot the red flags: Fraudster clients are often in a rush and pressure you to take shortcuts and get the deal done quickly. They have no issue with paying higher fees. They may use names that do not match their email addresses and often express a preference to only communicate by email. Without explanation, the payment amounts may not match the expected payments and no explanation is forthcoming. The cheque is drawn from an unrelated party. And in all cases, fraudsters demand the funds from the cheque to be transferred before the cheque clears.

Protect yourself with these tips: Never disburse funds from your trust account until you are sure the incoming funds are real and in your account. Be aware the bank can reverse a bad cheque, even a certified cheque or bank draft, after any amount of time. Familiarize yourself with the requirements of LawPRO's coverage for counterfeit cheques and bank drafts. Cross-check names online and on practicePRO's AvoidAClaim.com blog where you can find the names of confirmed fraudsters. Look up addresses using Street View in Google Maps, and conduct reverse searches on phone numbers using canada411.ca. And if you are in doubt, call LawPRO. We will help you determine if the matter is legitimate.

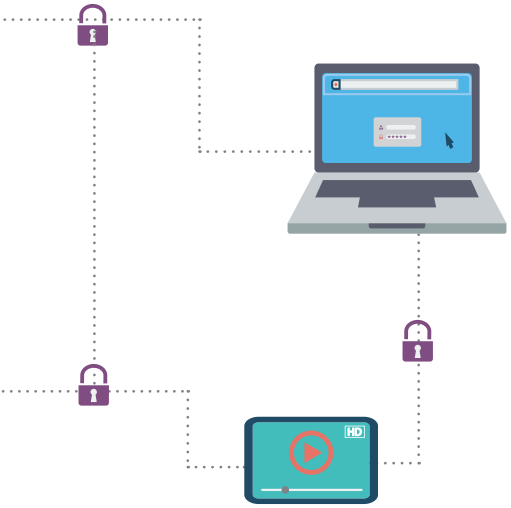
Email dangers

Email is the most frequent way law firm systems are compromised. This occurs when someone opens an infected attachment, clicks on a link in an email, or responds to a phishing message. Once installed, malware can give hackers access to your system and/or destroy your data. Educate your staff about the dangers of email.

Phishing – don't take the bait

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an email. Phishing scams are usually bulk emails sent to large numbers of people. Even if only two or three per cent of recipients fall for them, hundreds or even thousands of people can be victimized.

Phishing messages take the form of an email, allegedly from your bank or another business you know that suggests your account has been compromised or that payment is overdue. They will have the same layout, logos and links as legitimate emails from these companies. They try to create a sense of urgency and ask you to login to reset your password or verify a payment was made. However, the link you click takes you to an imposter website that looks much like the familiar company site, and when you login you are actually giving your



password or other personal information to the hackers. They will use your information for malicious purposes such as ID theft or credit card fraud.

Prevent phishing by putting your cursor over the link in an email. Your email program will show the actual web address at the bottom of the screen. If it is not familiar to you, it is likely a phishing attempt.

Spear phishing – a bait just for you

The "spear" in spear phishing alludes to the fact that messages are targeted to specific individuals. Spear phishing messages are more convincing because they are personally addressed, appear to be from someone you already know, and may include other detailed personalized information. In some cases a phone call will come in as a follow-up to the message. In one case, a senior accounting staff member at a large firm received a request on an active file, purportedly from the firm's managing partner, to send a bank account number and account signatures to a person in Europe so they could verify a certified cheque was from the firm.

Follow firm processes and procedures for the review and approval of financial transactions – and don't bypass them due to urgent circumstances. Never share confidential client or firm information without being sure it is appropriate to do so by getting confirmation from someone familiar with the file. Be on the lookout for and question any last minute changes on fund transfers or payments.

Loss of client data on portable devices

Laptops, tablets, and mobile phones may contain confidential and sensitive information. Should a portable device be lost or stolen, client data may go with it. Prevent the intrusion by ensuring all portable devices have a strong password and are encrypted. A good practice is to enable the device to allow a remote wipe of all data.

Other devious cyber frauds

There is no end to the efforts and imagination hackers will put into infiltrating law practices. In 2012, a Trojan banker virus infected an Ontario law firm. This virus presented a spoofed version of the website of the firm's bank on the bookkeeper's computer, and passwords entered on the fake site were passed to the hackers, who then used them to wire funds from the firm's trust account.

LawPRO has also recently seen instances where a fraudster hacks into a client's email and surreptitiously monitors emails going back and forth between the lawyer and the client. At the opportune time, usually just before a real estate deal is closing or the loan funds are to be advanced, the hacker sends an email redirecting where the funds should go. This change of instructions appears to be coming from the client via the client's email, but if the lawyer follows these instructions, the money goes to the fraudster.

Ransomware is an under-reported but increasingly common form of attack. It is usually spread by clicking on an infected email attachment or website and encrypts all the data files on a firm's computers. A message then pops-up stating that if you don't pay a certain amount of money within a tight deadline, the files will be destroyed.

Poor tech hygiene often weakest link

As with brushing your teeth, maintaining good tech hygiene needs to be done regularly and with care.

Passwords should be used at entry points and changed regularly. A good rule of thumb is a 12-character password which includes mixed lower and upper case letters, and symbols. Poor passwords are one of the main ways hackers gain access to law firms.

Operating systems (Windows, Linux, OS X) and other software should be updated regularly. Once out-of-date (some lawyers still use the now-defunct and unsupported Windows XP), operating systems are vulnerable as known weaknesses can be exploited. Firewalls, which protect access to the network, should be turned on. Anti-virus software should be installed and updated. Networks and systems should be checked regularly.

Protect by being proactive

The profession handles massive amounts of information and money. Organized crime and other entities with significant resources continue to find inventive ways to hack in. The need to be vigilant and keep up with technological safeguards is high. Hackers will look for and exploit the weakest link in your systems and hardware.

Be proactive and take the steps discussed here. See the *LawPRO Magazine* "Cybercrime and Law Firms" for more information on how to keep your professional and personal data safe. The magazine is chock-full of simple tips you can use now to improve your cybersecurity. ■

Ian Hu is Counsel, Claims Prevention and practicePRO at LawPRO.