LAWPRO magazine

DECEMBER 2013 VOL 12.4

CYBERCRIME AND LAW FIRMS

The risks and dangers are real

How to protect yourself and your firm

Also:

- LawPRO cybercrime coverage and other insurance options
- How to make your passwords strong and secure
- Recognize and avoid phishing scams

keyDATES

LawPRO Key Dates for 2014

Make a note of the key dates for 2014 and mark your calendars accordingly.

January 31, 2014:

Real estate and civil litigation transaction levies and forms are due for the quarter ending December 31, 2013.

February 5, 2014:

Last date to qualify for a $50 early payment discount on the 2014 policy premium (see page 13 of the 2014 Program Guide for details).

April 30, 2014:

Real estate and civil litigation transaction levies and forms are due for the quarter ending March 31, 2014.

April 30, 2014:

Annual exemption forms from lawyers not practising civil litigation or real estate in 2014 and wanting to exempt themselves from quarterly filings are due.

July 31, 2014:

Real estate and civil litigation transaction levies and forms are due for the quarter ending June 30, 2014.

September 15, 2014:

File your LawPRO Risk Management Credit (for Continuing Professional Development) Declaration by this date to qualify for the $50 premium discount on your 2015 insurance premium for each LawPRO-approved program (to a maximum of $100) completed by this date.

On or about October 1, 2014:

LawPRO online filing of Professional Liability Insurance renewal applications for 2015 is expected to begin. If you wish to file a paper application instead, please note that paper renewal applications will not be automatically mailed out, but it is expected that you will be able to download a 2015 pre-populated paper renewal application from our website on or about October 1, 2014.

October 31, 2014:

Real estate and civil litigation transaction levies and forms are due for the quarter ending September 30, 2014.

November 3, 2014:

E-filing discount deadline: Renewal applications filed online on or before November 1, 2014 qualify for the e-filing discount to be applied to the 2015 insurance premium.

November 10, 2014:

Renewal application filing deadline: 2015 LawPRO insurance applications filed/received after this date will be subject to a surcharge equal to 30 per cent of the base premium.

LawPRO customer service department can be reached at: 416-598-5899 or 1-800-410-1013, by fax at 416-599-8341 or 1-800-286-7639; or by email at service@lawpro.ca

LawPROFAQ

Higher deductible for certain administrative dismissal claims

Q. Is it true that the deductible that I will have to pay for certain administrative dismissal claims will now be $10,000 more than (*i.e., on top of*) my usual deductible amount?

A. Yes.

In order to control claims costs related to often-preventable administrative dismissal claims, LawPRO has introduced a $10,000 deductible increase that will be imposed in addition to (i.e., on top of) the insured's existing deductible amount for claims that result where an administrative dismissal is not set aside through steps taken by or under the direction of LawPRO.

More information

For more details, please see "$10,000 increase in deductible for certain administrative dismissal claims" on page 2 of the October issue of *LawPRO Magazine*.

As well, for such claims, the deductible will be deemed to apply to claim expenses, as well as indemnity payments and/or costs of repairs, regardless of the deductible option selected by the lawyer.

Contents

Volume 12
Issue 4
December 2013

TECH TIP | COULD THIS HAPPEN TO YOU? | PRACTICE TIP | BOOK REVIEW | SOCIAL MEDIA

Departments:

Features:

In practice:

Publications Mail Agreement No. 40026252

Return undeliverable Canadian addresses to:
LawPRO
250 Yonge Street
Suite 3101, P.O. Box 3
Toronto, ON M5B 2L7

New hire in the LawPRO finance department

LawPRO is pleased to welcome Steve Onona to our finance department as the new director of actuarial services. Before joining LawPRO Mr. Onona worked at Northbridge Financial Corporation in the actuarial department. Mr. Onona attended the University College of London where he graduated with his BSc (Hons) statistics, computing, operational research and economics.

We're hiring: Two claims counsel positions and practicePRO counsel

We are currently seeking two claims counsel to join the LawPRO claims team. Both are permanent full-time positions in LawPRO's primary professional liability claims department. The successful candidates will have the opportunity to handle interesting cases in a variety of areas of law. LawPRO claims counsel interact with insured lawyers in investigating, evaluating, and resolving errors and omissions claims against them. They manage these claims in-house or direct external legal counsel and professionals in resolving them.

LawPRO is also looking for a dynamic and resourceful team player for our practicePRO program, our internationally recognized risk management and claims prevention initiative. As practicePRO counsel you will develop, implement and support all aspects of practicePRO operations.

Think you would be a perfect fit, or know a colleague or friend that would? Please visit lawpro.ca/Career/default.asp for information about how to apply.

LawPRO external counsel recognized for their achievements, briefed on trends and procedures

In October of this year, LawPRO held its biennial seminar for its outside counsel. At this meeting, several LawPRO claims professionals and executives delivered presentations detailing emerging claims trends, provided information about changes to procedures for working on LawPRO matters, and answered questions about recently-introduced improvements to the technology we use to connect with external counsel. As always, this meeting also provided an important opportunity to recognize the efforts and successes of our outside counsel for their important work on behalf of Ontario lawyers.

LawPRO employees put their charity day to good use

As part of LawPRO's corporate social responsibility initiative, the company grants employees one charity day every year to use in lieu of working at the office. As an example of how our employees have used that charity day, the group pictured at right spent a day in October preparing over 300 sandwiches to be served through the Lawyers Feed the Hungry program operated by the Law Society of Upper Canada.

For more information on our charity efforts please visit: lawpro.ca/AboutLawpro/lscsr.asp

eBRIEFS

Below is a summary of electronic communications you should have received from LawPRO this fall. The full content of these newsletters is available at practicepro.ca/enews.

To ensure that you receive timely information from LawPRO about deadlines, news and other insurance program developments, please make sure you have whitelisted service@lawpro.ca.

Webzines

practicePRO 15th anniversary edition of *LawPRO Magazine*

September 30

LawPRO's practicePRO program, created to support lawyers in building thriving practices while managing risks, was launched 15 years ago! This webzine includes links to specific articles of the magazine.

2014 LawPRO policy responds to changes in the profession and related risks

October 17

In late September, Convocation of the Law Society of Upper Canada approved LawPRO's program of insurance for 2014. This webzine includes links to our October Insurance Issue of the *LawPRO Magazine*, along with links to job postings.

Insurance News

2nd REMINDER: Apply for your LawPRO Risk Management Credit by September 15

September 11

Reminder for lawyers to apply for the LawPRO Risk Management Credit by September 15th to save $100.

2013 Second quarter transaction levy filings overdue

September 18

A reminder to lawyers that we have not yet received their transaction levy filings for the second quarter of 2013.

Renew your LawPRO exemption status for 2014: File online now

September 26, October 9

A reminder and instructions for renewing your exemption status before November 8, 2013.

Convocation approves LawPRO's insurance program for 2014

September 27

For the fourth consecutive year, LawPRO will hold the base premium for the mandatory insurance program steady at $3,350. This webzine includes additional details on the insurance program for 2014, along with the media release and report to Convocation.

Renew your professional liability insurance for 2014 starting October 1

October 1, 15, 25; November 4, 18

A message to lawyers to E-file your 2014 insurance application by November 1 to save $25.

Renew your firm's professional liability insurance for 2014 now

October 2, 16, 28; November 5, 18

A message to all firms to E-file their 2014 insurance application by November 1 to save $25.

LawPRO magazine

President & CEO: Kathleen A. Waters

LawPRO Magazine is published by Lawyers' Professional Indemnity Company (LawPRO) to update practitioners about LawPRO's activities and insurance programs, and to provide practical advice on ways lawyers can minimize their exposure to potential claims.

lawpro.ca
Tel: 416-598-5800 or 1-800-410-1013 Fax: 416-599-8341 or 1-800-286-7639

Editors: Dan Pinnington dan.pinnington@lawpro.ca
Nora Rock nora.rock@lawpro.ca

Design & Production: Freeman Communications studio@freemancomm.com

Photography: Rick Chard rickchard@bmts.com

Interesting times (and cybercrimes)

call for active risk reduction efforts, not just insurance coverage

Legal systems and their participants have a reputation – perhaps no longer just – for being slow to embrace technological change. But while good lawyers know that technology tools are not (at least not yet!) a full replacement for the exercise of professional judgment and the application of legal knowledge, they also know that a head-in-the-sand approach to the hurtling evolution of computer technology is a recipe for being trampled.

The stampede, in this analogy, involves two different herds: the first is comprised of honest competitors who, using technology to their own and their clients' advantage, will claim an ever-increasing share of the legal services market. The second herd is more sinister: tech-savvy criminals increasingly use the Internet to exploit both human and technological vulnerabilities in their quest to steal money and valuable information.

In the previous issue of *LawPRO Magazine* we explored the future of legal services, and in doing so, touched on some of the technologies driving that evolution. In this issue, we turn our attention to the "black hats" of the high tech world: the perpetrators of cybercrime.

Cyber criminals have lawyers and law firms in their sights. For one thing, lawyers' computer systems often harbour valuable information – not just clients' personal information, but also information about pending commercial deals, trade secrets, and intellectual property: information that is worth money. Lawyers' computers also, in many cases, provide access to actual funds, in the form of trust account monies accessible via electronic banking.

Not only do law office computers contain valuable information, but they can also be fairly vulnerable from a security perspective. Smaller firms may not have staff with the knowledge needed to build state-of-the-art security systems, and generally do not have in-house computing professionals available to monitor and respond to immediate threats. While good-quality security products are available at a cost that is affordable for most small firms, the extent to which firms have

actually invested in and implemented these protections varies widely. Cyber criminals prey on the most vulnerable firms. When a firm's security system is weak, the firm can easily become a target.

We know that law firms are targeted by cybercriminals, because these attacks are often in the news, and even directly reported to us via the practicePRO program's AvoidAClaim blog or in the form of claims. We reviewed the issue of cyber risk in 2013, and have introduced a $250,000 sublimit of coverage for eligible cybercrime claims in our 2014 policy. See "The LawPRO $250,000 cybercrime coverage: What it covers and why" at page 25 for more information on this coverage.

While "coverage" can be a comforting word, lawyers would be making a big mistake in feeling comfortably complacent about cybercrime. The potential for losses from cybercrime for any firm is equal to *or greater than* the balance in the firm's trust accounts plus the value of the confidential information contained in its computer systems. Why greater? Because cybercrime can lead to reputational, equipment, and business interruption losses, too. These losses are not covered by your LawPRO policy.

In the article "Other cyber risk insurance options: Do you have the coverage you need?" on page 26, we discuss types of cybercrime insurance coverage, other than professional indemnity coverage, that you may want to consider. But this information – and those types of coverage – come with a very important caveat: *no* form of insurance coverage should be seen as a complete answer to cybercrime.

In fact, to the extent that overly rich insurance coverage for cyber losses creates a disincentive to law firms to invest in appropriate security protections, such coverage actually encourages cyber attacks. In introducing modest sublimit coverage, we hope to provide a small safety net, without inspiring dangerous complacency on the part of lawyers and exploitative behaviour on the part of criminals.

An insurance "band-aid" is not enough. Preventing cybercrime requires an active, vigilant, and multi-faceted approach. It is the responsibility of each of us to reduce our vulnerability to cybercrime, both in our professional and in our personal lives. Cyber security is a complex discipline that requires not only technical protections (such as antivirus and anti-malware programs), but also the learning, adoption, and consistent application of protective behaviours like using strong passwords and changing them regularly.

The first step in improving your firm's cyber security is to educate yourself about the nature of the risks and the approaches available for dealing with them. In this issue, we introduce some of the most important cyber risks in "Cybercrime and law firms: The risks and dangers are real" at page 6. In "Protecting yourself from cybercrime dangers: The steps you need to take" at page 10, we review some of the best strategies that firms can use to reduce their exposure to those threats.

But lawyers must not stop there. Each of us must come to embrace cyber security as an important aspect of life-long learning. While I don't count myself an expert quite yet, I've had my share of learning experiences. For example, when I needed to have a new wireless network established for my home computer, I watched with interest as the technician stepped outside to see if he could gain unauthorized access to my system. He couldn't, but I was shocked to discover the number of unprotected networks in my own neighbourhood. More recently, I learned about the differences between an antivirus program and an anti-malware program – the biggest take-away being, it's not a question of choosing one or the other – you need both! But while there are doubtless many other aspects of cyber security that I will need to investigate further, my awareness is growing, and my behaviours are evolving. These days, when I encounter a site that does not allow (or require) me to choose a "strong" password (don't know what that means? See the "Tech Tip: Keeping your passwords strong and secure" on page 30!), I find myself wondering about other aspects of the site's security, and about what risks I might be incurring by doing business there. I know that I'm gradually developing the cyber safety instincts that will reduce my risk of becoming a victim of cybercrime. I hope that the articles in this issue will help other lawyers do the same. Relying on insurance coverage to prevent or "solve" cybercrime is tantamount to shutting the stable door after the horse has bolted. Only active risk reduction will give us a fighting chance against those who would threaten our funds, our privacy, and our professional reputations.

Kathleen A. Waters
President & CEO

Cybercrime and law firms:

The risks and dangers are real

Historians may well look back and call 2013 "The year of the hacker." There have been numerous high-profile data breaches involving major corporations and online services: Facebook, Apple, Twitter, Adobe, NASDAQ, The New York Times and LexisNexis, to name just a few. Everyone reading this article likely has information stored by at least one, if not several, of these companies.

And it doesn't stop there. Millions of other business entities and individuals have experienced data breaches this year, either directly on their own computers or systems, or indirectly where there was a data breach involving information about them that was stored with a third party. Countless others will have lost money after being duped in various online scams.

Law firms and lawyers take notice: cyber criminals are specifically targeting *you* because they want your data or the money in your trust account. Law firms are actually very appealing and sought-after targets for cyber criminals for three reasons. Firstly, law firms have large amounts of sensitive and confidential information that can be very valuable. Secondly, law firms tend to have very large sums of money in their bank accounts. Lastly, and not the least, relative to their clients and based on anecdotal information, law firms tend to have weaker security protection in place on their networks and systems.

Cybercrime has hit very close to home. In 2011, several major Bay Street firms were targeted by hackers traced to China who appeared to be seeking information on a multi-billion-dollar commercial transaction. In late 2012, LawPRO handled a claim involving a significant theft from a firm trust account by a Trojan banker virus (see sidebar on facing page). There have likely been thousands of attempts to breach Ontario law firm systems this year, and probably some actual breaches as well. But we will likely never hear about them because firms that experience breaches usually try to keep their names out of the news.

Information on cybercrime tools and techniques is widely available online, making it easy for even non-technical people to undertake malicious cyber activities. But make no mistake, while rank amateurs may launch attacks on law firms, industrial espionage on high value targets can involve the most skilled hackers in the world including, potentially, foreign governments.

Cyber criminals will use every tool at their disposal to attack law firms. They will send spam and phishing messages. They will try to install malware and create backdoors into your firm's computers.

LawPRO claim involving significant theft from firm trust account by Trojan banker virus

In December, 2012, an Ontario law firm provided notice of a claim involving the infection of one of its computers by a Trojan banker virus. This was a very sophisticated fraud in which the firm's bookkeeper was induced, by a fraudster posing over the phone as a bank representative, to key in account and password information on her infected computer. Through the virus, the fraudsters were able to capture this information which they then used to access the firm's bank account. Over the course of several days, fraudsters wired several hundred thousand dollars from the firm's trust account to offshore accounts.

A more detailed review of how this fraud happened will help you appreciate how sophisticated these frauds can be. It appears the bookkeeper's computer was infected when she clicked on a link on a popular news website. Despite being the most current version with all updates, the antivirus software running on her computer did not recognize or stop the infection.

After being infected, the bookkeeper's computer appeared to have difficulties accessing the bank's website. She got a "This site is down for maintenance" message. This was actually not a page from the bank's website; rather, it was a fake or "spoofed" page pretending to be the bank's website. On another screen that appeared on her computer – which also looked like it was the bank's real website – she was asked to enter her name and phone number. This appears to have given the fraudsters her contact information, as later that day the bookkeeper received a telephone call from someone, allegedly from the firm's bank. That caller said she was aware of the login attempts and stated that the site had been down for maintenance. The caller said the site had been fixed and asked the bookkeeper to try logging in again. The bookkeeper did so, entering the primary and secondary login passwords for the account on screens that appeared on her computer – the passwords were not given to the person on the phone. The second password came from a key fob password generator. This appears to have given the hacker both passwords and access to the firm's trust account.

On each of the following two days there were similar phone calls to the bookkeeper from the woman who allegedly worked for the bank to "follow up on the website access problems." On each occasion, the bookkeeper tried to log in again and entered the primary and secondary passwords on screens that appeared on her computer.

The fraudsters went into the account during or immediately after each of the three phone calls and wired funds overseas. An amount less than the balance in the account was wired out each time. This was an infrequently used trust account and the firm had never done wire transfers from the account. The bank did not detect these frauds or stop the wires. The people behind this fraud appear to have had intimate knowledge of how to send wires from a bank account. By the terms of the banking agreements the firm had signed with the bank, the firm was responsible for replacing the funds that were taken out of the firm's bank account.

Lawyers should not underestimate the sophistication of frauds targeting trust accounts. To better protect yourself from one of these frauds, see "Increasing your online banking safety" on page 14.

They will look for weaknesses in security configurations and exploit them in order to access firm networks. In very devious ways, they will try to trick you or your staff into helping them. It is quite possible they would target you individually, including attacking your home computer to hack into your office systems.

The bottom line: cybercrime is a real and present danger for law firms. All firms should work to understand the cybercrime risks they are exposed to and take steps to reduce the likelihood they will experience a data breach at the hands of cyber criminals.

How prepared are you?

To assess your cybercrime preparedness, see if you can answer the following questions:

- Are your passwords secure enough?
- Would you or your staff be duped by a phishing message?
- How would your firm respond if one of its servers was hacked?
- Is your anti-malware software the most current version and is it updated?
- Could you tell if your computer had malware on it?
- Are your computer's security settings adequate?
- Is there a backdoor into your network?
- What would happen if a firm laptop or smartphone were lost or stolen?
- How would you deal with a major data theft by an ex-employee?
- Is your home computer safe?

The remainder of this article, and the next one, will start you on the journey to help you understand and answer these questions. Tread carefully and thoughtfully as the health and the future of your practice could well rely on how well you address cybercrime risks.

The menace of malware

*Mal*icious soft*ware* ("malware") is one of the most common ways law firm computers and networks are infiltrated and compromised by cyber criminals. The malicious intent behind malware usually involves gaining unauthorized access to computers or networks to steal money, passwords or valuable information, or to cause disruptions or destroy data. Malware can affect individual computers, firm networks and even the operation of the Internet. In many cases, people will not know their computer is infected with malware (see "How to recognize if your computer is infected with malware" on page 16). Worse yet, removing malware from a computer is often very difficult.

There are many types of malware and they usually do one or more of the following tasks or damaging things:

- Record your keystrokes to capture usernames, passwords, credit card numbers and other personal information you enter while making purchases or doing online banking. This information is then sent to cyber criminals who will use it to hack your online accounts or systems.
- Create a "backdoor" that allows hackers to access your computer or network without your knowledge by bypassing normal authentication and security mechanisms.
- Disable your security settings and anti-malware software so the malware won't be detected.
- Use your computer to hack into other computers on your firm's network.
- Take control of individual programs and even an entire computer.
- Use your computer to send email messages to the people in your address book, who will in turn become infected if they click on links or open attachments in these messages.
- Use your computer to send spam to thousands of people, usually with the intent of infecting them.
- Steal the data on your computer.
- Alter or delete your files and data.
- Display unwanted pop-up windows or advertisements.
- Slow down your computer or network or prevent access to your firm website.
- Allow someone to secretly watch you through your webcam.

Malware employs varying mechanisms to self-replicate and infect other computers. Malware often requires some kind of deliberate action by a user to infect a computer or hijack an online account. For example, you can become infected with malware by doing the following things – most of them are common tasks that occur many times a day in every law firm:

- Opening an infected email attachment.
- Just visiting a website (no need to click on a link).
- Triggering a download by clicking on a link on a website.
- Triggering a download by clicking on a link in an email, instant message or social media post.
- Plugging an infected USB stick or external hard drive into your computer.
- Downloading a program to your computer, or an app for your tablet or smartphone.
- Installing a toolbar or other add-on to your browser.

Documents created on an infected computer can be silently infected, and if those documents are sent as an email attachment, anyone opening them can be infected. USB sticks or external hard drives that are plugged into an infected computer can become infected, and they in turn can infect other computers they are then plugged into. Once malware gets into a firm network, it will often spread to other computers on the same network. As they often have mixes of people from many different firms or online communities, deal rooms and document sharing sites can be a breeding ground for malware.

In some cases the computer user doesn't have to do anything – some types of malware (e.g., worms) can spread on their own without any user actions.

While viruses and worms are the most common types of malware, there are many other types which are described in more detail in the adjacent "Common types of malware" sidebar.

Cybercrime dangers can originate inside your firm too

Many people assume, incorrectly, that the biggest cyber dangers come from outside a law office. Statistics actually show that the majority of incidents involving the destruction or loss of data are perpetrated by current, soon-to-be dismissed or recently dismissed employees. Few, if any, know more about your firm's systems than your employees; and few, if any, are in a better position to cause major damage. In particular, your IT staff, employees with advanced technology knowledge, and outside technology support people are potentially the greatest threat. They have the greatest knowledge about your system configurations, the technical know-how to be very destructive, and they are often savvy enough to cover their tracks – erasing evidence of their presence and activities. Your cybercrime prevention efforts should address these internal dangers as well.

Now that you are familiar with basic cybercrime dangers, review the next article to gain an understanding of the steps you need to take to reduce your exposures to the cybercrime dangers that occur in law firms. ■

Dan Pinnington is vice president, claims prevention and stakeholder relations at LawPRO.

Common types of malware

Malware is classified by how it propagates itself or what it does. The names and a brief description of the common types of malware appear below:

Viruses:

Viruses are one of the most common types of malware and will do one or more of the tasks and damaging things listed in the adjacent text. Like their biological namesakes, computer viruses propagate by making copies of themselves. When an infected program runs, the virus will attempt to replicate itself by copying itself into other programs, usually while completing the malicious actions it is designed to do. Viruses often arrive in infected email attachments or via a download triggered by a click on a link in an email or on a website. Even just visiting a website can start an automatic download of a virus. Some viruses will send themselves to everyone in your contact list; others will use your computer to infect strangers as they come with their own address lists.

Worms:

After viruses, worms are one of the next most common types of malware. Unlike a virus, a worm goes to work on its own without attaching itself to programs or files. Worms live in a computer's memory and can propagate by sending themselves to other computers in a network or across the Internet itself. As they spread on their own, they can very quickly infect large numbers of computers and may cause a firm's network – or even parts of the Internet – to be overwhelmed with traffic and slow down or stop working all together.

Trojans:

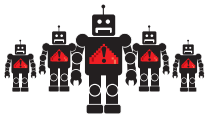
Trojans are named after the wooden horse the Greeks used to infiltrate Troy. A Trojan is a malicious program that is disguised as, or embedded within, otherwise legitimate-looking software. Computer users often unwittingly infect themselves with Trojans when they download games, screensavers, utilities, rogue security software or other enticing and usually "free" software from the Internet. Once installed on a computer, Trojans will automatically run in the background. Trojans are used for a variety of purposes, but most frequently they will open a backdoor to a computer or capture keystrokes so that sensitive information can be collected and sent to cyber criminals. See the sidebar on page 7 for details of a large fraud involving a Trojan infection.

Spyware:

Like Trojans, spyware also often comes in the form of a "free" download, but can also be installed automatically when you click on a link or open an attachment. Spyware will do many different things, but usually it will collect keystrokes or other information about you that will be shared with third parties without your consent. This can include usernames, passwords and surfing habits.

Adware:

Adware works like spyware, but will focus on your surfing habits and will slow down or stop your browsing by taking you to unwanted sites and/or inundating you with uncontrollable pop-up ads while you are browsing the web.



Botnets:

A botnet is a collection of software robots ("bots") that together create an army of infected computers (known as "zombies") that are remotely controlled by the originator. Your computer may be part of a botnet and you may not even know it. On an individual level, bots will do most of the typical malware tasks and damaging activities. When working together, botnets are used to execute denial-of-service attacks (DoS attack) or distributed denial-of-service attacks (DDoS attack). A DoS attack is accomplished when thousands of computers are told to visit a particular website or server at the same time, thereby crashing it and/or making it impossible for regular users to access it.

Rootkits:

Once malware is installed on a system, it is helpful if it stays concealed to avoid detection. Rootkits accomplish this by hiding inside the host computer's operating system. They can be very hard to detect and will do most of the typical malware tasks and damaging activities.

Scareware:

Scareware is plain devious. While visiting a website, a pop-up advertisement will appear with a "Your computer may be infected with harmful spyware programs. Immediate removal may be required. To scan, click 'Yes' below." If you click "yes," you download malware onto your computer.

Ransomware:

Ransomware infections are becoming much more common recently and are usually spread by infected email attachments or website links that trigger a download. The most common type, Cryptolocker, will scramble all the data files on your computer with virtually unbreakable encryption. You learn you are infected when a pop-up window tells you that your data has been scrambled and will be deleted unless you pay a ransom within a very short period of time, typically 48 hours or so. The ransom is typically in the range of $100 to $300 and payable only in Bitcoins, a type of virtual currency that makes payments untraceable. It is a relatively low amount so you have an incentive to pay it as a nuisance; but as you are dealing with criminals, paying it does not guarantee that you will get your data back.

Protecting yourself from cybercrime dangers: The steps you need to take

Cybercrime dangers are many, complex and ever-changing. Hardly a day goes by without another news report of a data breach or other cyber-related scam or theft. Cyber criminals have considerable resources and expertise, and can cause significant damage to their targets. Cyber criminals specifically target law firms as law firms regularly have funds in their trust accounts and client data that is often very valuable. LawPRO encourages all law firms to make dedicated and ongoing efforts to identify and understand their potential cybercrime vulnerabilities, and to take steps to reduce their exposure to cyber-related dangers. This article reviews the specific cybercrime dangers law firms need to be concerned about, and how they can mitigate their risks.

It starts with support from senior management

Any effort to tackle cybercrime must start at the top. Senior partners and firm management must be advocates of cyber security, support the implementation of appropriate practices and policies, and allocate sufficient resources to address cybercrime exposures. While there are some quick fixes that can help make your office and systems more secure (to find them see "quick fixes" opposite), most firms will need to spend some time and money to better protect themselves from cybercrime. This may include upgrading or installing new technology, training staff, and changing how some tasks are done.

Firms should also put some thought into how a cyber breach – the loss of client data or hacking of a firm server – would be handled. Firms should have a formal incident response plan so they can avoid making bad decisions on an ad hoc basis in the middle of a crisis. See page 28 for an article on incident response plans.

You likely need expert help

Beyond the very practical issue of wanting to avoid being the victim of cybercrime, remember that when using technology, lawyers and paralegals must meet their professional obligations as outlined by the lawyers' *Rules of Professional Conduct* and the *Paralegal Rules of Conduct*. These rules provide that you should have a reasonable understanding of the technology used in your practice, or access to someone who has such an understanding [Rule 2.01 of the lawyers' Rules, Rule 3.01 of the Paralegal Rules].

It is unlikely that sole practitioners and smaller firms will have someone on staff who has the technical expertise to properly address all relevant cyber security issues. With their larger and more complex technology infrastructures, even medium and larger firms may also need to seek outside help. One of the biggest dangers here is that people just don't realize what they don't know when it comes to cybercrime dangers and how to prevent them. LawPRO encourages firms to seek appropriate help from knowledgeable experts when required. To identify vulnerabilities, firms may want to consider engaging an outside expert to do a formal security assessment.

Staff education and technology use policies

As you will learn in this article, despite being technology-based, many cybercrime dangers involve a human element. Cyber criminals create situations in which law firm staff and lawyers will unintentionally and unknowingly facilitate cybercrimes as they go about their

Immediately increase your security with these "quick fixes"

While some of the work that must be done to protect a firm from cybercrime will take time and effort to implement, there are a number of things you can do that are fast and easy and that can be done at little or no cost. These "quick fixes" are highlighted throughout this issue with this quick fix logo.

common daily tasks. Educating staff to help them understand, recognize and avoid cybercrime dangers is a critical part of reducing cybercrime risk.

Written policies that clearly establish guidelines and requirements governing the acceptable use of all firm technology resources can also help reduce cyber exposures. Through technology use policies, law firm staff should be given clear direction on what they are permitted and not permitted to do with law firm technology resources. These policies should use simple and non-technical language that all employees can understand. They should be reviewed with new employees at the commencement of employment, and on an annual basis with *all* staff. It is also essential that these policies be consistently and strictly enforced.

Every technology use policy should cover some basics. They should clearly state that technology resources provided by the firm, including Internet and email access, are to be used for legitimate firm activities. Staff should understand that they have an obligation to use resources properly and appropriately. Technology use policies should also direct firm staff to ensure that the confidentiality of firm and client information is protected at all times, that there is compliance with network system security mechanisms, and that resources are not used in a manner that would negatively affect others on the system. Technology use policies should also indicate that the firm retains the right to monitor any and all electronic communications and use of the Internet to ensure the integrity of the firm's systems and compliance with the firm's technology use policy. As well, the policy should indicate that there may be sanctions for failure to comply.

You can find some sample technology use policies you can use and adapt for your firm on practicePRO.ca.

The cybercrime dangers you need to address

The cybercrime dangers firms need to address are many and varied. This article reviews these dangers in more detail and will help you start on the work that is necessary to address them so you can reduce the likelihood that cyber criminals will breach your law firm's systems. These topics covered in the sections to follow are:

1. Avoid the dangers of email
2. Lock down your browser and avoid surfing dangers
3. Avoid infections with antivirus and/or anti-malware software
4. Lock things up by using passwords properly
5. Address security vulnerabilities by installing operating system and program updates
6. Keep the bad guys out with a firewall on your Internet connection
7. Stump hackers by changing key default settings
8. Lock down and protect your data wherever it is
9. Scrub confidential client information on discarded equipment
10. Be safe when using remote access and public computers
11. Secure your mobile devices to protect the data on them
12. Harden your wireless and Bluetooth connections and use public Wi-Fi with extreme caution
13. Be careful about putting your firm's data in the cloud
14. Inside people can be the most dangerous
15. Be careful of the dangers of BYOD and family computers
16. A backup could save your practice after a cybercrime incident

As they can be used as a point of access to your firm's systems, it is critical to address the above issues on your personal smartphones and tablets, as well as your home computers and networks.

You must address all the dangers

Don't be tempted to ignore any of the dangers listed above, or to skip or skimp on the steps suggested to deal with them. Remember, your data and systems are only as safe as the weakest link in your security plan. When you leave on vacation, you lock every door and window in your house. Leaving just one door or window open gives a thief easy and instant access. To protect yourself from cybercrime, it is critical that you fully and properly address all cybercrime dangers. Cyber criminals will look for and exploit holes in your security plan.

Note that some of the configuration changes suggested in this article will require you to have "administrator" access to your device or systems. Operating your computer or device with the administrator account (or an account that has administrator status) will allow you to freely change your configuration or settings. A regular "user" account will not have the ability to change many device or software settings. To prevent regular staff from changing their settings and intentionally or unintentionally causing damage to your systems, everyone in your office should be using a "user" account, not an administrator account or accounts with administrator status. Doing your day-to-day work while logged into a "user" account can also reduce the damage that a malware infection will cause. Without administrator access, the malware will be restricted in its abilities to change settings on your computer.

As a final note, you may find yourself unable to change your configuration if your firm centrally administers and controls the settings for computers and other devices. Speak to your technology support person if you have questions or concerns.

Avoid the dangers of email

1

Email has become a primary communications tool for the legal profession. It allows virtually instant sharing of information and documents between lawyers and their clients. Email is also one of the most dangerous tools in a modern law office. Infected attachments, spam and phishing attacks delivered by email make it easy for cyber criminals to deliver malware and breach law firm security protections. It is essential that you educate your lawyers and staff about these dangers and the steps they should take to use email safely.

Be wary of attachments

While email attachments are frequently used to share documents between lawyers, law firm staff, and clients, they are also one of the most common delivery mechanisms for malware. While most messages that have infected attachments will be stopped if your anti-malware software and/or spam filter are working properly and updated, some will make it through. For this reason, everyone at a law firm should follow these two simple rules:

QUICK FIX

1. No matter how interesting or enticing they appear to be (e.g., jokes, celebrity gossip or pictures), never open attachments from strangers.
2. No matter how interesting or enticing they appear to be, never open attachments unexpectedly sent to you by people you know.

The reason for Rule #1 should be obvious – enticing attachments from strangers usually have a malware payload. The reason for Rule #2 might be less obvious: to trick you into feeling comfortable about opening an attachment, some types of malware will send an email with an infected attachment to all the address book contacts it finds on a computer that it has just successfully infected. This is done intentionally with hope that people getting such a message will be comfortable opening the attachment as it came from someone they know – and bingo – the person opening the attachment will become infected and all *their* contacts will get a similar message.

Use spam filters to avoid annoying and dangerous spam

On a daily basis you undoubtedly receive unsolicited commercial junk email, advertising or other offensive messages commonly known as spam. Spam is not only annoying – it is also very dangerous as it is commonly used to deliver malware (if you click on a link in the message) and phishing scams (see the next heading).

To combat spam, many firms use spam filters that are intended to detect unsolicited and unwanted email and prevent those messages from getting into a user's inbox. Spam filters use various criteria to identify spam messages, including watching for particular words or suspicious word patterns, messages that come from websites that are known to send spam, etc. Anti-spam products also use "blacklists" that intercept messages from recognized spammers, and "whitelists" that let messages through only if they come from your personal list of recognized email addresses or domains (the domain is the main part of an email address or website, for example, lawpro.ca or gmail.com).

QUICK FIX

If your email program includes a spam or junk mail feature, you should turn it on. For additional protection, consider installing a third party spam filter. They are often included in anti-malware suites. See page 14-15 for more information on anti-malware software.

QUICK FIX

While spam filters can significantly reduce the amount of spam you receive, they are not perfect. They will sometimes let spam messages through. Advise firm staff not to open or respond to spam messages, and to flag them as spam so that the spam filter can learn to recognize and prevent a similar message from getting through in the future.

QUICK FIX

Links in spam messages will often cause malware to be downloaded to your computer. For this reason, everyone at a law firm should be told to never click on links in spam messages, no matter how interesting or enticing they appear to be.

Don't be fooled by phishing

Did you know that emails appearing to come from companies you trust may actually be from criminals trying to steal your money or identity? Because they are so successful at duping people, "phishing" emails have quickly become one of the most common and devastating scams on the Internet.

Phishing scams use spoofed (meaning faked or hoax) emails and websites to trick you into revealing your personal and financial information. By using the trusted brands and logos of online retailers, banks, or credit card companies, phishing scammers trick surprisingly large numbers of people. The phishing email directs users to visit a website where they are asked to confirm or update personal information such as: passwords; and credit card, social insurance and bank account numbers. In doing so, people are tricked into giving this information directly to cyber criminals, who, in turn, use it for identity theft, financial theft or other cybercrimes.

Legitimate companies will never ask you to update your personal information via an email message. Don't get tricked by phishing scams. See the "Could it happen to you" column on page 32 to learn how to recognize and avoid phishing scams.

Lock down your browser and avoid surfing dangers

2

After email, your Internet browser is probably the second most dangerous technology tool in your office. Even casual surfing on the web can expose you to malware and other cyber security issues. You and your staff need to know how to safely surf the web and configure your browsers so that surfing is less dangerous.

Safely surf the web

Teaching your staff the following surfing "don'ts" will help you reduce cyber-related surfing risks, and reduce the likelihood of a malware infection:

- Don't complete online transactions involving account information, passwords, credit card numbers or other personal information, unless you are on a secure connection as indicated by an "https" in the website address (see sidebar on page 14).
- Don't visit unknown websites, and especially music, video, or pornography sites because they are often loaded with malware.
- Don't use file sharing sites, or services unless you are familiar with them and know the people you are sharing files with.
- Don't download software, unless it's from a reputable and trusted site.
- Don't download new apps (wait until downloads hit the thousands and it is likely any malware in the app has been detected).
- Don't download browser add-ons, plug-ins or toolbars, especially from unknown or untrusted sites.
- Don't click on "OK," "Yes" or anything else in browser "pop-ups" (the small windows that sometimes open within a browser). These are sometimes made to look like "dialog boxes" (the windows you change settings or options in) to make you think you are clicking on options or settings you normally deal with. Quickly closing all browser windows and tabs can help, especially if you are being flooded with multiple pop-ups. On Windows-based browsers use Ctrl+W or Alt+F4 to repeatedly close the top-most tab or browser window. In Safari, ⌘+Shift+w will close all tabs in the current window and ⌘+q will close all Safari windows and tabs.

Run an antivirus or anti-malware program that runs in the background and scans for dangers (see below for more information on anti-malware software).

If you are doing online banking for your firm trust or general accounts, it is critical that you ensure all security risks are addressed. See the "Increasing your online banking safety" sidebar on page 14 for the extra steps you need to take.

Beware the dangers of social media

Many people are comfortable sharing a great deal of personal information on Facebook, Twitter, Instagram and other similar social media tools. While family and friends may enjoy this information, people should keep in mind that cyber criminals could use the same information to assist them in personal identity theft or the hacking of online accounts. Be cautious about the amount and type of information you share on social media. Posting vacation pictures while you are away or using apps that broadcast your location (e.g. Foursquare) tells the world you are away from your home and office.

Facebook, Twitter, LinkedIn and some other sites can be configured to only let you login on a secure connection (see the adjacent sidebar on https connections). This can prevent your account from being hacked since your login credentials and connection are encrypted, making it harder for someone to intercept them.

Lock down your browser

Malware programs can automatically and secretly install themselves while you are browsing. These are called "drive-by downloads." This occurs when websites run scripts (small bodies of code designed to perform a specific action) or ActiveX controls (a module of code that adds extended functionality to the browser).

All browsers allow you to change individual configuration settings, many of which can deal with these and other security issues. Some browsers let you easily change multiple security or privacy settings by choosing from different levels of security (Medium-high or high are best). While changing browser settings can provide greater protection, it may also prevent some websites from running properly. While the options and terminology will change slightly between the various browsers, these are some of the settings you should change to lock down your browser:

- prevent pop-ups from loading (or prompt you before loading a pop-up).
- disable JavaScript.
- don't accept third party cookies.
- delete cookies on exit.
- clear history at close.
- disable ActiveX controls (or prompt to run ActiveX controls).
- enable automatic updates.

See the "Browser Security Settings for Chrome, Firefox and Internet Explorer: Cybersecurity 101" webpage for detailed instruction on how to lock down these three browsers. "iOS: Safari web settings" on the Apple Support site has information on Safari security settings.

There are also various browser plug-ins and add-ons that can increase browser security and warn you about suspicious activity. Widely used WOT (Web of Trust) will warn you about untrustworthy sites (available for all browsers).

Pharming

"Pharming" is another common trick used to perpetrate scams. Pharming takes you to a malicious and illegitimate website by redirecting a legitimate website address. Even if the website address is entered correctly, it can still be redirected to a fake website. The fake site is intended to convince you that it is real and legitimate by spoofing or looking almost identical to the actual site. When you complete a transaction on the fake site, thinking you are on the legitimate site, you unknowingly give your personal information to someone with malicious intent.

You can avoid pharming sites by carefully inspecting the website address in the address bar. Make sure you are on the site you intended to visit and look for "https" (see sidebar on next page) before you enter any personal information, passwords, credit card numbers, etc.

The S in https means you are on a safe and secure connection

QUICK FIX

When logging in on any website, you should always check for a secure connection by checking to see if the web address begins with https://..., as opposed to http://... Look for the "s" which signals that your connection to the website is encrypted and more resistant to snooping or tampering.

Avoid infections with antivirus and/or anti-malware software

3

Good behaviour alone will not protect you from viruses or other malware infections. You must run software that will prevent and/or detect infections on your computers, and you may want to consider it for your tablets and smartphones too.

But what is the difference between antivirus and anti-malware software? As explained in the "Common types of malware" sidebar on page 9, viruses are a specific type of malware. Malware is a

Increasing your online banking safety

Many law firms manage their trust and regular bank accounts on the Internet, and some firms have the ability to initiate various banking transactions online, including account transfers and wiring funds. While the convenience and efficiency of online banking are huge benefits, the downside is that online banking exposes you to security risks. The steps outlined below will help law firms to understand, address and reduce online banking risks – for both your firm and personal accounts.

- **Know and understand the terms of your banking agreements:** As a starting point, carefully read your bank account and electronic banking services agreements. Make sure you understand the obligations these agreements place on you with respect to using the account. In particular, make sure you are familiar with the notice requirements for unauthorized transactions, and who is responsible for unauthorized transactions. In most circumstances it will be you, unless in specified and usually narrow circumstances you give prompt notice to the bank.
- **Remove account features you won't use:** If hackers ever managed to get into your account, the ability to access multiple accounts or to initiate transfers or send wires could allow them to easily remove funds from your account. If you don't intend to use your online banking facility for these types of transactions, have this functionality removed from your account.
- **Only do online banking from a secure firm computer:** The computer used for online firm banking should be a firm computer that has all software updates installed, is running updated anti-malware software, and is behind a firewall. To reduce the potential for other cyber risks, consider restricting the activities that occur on the computer used for online banking.
- **Have real-time protection running and run regular malware scans on your banking computer:** This should hopefully help detect an infection as it is happening, or detect one that occurred without triggering the real-time protection warnings. See "Avoid infections with antivirus and/or anti-malware software" on page 14.
- **Never use public computers to do banking for the firm:** If doing so, passwords or account data may be accidentally stored on the computer or captured by malware making it accessible to others.
- **Never conduct financial transactions over an unsecured public Wi-Fi network:** Communications on an unsecured Wi-Fi connection can easily be intercepted. See additional comments on Wi-Fi at page 20-22.
- **Use a secure and unique password that is changed regularly:** Your online bank account should not have the same password as any other account. It should be a strong password (see the Tech Tip on page 30 to learn how to create a strong password). Online banking passwords should never be stored on a mobile device or anywhere else that could make them easily accessible by another person.
- **Check your online bank account every day:** By monitoring your daily account activity, you'll be able to promptly identify any unauthorized transactions or other indications that your account has been hacked. Check the last login time and make sure it is consistent with the last time someone from your office accessed the account. Immediately report suspicious or unexplained activity to your bank.
- **Configure email or text message activity alerts:** Most banking websites allow users to sign up for notifications. You will then receive an email or a text message whenever a specified amount of money is withdrawn or deposited to your account, or if there is unusual activity such as international transactions. Some banks will also phone a firm for confirmation that a transaction that was initiated online is to go through.

broad term used to describe many different types of malicious code, *including* viruses, but also Trojans, worms, spyware, and other threats.

Does this mean antivirus software will only protect you from viruses and anti-malware software will protect you from all kinds of malware, including viruses? The answer is, unfortunately, it depends. While most of the more popular tools will scan for many types of malware, you need to look at the specific functionality of each product to know for sure what it will protect you from. From this point forward this article will refer to the broader category of anti-malware software.

The options

Windows computers are prone to infections so you must run anti-malware software on them. Microsoft Security Essentials is a free product you can download to help protect computers running Windows XP, Windows Vista, and Windows 7. Windows 8 includes Windows Defender, also free. Both offer good real-time anti-malware protection.

There are a number of widely used commercial anti-malware programs, some that come in suites that include other functionality like anti-spam, firewalls, remote access, device location and scrubbing.

The two most widely used antivirus programs are Norton™ AntiVirus (symantec.com) and VirusScan (mcafee.com). Expect to pay $40-$60 per computer to buy the software, plus an additional annual fee for virus signature file updates (see opposite). Buying antivirus software that is bundled with other products, such as firewall and anti-spam software, will save you money.

Until recently, it was generally felt it was not necessary to run anti-malware software on Apple computers as the Mac OS architecture prevented infections and there were no real malware threats targeting Macs. There are now potential malware threats, and consider ClamXav, an effective and free antivirus program for Mac OS X computers. Note: If you run a Windows emulator on a Mac computer you open yourself to the full gamut of Windows malware risks and you must use a Windows anti-malware tool.

Tablets and smartphones are, in general, much less likely to get malware infections, but you may want to run anti-malware apps on them for greater protection.

As no one tool will catch everything, you may want to consider using more than one anti-malware tool. To better protect yourself, install one security tool that scans for as much as possible and that runs all the time in the background with an on-access scanning engine. This will protect you from threats as you surf the web, install applications, open files and complete your other daily activities. Then, install another anti-malware tool that you can occasionally use on demand to make sure nothing got through or was overlooked. Scan your entire hard disk(s) at least weekly, either manually or automatically (automatic is better as you don't have to remember to do it).

Bitdefender QuickScan is a free online scan that is handy if you need a second opinion on a Windows computer.

But note, it is important to make sure you do not run two antivirus applications simultaneously. Anti-malware programs do not usually play well together, and running two at the same time can often lead to one identifying the other as a virus, or in some cases, file corruption. Running two at the same time will likely also slow your computer down.

Malware can be extremely difficult to remove from a computer, so it is best to prevent infections. However, if you do get an infection, Malwarebytes Anti-Malware is a good free tool for removing malware from a Windows computer.

QUICK FIX

Installing anti-malware software updates is a must

Installing anti-malware software is only the start. You also need to regularly update your virus definition or signature files. Anti-malware programs use the information in these files to recognize virus infections when they are occurring. As there are new viruses being created every day, you need to have the most recently released virus signature file to be protected against all known infections. These updates are available on your anti-malware vendor's website. Expect to pay about $30-$40 per year for these updates.

Most anti-malware programs can be configured to download these updates automatically, without user intervention. Make sure the automatic update feature is enabled as this helps ensure that your protection is always up-to-date.

QUICK FIX

Staff can help you spot malware infections

Sometimes anti-malware software will not detect that an infection has occurred. While malware can be on a computer and never give any hint of its presence, in many cases there are clues that a computer is infected with malware. See the "How to recognize your computer is infected with malware" sidebar for a list of these symptoms. Teaching your staff to recognize these symptoms could aid in the earlier detection of an infection.

4 Lock things up by using passwords properly

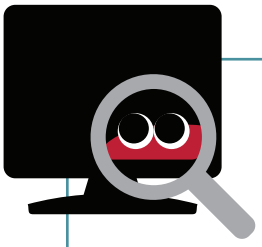
Like the keys that start your car or open the front door of your home or office, computer passwords are the keys that "unlock" your computer, your mobile devices and access to all the data on your network systems. We all have more passwords than we can remember. This tends to make us a bit lazy. We use obvious and easy to remember passwords – even the word "password" itself. Or worse: We don't use them at all.

Cyber criminals know and exploit bad password habits as they are often one of the weakest links in data security schemes. For this reason, it is critical that all lawyers and staff in a law office use passwords properly. The Tech Tip in this issue, "Keeping your passwords strong and secure" (see page 30), reviews the steps you can take to properly use and protect the confidentiality of your passwords, and how you can create passwords that are harder to guess or determine.

Address security vulnerabilities by installing operating system and program updates

5

There are millions of lines of computer code in the operating systems and programs that run on your computers, tablets and smartphones. These operating systems and programs will have hundreds or even thousands of settings and features. These settings and features are intended to allow you to do all the things you want to on these different devices.



How to recognize your computer is infected with malware

Ideally you have one or more types of properly updated anti-malware software running on your computers and networks. And hopefully that software detects and prevents any malware infections from occurring. However, because anti-malware software may not detect an infection, watch for the symptoms that can indicate a computer is infected with malware. These include:

- It takes longer than usual for your computer to start up, it restarts on its own or doesn't start up at all;
- It takes a long time for one or more programs to launch;
- Your computer and/or programs frequently lock up or crash;
- Programs are starting and running by themselves;
- Your hard drive runs continuously, even when you aren't working on the computer;
- Your files or data have disappeared;
- You find files with new or unfamiliar filenames;
- Space on your hard drive(s) is disappearing;
- The homepage on your web browser has changed;
- Your browser starts launching multiple tabs;
- Web pages are slow to load;
- There is a lot of network or web traffic, even when you are not browsing the web or using the computer; and/or
- Parts, or all, of your computer screen look distorted.

If one or more of the above things are happening, make sure your security software is up to date and run it to check for an infection. If the first scan finds nothing, try running a scan with a second product. If the odd behaviours continue or there are other problems, seek technical help.

Amongst all these settings and features, cyber criminals look for "exploits." An exploit is a particular setting, feature or sequence of commands that will cause an unintended or unanticipated behaviour to occur on a computer or other device. Exploits create security vulnerabilities because cyber criminals can use them to open a back-door to your network, allow malware to run, or do other damaging things. New exploits are discovered on a weekly or even daily basis.

Updates

When an exploit is discovered, software companies quickly rewrite their code and release updates or patches to stop the exploit from working. To protect against newly discovered exploits, devices must be updated with the latest versions of operating systems and programs.

To keep your computers and other devices safe, you should be checking for and installing updates regularly, ideally on a weekly basis. This is particularly the case for Microsoft products, which are prone to security vulnerabilities. While not as prone to vulnerabilities as Microsoft products, Apple products should be updated regularly as well. Don't forget to update the other non-Microsoft or non-Apple software running on your devices. Sometimes direct links to an updates webpage can be found on the Help menu. Otherwise, you should be able to find the software product's site with a search on Google.

If you are using Windows XP or Office 2003, note that Microsoft will no longer be supporting these products as of April 8, 2014. Using these products after this date will expose you to greater security dangers. See the "Stop using Windows XP and Office 2003 on or before April 8, 2014" sidebar if this applies to you or your firm.

Automatic updates

QUICK FIX

Enabling automatic updates can help keep your computers and other devices up-to-date. Both Windows and Apple operating systems have an "automatic update" feature that automatically notifies you when updates are available for your devices. Once activated, the device will periodically check for updates. Available updates will be downloaded, and depending how you configure things, installed with or without your knowledge. Some people prefer to set the automatic updates feature to ask for permission to install updates to avoid problems that might arise due to an update installation. Others prefer to have updates installed without intervention from the computer user (this can help make sure updates get installed).

QUICK FIX

The Ninite.com site can help Windows computer users check for and install updates (for free). Note, in some firms individual users will have no control over updates as the installation of updates will be centrally controlled and managed. The paid version of Ninite can be used for this purpose for Windows computers.

Back up before you install updates

It is very important to remember that installing updates can unintentionally interfere with the way your computer/device or individual programs/apps operate. It is possible that a program/app may not operate properly or at all, that data could be lost, or that a device will fail to restart after an update is installed. Creating a restore point (a temporary backup of your configuration and data) and/or making a proper backup of all the programs and data on a device before you install updates can help you recover if there are unanticipated problems. See page 24 for more information on backups.

6 Keep the bad guys out with a firewall on your Internet connection

When you are connected to the Internet, the Internet is connected to you. For computers to transmit data back and forth over the Internet, lines of communication must be established. These communications work through "ports" that are opened on each computer. The problem is that all the computers on the Internet can see one another, and these ports can allow unauthorized people to access the data on a computer and even take control of it.

Regardless of how your office connects to the Internet, your computer systems must be protected by a firewall – a type of electronic gatekeeper that ensures all incoming and outgoing communications are legitimate. A firewall watches these ports and will warn you about or prevent unauthorized communications.

Firewalls come in two varieties: software and hardware. Software firewalls are easier to set up, usually protect a single computer, and are adequate for personal or small firm use. Hardware firewalls are usually used to protect an entire network of computers. The more recent versions of both the Windows and Mac operating systems have a built-in firewall that you should enable. High-speed modems generally include a basic firewall. If you are using remote access software, you should consider using a hardware firewall to better protect the ports that must be opened for the remote access software to work.

7 Stump hackers by changing key default settings

Changing the default settings for the hardware and software used in your office is another critical step in safeguarding the security of your data and protecting yourself from cybercrime. This is probably the most technical of the steps outlined in this article and you may need expert help.

Every computer operating system, program, and app, and every piece of hardware has certain preset or default settings. These are necessary to make them operate out of the box in a consistent manner that the vendor and user will expect.

However, these default settings are common knowledge (and if you don't know them, you can find them with Google in about five seconds), and hackers can use them to compromise a network, computer or other device. For example, if the administrator account on a computer is named "Administrator" (it frequently is), a cyber criminal only has to work on figuring out the password to hack into a system or device. If you change the name of the Administrator account to something different, your computer is much safer as the hacker has to work much harder to figure out both the name of the administrator account and its password.

You can make your systems much safer by changing the following key default settings:

- administrator account names
- server names
- network or workgroup names
- ports (change to non-standard ports and close standard ports that you don't use)
- standard share names

Stop using Windows XP and Office 2003 on or before April 8, 2014

Microsoft will no longer be supporting Windows XP SP3 (Service Pack 3) and Office 2003 (SP3) as of April 8, 2014. After this date, there will be no new security updates, non-security hotfixes, support or online technical content updates from Microsoft for these products. Your computer will still operate, but if you continue to use Windows XP or Office 2003, you will become more vulnerable to security risks and malware infections. Undoubtedly, cyber criminals will target computers that are still using these programs. For this reason, you should immediately start planning to migrate to more current versions of Windows and Office on all law firm and home computers running Windows XP or Office 2003. Note that most current versions of these products are Windows XP SP3 and Office 2003 SP3. If you are using SP2 or earlier versions of these products, you already have greater security vulnerabilities; as a short-term fix, you should update to SP3 if you don't already have plans to move off Windows XP or Office 2003.

Lock down and protect your data wherever it is

8

Long gone are the days when you had to worry about a single file folder that held all the documents for a particular matter, which you could easily secure by keeping it locked in a file cabinet. Today, client data can exist in electronic form in many different places inside and outside your office. You need to know where that data exists, who can access it, and what steps should be taken to secure and protect it from cyber criminals.

Physical access to servers, routers and phone switches

Protecting your server(s) and other key telecommunications equipment such as phone switches and routers starts with physical security. Intruders who have physical access to a server can get direct access to files and data on the server's hard drives, enabling them to extract the usernames and passwords of every user on the system, destroy data, or give themselves a backdoor for accessing the server remotely. Even curious employees who want to change settings can unintentionally cause serious problems. Put your servers and other key telecommunications equipment in a locked room to protect them from unauthorized access. Be cautious about any wall jacks for your network in unsecured areas of your office.

Access to devices on startup

QUICK FIX To protect the information on them, and the information on any network they connect to, every computer, tablet and smartphone should be configured to require a password at startup. Devices without a startup password allow free and unfettered access to anyone that turns them on.

Better yet, in addition to a startup password, consider encrypting the data on devices. Passwords will prevent the average person from accessing your device, but can be bypassed by people with greater expertise. Encryption will make information on devices far more secure. QUICK FIX The operating systems on some devices have built-in encryption capabilities or you can install third party encryption programs or apps.

Put a password on your screensaver

QUICK FIX Activating a password-protected screensaver is a simple and very effective way to prevent an unauthorized person from rifling through the data on a computer or other device that's been inadvertently left on. All versions of Windows and Apple operating systems allow you to add a password to a screensaver. QUICK FIX Remember to log out of any applications containing sensitive data and lock your screen when you leave your desk, or set a fairly short wait time on your screensaver so that it locks automatically if you step away. BlackBerry, Android, iOS and Windows mobile devices also have an automatic screen-locking feature.

Access across a network

Almost every law office has a computer network with one or more central servers. Client and firm information can be stored on these servers, making it accessible to everyone in the office. To better protect information from unauthorized access, take time to understand what information is stored on your network servers, and who has access to that information.

"Network shares" make folders available and visible across a network. "Permissions" control what people can do with the data in a folder. Someone with "full access" can create, change or delete a file, whereas someone with "read only" access can open and copy a file, but not delete it. Segment your data and set appropriate access levels (e.g., public, sensitive, very private) so that access to sensitive information is limited or prevented. Remember that privacy legislation requires that you limit access to some types of personal information (e.g., financial and health-related data) on a need-to-know basis.

Restricting access to more sensitive data can help protect it in the event your network is hacked or an unhappy employee with bad intentions goes looking for data.

Your desktop or laptop computer can act like a server in some cases, and content on your hard drive could be shared and accessible to someone across a network or through the Internet. QUICK FIX To prevent this from happening, you need to make sure that file and printer sharing is turned off on your computer.

Scrub confidential client information on discarded equipment

9

Many of the technology devices used today are essentially disposable. When they get old or break down, they are simply discarded as it is too expensive to upgrade or repair them. As a result, law offices will frequently find themselves discarding older computers and other devices. This is problematic as these devices often have confidential client information on them.

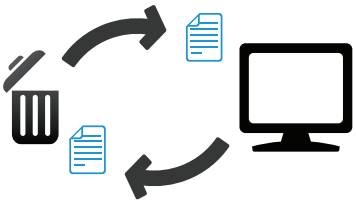
There are risks in donating your old computers to charity or a local school where a classroom of technology-savvy students will be itching to recover your data. Be sure to remove the hard drive from any computer you donate, or make sure the data on the drive has been thoroughly removed (see below).

Third party access to confidential client or firm information can also be an issue if you are sending your electronic equipment outside the office for repair or maintenance.

Client information can be in unexpected places. Most modern photocopiers and printers actually have hard drives on board that store copies of the images that go through them. This data can easily be found on, or recovered from, the hard drives on these devices.

Deleted doesn't mean deleted

It's a common misconception that deleted files are gone for good. In fact, the deleted files on most devices (e.g., computers, tablets,



smartphones, etc.) are easy to recover using widely available forensic recovery tools. Even reformatting or repartitioning a hard drive will not completely destroy all the data on it.

QUICK FIX Keep in mind that forensic technology can also be used to restore deleted files on portable media (e.g., CDs, DVDs, USB sticks, SD cards), so you should always use new media when sending data outside your firm.

Physically destroying a hard drive or other device with a hammer is the free and low-tech option. You can also use specialized software that will "scrub" all data from a hard drive so that it is not recoverable. Widely used free tools for this task include CCleaner, Darik's Boot And Nuke (DBAN), and File Shredder.

Being safer when using remote access and public computers 10

Being able to access your work network while you are out of the office can provide increased productivity and flexibility. However, opening your systems to remote access creates a number of security risks as external network connections are a ripe target for cyber criminals. And you should think twice about using public computers for firm work.

Setting up safe remote access

There are many tools that allow you to easily set up remote access (e.g., PCAnywhere, GoToMyPC, LogMeIn, TeamViewer, SplashTop). If properly configured, these are suitable for a smaller law office or home setting. Virtual private networks or VPNs may make remote access more secure. A VPN is a network connection constructed by connecting computers together over the Internet on an encrypted communications channel. VPNs are secure and fast, but may be expensive and harder to configure.

Securing remote access may require a degree of technical knowledge and advice from a computer expert. To make your remote access safe, you must secure your network and your remote access devices.

Do the following to secure your network:

- Use a firewall and security software to keep out unwanted connections.
- Only give remote access to people who really need it.
- In order to protect sensitive information, restrict the type of data that can be accessed remotely.
- Make sure all computers connecting to your network, including personal home computers, have up-to-date security software installed.
- Review firewall and other server logs to monitor remote access and watch for unusual activity.

Do the following to secure remote access:

- Ensure installation of remote access clients is done properly.
- Restrict access to the minimum services and functions necessary for staff to carry out their roles.
- Ensure that all staff use strong passwords on devices accessing your network remotely (see page 30).
- Change remote access passwords regularly. QUICK FIX
- Make sure that staff do not set their devices to login automatically and that they never store their passwords on them.
- Use strong authentication that requires both a password and token-based authentication.
- Have a formal remote access policy that clearly describes what staff are to do or not do with remote access.
- Delete staff remote access privileges if they are no longer needed, and immediately when a person leaves or is terminated (see "Inside people can be the most dangerous" at page 23).

The extreme dangers of using public computers

Public computers in libraries, Internet cafes, airports, and copy shops are an extreme security risk. While you can take steps to reduce these risks, it is still very dangerous to access sensitive client information on them. Start with the assumption that most public computers will have malware on them and let this govern your activities accordingly.

The following steps can reduce some of the risks associated with public computers: QUICK FIX

- Try to turn on the "private browsing" feature.
- Watch for over-the-shoulder thieves who may be peeking as you enter sensitive passwords to collect your information.
- Uncheck or disable the "remember me" or "log in automatically next time" option.
- Always log out of websites clicking "log out" on the site. It's not enough to simply close the browser window or type in another address.
- Delete your temporary Internet files, cookies and your history.
- Never leave the computer unattended with sensitive information on the screen, even for a moment.
- Never save documents on a public computer.

These measures will provide some protection against a casual hacker who searches a public computer you have used for any information that may remain on it. But keep in mind, a more sophisticated hacker may have installed a keylogger to capture passwords and other personal information entered on a public computer. In this scenario

the above steps won't prevent your information from falling into the hands of the hacker. This is why it is not a good idea to access sensitive client information or enter credit card numbers or other banking information on a public computer.

11 Secure your mobile devices to protect the data on them

Lost or stolen laptops, smartphones and USB sticks are frequently involved in major data breaches. This is because they often contain large amounts of confidential or sensitive information (e.g., client data, firm and personal information, usernames and passwords, etc.) and they are also easily lost or stolen as they are small and very portable. You can significantly reduce your exposure to breach involving a mobile device by doing the following things:

- Take steps to prevent mobile device theft or loss;
- Make it harder to access information on the device; and
- Configure remote "find and wipe."

Preventing theft or loss

Here are some very easy ways to prevent the loss or theft of your mobile devices:

- Never leave your portable devices unattended in a public place. In particular, don't leave them in your vehicle – even locked in the trunk is not safe;
- To be a less obvious target, use a briefcase or bag that does not look like a standard laptop bag;
- Inexpensive cable locks from Targus (targus.com) and others can help deter a casual thief, but are no obstacle for a determined thief with cable cutters; and
- If you are staying at a hotel, put the device in a safe in your room or at the front desk.

Making it harder to access data on the device

If a device is lost or stolen, you want to make it as difficult as possible for someone to access the information on it. This is very easy to do. As a first line of defence, you can enable the startup password. After enabling this feature, anyone turning the device on will be challenged for a password and they won't be able to see any information on the device. Most laptops and smartphones have this feature. However, while this should protect the data on the device from the average thief or person that might find a lost device, someone with specialized knowledge can bypass these built-in password-protection features.

For an extra level of security you can use encryption, which scrambles the data on a device making it very difficult for someone to access it. Some devices have an encryption feature in the device operating system, and, if not, you can use a third party encryption program or app. Truecrypt is a widely used encryption tool that works on many different platforms.

One other option to consider: if you allow remote access, have people travel with a device that has no client data or other sensitive information on it. They can use it to access client data in the office via remote access and if the device is lost or stolen there is no lost information to be concerned about.

You may want to keep in mind that current case law provides that law enforcement does not need the permission of a device owner to access information on a device that is not password protected.

Device locators and remote wipe

To prepare for the eventuality that of one of your smartphones, tablets or laptops gets lost or stolen, you should enable or install device locator and remote wipe functionalities. These features are built in on some devices, and there are many third party programs and apps that do the same things. Using GPS technology or the tracing of IP addresses, you can potentially view the location of your device on a web-based map, sometimes along with where and when it was last used. Just in case the device is lost in your residence, you can also trigger a high volume ring to help you locate it, even if the device is on silent or vibrate. If the worst has happened and it appears that the device is permanently lost or was stolen, you can usually lock the device so no one can use it or access the data, and you can also remotely tell the device to do a factory reset, which will delete all data on it.

Beware of data theft with USB sticks

Tiny, high-capacity USB sticks are commonly used for moving data around. A combination of three things makes them a major security concern: (1) they are very easy to use, (2) they are compact, light-weight and ultra-portable, and (3) they can store huge amounts of information. They are, in other words, the perfect tool for a disgruntled or soon-to-be ex-employee who plans to easily and quickly steal firm data.

How do you protect yourself? Make sure you have appropriate security and access rights to confidential client and firm information on your firm's computers and servers. Auditing file access may help you spot someone who is accessing information they should not. Consider disabling USB ports on firm computers used by people that have no reason to use USB sticks. Lastly, take extra care with employees who may be leaving the firm (see page 23).

12 Harden your wireless and Bluetooth connections and use public Wi-Fi with extreme caution

At home, coffee shops, restaurants, hotels, conference centers, airport terminals and many other locations, many of us use wireless and Bluetooth for our smartphones, tablets and even our computers without a second thought. While very convenient, anyone using wireless and Bluetooth should know that they are fraught with serious security issues. Unless you lock down your wireless network and

devices, someone sitting in a car across from your office or home could easily find and connect to them. Hackers known as "wardrivers" actually cruise around looking for networks they can hack into. There are even websites that list "open" networks by street address.

Hardening your wireless networks

Use wireless with caution, and only after you enable all possible security features on your wireless routers and devices. The hub of your wireless network is a router. It connects to your Internet service provider through a telephone line or other wired connection. Anyone connecting to your wireless network through your router can likely connect to the web and quite possibly access other devices on your network.

Completing these steps will make it much harder for strangers to connect to your wireless network:

- use WPA or WPA2 (WPA2 is better) or 802.1x wireless encryption. WEP encryption is found on older devices and it is recommended that you not use it as it can easily be cracked;
- turn off SSID broadcasting;
- disable guest networks;
- turn on MAC filtering;
- change default router name and password; and
- disable remote administration.

More detailed directions for completing these steps can be found on the practicePRO website in the "How to enable the security settings on a wireless router" checklist.

Bluetooth vulnerabilities

Bluetooth technology makes it easy for keyboards, headsets and other peripherals to connect to smartphones, tablets and computers wirelessly. Although security is available for Bluetooth, many vendors ship Bluetooth devices in Mode 1 (discovery/visible-to-all mode) to make it much easier for people using the devices to connect to them. In this mode they will respond to all connection requests. This introduces a number of vulnerabilities, including making information on the device more accessible to hackers and making the device more vulnerable to malware installation.

LAWPROFAQ

How do I get LAWPRO insurance coverage, now that I've been called to the bar?

Q. I have just been called to the Ontario bar, and will begin work for a law firm in a few weeks. I know I need insurance from LAWPRO – but that's all I know! How do I get started?

A. The LAWPRO program of professional indemnity insurance is approved each year by the Law Society of Upper Canada, and coverage under the program is mandatory for lawyers in private practice. When new lawyers are called to the Ontario bar, the Law Society provides LAWPRO with their contact information, and LAWPRO sends each new call a package of materials that includes information about the LAWPRO program and how to apply for coverage or, in certain cases, exemption from the coverage requirement. **Please note that you will not be automatically signed up for LAWPRO insurance coverage simply by virtue of being called to the bar.** LAWPRO and the Law Society of Upper Canada operate independently of each other, and you must contact each entity separately if you need to report a change in contact information or a change in practice status.

Applications for coverage or for exemption can be made online via a secure portal at lawpro.ca.

If you are a new call and you have NOT received a package (for example, because you have recently moved), please contact LAWPRO's customer service department to request a package.

More information

For more information about insurance requirements, exemption eligibility, run-off coverage, and other insurance issues, please visit the FAQ section of the LAWPRO website at lawpro.ca/faqs

If you have any questions regarding your coverage or practice status, please contact LAWPRO's customer service department by email at service@lawpro.ca, or by phone at 416-598-5899 or 1-800-410-1013.

To make your Bluetooth devices more secure, you should do the following:

- Configure devices so that the user has to approve any connection request;
- Turn off Bluetooth when not in use;
- Do not operate Bluetooth devices in Mode 1 and ensure discovery mode is enabled only when necessary to pair trusted devices;
- Pair trusted devices in safe environments out of the reach of potentially malicious people;
- Minimize the range of devices to the shortest reasonable distance;
- Educate your staff about how to safely use Bluetooth devices; and
- Consider installing antivirus and personal firewall software on each Bluetooth device.

Be extremely cautious with public Wi-Fi

Public Wi-Fi has become ubiquitous and a lot of people use it without a second thought. Unfortunately, there are major security issues with it. If you connect to a Wi-Fi network without giving a password, you are on an unsecured and unencrypted connection. On an unencrypted or "open" wireless network, anyone in your proximity can intercept your data and see where you are surfing (except if you are on an https website). Using an unencrypted connection to check the news or a flight status might be acceptable, but keep in mind that performing other activities is akin to using your speakerphone in the middle of a crowd.

Even worse, hackers will create fake Wi-Fi hotspots in public places to trick unwitting Wi-Fi users. "Free Starbucks Wi-Fi" may not be the legitimate Starbucks network. Connecting to a fake network puts your data in the hands of a hacker.

And don't equate subscription (paid-for) Wi-Fi Internet with secure browsing. It may be no more secure than open Wi-Fi.

To be avoid these dangers, it is best avoid using public Wi-Fi hotspots altogether. Get a device that has mobile cellular capability, tether to your smartphone, or use a mobile Wi-Fi hotspot. This is a small Wi-Fi router you carry around that has mobile cellular functionality. It gives you a personal and private Wi-Fi cloud you can configure to securely connect your other devices to.

If you are going to use public Wi-Fi, here are some steps you can take to connect your device as securely as possible:

- If your firm has a Virtual Private Network or VPN, use it. This will encrypt your data and make it harder for it to be intercepted.
- Never connect without using a password (this means you are on an unencrypted network) and avoid using Wi-Fi that uses WEP encryption as it can easily be cracked. Use networks that have WPA, WPA2 (WPA2 is better) or 802.1x wireless encryption.
- Enable the firewall and run updated antivirus software on your device.
- Turn file, printer and other device sharing off.
- Disable auto-connecting so network connections always happen with your express permission.
- Confirm the network name in your location before you connect (i.e., avoid the Starbucks imposter).
- Use sites that have "https" in the address bar as they will encrypt data traffic (See "The S in https means you are on a safe and secure connection" on page 14).
- "http" sites transfer data in plain text and should be avoided as a hacker can easily read the data transmissions. You could use browser extensions or plugins to create https connections on http sites.
- Follow the best practices for safe and secure passwords (see page 30).

By taking these steps you can reduce your Wi-Fi risks, but you should save sensitive tasks like online banking for when you are on a network you know is safe and secure.

13 Be careful about putting your firm data in the cloud

Almost everyone has data in the cloud, although many people may not realize it. If you are using Gmail or another free email service, iTunes, Facebook, LinkedIn or other social media tools, Dropbox, or doing online banking, your data is in the cloud. The "cloud" is the very large number of computers that are all connected and sharing information with each other across the Internet. If you create or post information that ends up outside your office, you are most likely in the cloud.

Cloud computing offers many benefits to lawyers. There is a vast selection of services, software and applications that can assist with just about every task in a modern law office, in many cases allowing those tasks to be accomplished more efficiently and quickly. Many of these services permit remote access, thereby allowing lawyers and staff to work from anywhere with full access to all documents and information for a matter. Using these services is usually economical as they can significantly reduce hardware and software maintenance costs and capital outlays. Storing data with suitable cloud service providers will likely mean that it is more secure and better backed up than it might be in a typical law office.

However, placing your client or firm data in the hands of third parties raises issues of security, privacy, regulatory compliance, and risk management, among others. Firms should have a process in place to ensure due diligence is performed and all risks and benefits are considered before any firm data is moved to the cloud. The evolving

standard from U.S. ethics rules and opinions seems to be that lawyers must make reasonable efforts to ensure any data they place in the cloud is reasonably secure. Contracts with any third party that is in possession of confidential client information should deal with relevant security and ethical issues, including having specific provisions that require all information is properly stored and secured to prevent inappropriate access.

The Law Society of British Columbia has a "Cloud Computing Checklist" that will assist firms in identifying the issues that should be considered when performing the due diligence on a cloud provider. When considering your options, keep in mind that a cloud product or service designed for lawyers may have been developed with the professional, ethical and privacy requirements of lawyers in mind.

Inside people can be the most dangerous

14

People inside your office have the greatest knowledge of your systems and where the important data is located. Many of the largest and most damaging cyber breaches have been caused by rogue or soon-to-be-departing employees. You should take steps to reduce the likelihood that a cyber breach will be caused by someone inside your office.

When hiring a new employee, make sure you are diligent. Carefully check their background and speak to references. Look for any red flags on an application letter or résumé, and watch for issues during the interview process. Watch for someone who is withholding relevant information, or who has falsified information on the application. Assess the overall integrity and trustworthiness of the candidate. Consider doing police and credit checks (after obtaining consent) as persons in financial difficulty may be under pressure and become tempted to steal your firm's financial or information resources. Doing all these things can help you avoid hiring an employee who could be a problem.

When any employee leaves your firm, regardless of whether they are leaving of their own accord or are being terminated, ensure that your systems are protected. Keep a log of any mobile devices held by your staff (e.g., laptops, smartphones, USB drives, etc.) and ensure that they are recovered immediately upon termination. Immediately close all points of access to your office and computer systems, including keys and access cards, login accounts and passwords, email accounts, and – in particular – remote access facilities. If you discharge an employee who has access to critical company data, let them go without warning (you may have to give them a payment in lieu of notice), and don't allow them any access to a computer after termination.

There are literally dozens of steps you should complete systematically to make sure all points of access for departed employees are closed down. See the practicePRO website for a detailed "Employee departure checklist".

If you have given vendors, IT consultants, contract or temp staff access to your systems or networks, remember to change system passwords and revoke access rights when they have finished their work.

Be careful of the dangers of BYOD and family computers

15

In many firms, it is common for lawyers to use personal smartphones or tablets for work purposes. This is often referred to as "Bring Your Own Device" or "BYOD." Lawyers or staff may also work at home and even access the office network from a personal home computer. Both of these practices raise significant cyber risks.

BYOD

Permitting staff to use their own smartphones or tablets makes great practical sense. They already own and are comfortable with the devices so the firm does not have to incur the cost of buying them or paying for wireless plans. However, if these devices connect to the office Wi-Fi or network, or if they are used to create documents that will be sent to the office, they can potentially deliver a malware infection to the office network.

Family computers

Young people have a very high exposure to malware as they are more likely to engage in many of the most dangerous online activities, including using social media, downloading programs, and file sharing. As a result, it is far more likely that any device children or teenagers are using is infected with malware. This is a concern because using a compromised computer for remote access to your office can bypass the firewall and other security mechanisms, potentially delivering a malware infection to the heart of your network.

To be absolutely safe, avoid using a home computer or other device for work purposes if it is used by others. Where a home computer is being used for work purposes, the steps outlined in this article must be followed to protect the office network and systems from cyber risks. Creating separate user accounts will make things more secure, but a better alternative is to have two partitions on your home computer. This essentially means there are two complete sets of software on the computer: one that only you would use, and one that others in the house would use.

Where a home computer or other BYOD device is being used for work purposes, the steps outlined in this article must be followed to protect the office network and systems from cyber risks. Staff education is key for reducing the risks associated with the use of personal equipment. Technology use policies should be in place to ensure all necessary steps are taken to address relevant cyber risks. See the practicePRO Technology Use Policies Resource page for sample BYOD and remote access policies.

A backup could save your practice after a cybercrime incident

16

Every law firm has huge amounts of irreplaceable data on its servers, desktop computers, laptops, tablets and smartphones. A cybercrime incident such as a malware infection or the hacking of firm systems could result in the destruction or loss of firm data. Having a current and full backup of all firm data will be essential for recovering from such an incident with the least possible interruption to a firm's operations. And beyond any concern about a cybercrime incident, every law firm should have a current full backup of firm data as part of its disaster recovery plan.

When keeping past copies of backups, consider that firm systems could have an undetected malware infection for a considerable period. If you have an undetected infection, you may have to go back in time to get a backup that is clean or has uncorrupted data. For this reason, you may want to keep a series of past backups (e.g., daily for last week, end of week for last month, end of month for last 3 months, quarterly, etc.) so that you can do a complete and clean restoration of your data.

There are many options for doing data backups, including using a dedicated backup system, external hard drives or other portable media, or the cloud. Apple users can easily set up an automatic backup with Time Machine.

QUICK FIX

Our "Data backup options and best practices" article, available on the practicePRO website, can help ensure you have a current and full backup of all the data in your office.

Conclusion

Cybercrime is a real and present danger to you and your firm. LawPRO strongly encourages Ontario lawyers to take this danger seriously and to take appropriate steps to reduce exposures to all relevant cyber risks. The "quick fixes" highlighted in the feature articles in this issue of *LawPRO Magazine* will get you off to a good start with minimal cost and effort. At many firms, further time and work will be necessary. This extra effort is worth the investment as, at the very least, a cybercrime incident will be a costly and significant interruption to your firm's business. And in a worst-case scenario, the financial and business interruption associated with a cyber breach could destroy your firm. ■

Dan Pinnington is vice president, claims prevention and stakeholder relations at LawPRO.

Thanks to David Reid, CIO at LawPRO, and Mike Seto, of Mike Seto Professional Corporation for their invaluable assistance.

Resources

Cyber security resources

Get Cyber Safe Guide for Small and Medium Businesses from Government of Canada: Practical information and guidance for firms on cyber security risks and how to avoid them. There are other helpful resources and checklists on the GetCyberSafe.gc.ca website.

Cyber Security Self-Assessment Guidance Checklist: A self-assessment template of cyber-security practices from OSFI that would be suitable for larger firms.

Cyber Security Resources for Teachers page on Media Smarts website: Various information and tips sheets for consumer and personal cyber-safety.

StaySafeOnline.org: Good general information and resources for staying safe while online.

Microsoft Safety and Security Center page: General information on cyber-security.

PCThreat.com: Comprehensive list of malware threats, tips on how to spot them and commentary on how to clean up if you are infected.

Snopes.com – The Urban Legends page: A website that lists common email scams and hoaxes.

ICSPA Canada Cyber Crime Study: Statistics and background information about cybercrime.

Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age Report: A report by the Ponemon Institute that contains an overview of cyber dangers.

Security Resources page on SANS.org: Extensive security information and resources on the site of this research and education organization.

Note: Live Links for these resources are available in the electronic version of this issue.

General technology resources

Technology page on practicePRO website: Large collection of article on the use of technology in the practice of law.

Technology books published by American Bar Association's Law Practice Division: Large collection of books on many technology topics. Many of these books are available in the practicePRO Lending Library (practicepro.ca/library).

Law Society of Upper Canada's Technology Practice Management Guideline: General guide on use of technology in a law practice.

The LawPRO $250,000 cybercrime coverage:

What it covers and why

As of the 2014 policy year, the LawPRO mandatory insurance program will include express coverage in the amount of $250,000 for losses related to cybercrime, as defined in the policy. This sublimit (or cap) of coverage provides a modest "safety net" for lawyers in the area of cybercrime exposure. We say modest because like the fraud risks the profession has faced over the years, there is no way to predict the total possible exposure, and prevention is a far better tool to deal with this societal risk than insurance.

In the specialized world of Canadian lawyers' professional indemnity insurance, the most common approach so far has been to expressly exclude coverage for cybercrime losses. In considering what LawPRO program protection should be made available to Ontario lawyers in 2014 regarding claims involving cybercrime, and what steps should be taken to better ensure that lawyers and law firms are aware of this growing exposure and what they might do to better protect their clients and themselves, consideration has been given to:

- The threat that cybercrime represents to clients and the viability of law practices in Ontario;
- The limited technology resources adopted to date by many members of the bar to comprehensively address cybercrime risks;
- The increasing availability of commercial business insurance to address the broader aspects of cyber risks;
- The growing and evolving nature of cyber risks and related need for increased awareness and active risk management by lawyers and law firms;
- The choices and options available to lawyers and law firms to reduce their vulnerability to cybercrime through adopting technology and security best practices;
- The potential impact of a systemic or catastrophic loss on the LawPRO program and premiums charged to lawyers, especially if a group of law firms experiences a loss; and
- The need for LawPRO to continue operating in a commercially reasonable manner and ensuring that risk-rating is maintained.

CYBERCRIME means an incursion, intrusion, penetration, impairment, use or attack of a COMPUTER SYSTEM(S) by electronic means by a third party, other than the INSURED or the INSURED'S LAW FIRM.

COMPUTER SYSTEM means any electronic device, component, network or system, or any protocol, portal, storage device, media, or electronic document, or any computer software, firmware or microcode, or any associated technology which receives, processes, stores, transmits or retrieves data either locally or remotely, or any part thereof, whether stand-alone, interconnected or operating as part of an integrated system or process, for use by or on behalf of the INSURED and/or the INSURED'S LAW FIRM.

In late 2012, LawPRO learned of a high-value cyber attack on an Ontario firm. The attack was highly sophisticated and complex, and was designed to permit the fraudster to gain direct access to a firm's trust account using online banking privileges. This attack, and media reports of many others, have served to demonstrate the potential exposure of the insurance program to losses arising out of cybercrime.

After careful consideration of the potential risk, including the potential for clusters of such claims across law firms, it became clear to us that a two-pronged response was warranted. For the 2014 policy year, we have opted to 1) explicitly address cybercrime risk in the mandatory insurance program policy, and 2) take steps to educate the bar about cyber risks and to recommend that all lawyers take active steps to prevent cybercrime before it happens.

Thus, as of the 2014 policy year, the LawPRO mandatory insurance program will include a sublimit of coverage in the amount of $250,000 for losses related to cybercrime as defined in the policy. See the sidebar for the definition of cybercrime, and the related definition of a computer system.

The LawPRO insurance coverage for cybercrime claims is only one of several aspects of a fulsome and responsible response to a complex problem. We urge you to carefully reflect on the extent to which, despite the coverage available under our policy, you remain vulnerable to the potentially serious consequences of a cyber attack.

Remember that any losses from cybercrime that are not connected with the provision of professional legal services will not be covered under the LawPRO policy. These losses could include damage to equipment or software, business interruption, and reputational harm. See "Other cyber risk insurance options: Do you have the coverage you need?" on page 26 for a basic overview of other types of insurance that firms may wish to consider to cover those risks or loss amounts that fall outside the LawPRO policy.

However, even where a firm chooses to obtain other coverage, insurance against cyber losses should be viewed as a worst-case remedy, and not a regime of prevention. If businesses insure themselves without taking active steps to secure their computers and networks, cyber criminals will continue their efforts undeterred.

Law firms and individual staff members and lawyers who work in them must educate themselves about cyber risks and take all reasonable steps to ensure that data and funds are securely protected. We hope that the content in this issue will serve as a useful resource in that regard. ■

Other cyber risk insurance options:

Do you have the coverage you need?

The prevalence of cyber-related crime has been steadily increasing for a number of years. Many businesses invest heavily in the necessary IT infrastructure to protect their data, but despite best efforts and intentions, the frequent news stories in the press should serve as confirmation that breaches do occur.

The cost implications of having personal or financial information stolen are significant, especially for law firms, because the information they hold can be confidential and even privileged, and is often very sensitive. When you consider all the potential first- and third-party liabilities a major breach could place on a law firm, the extreme cost could put a financial burden on a firm that could destroy it.

Thus, from an insurance standpoint, it is paramount to consider whether your coverage is adequate. Keep in mind that the coverage afforded under the LawPRO policy is subject to eligibility criteria and to a modest sublimit of coverage.

The evolution of the cyber insurance policy has made significant strides in recent years. The most common element of coverage found within cyber and privacy liability policies is for claims brought against you arising as a result of a breach. This would include legal defence costs and indemnity payments, and is provided on an "all risks basis." Some current extensions of coverage include protection against the spread of computer viruses, or in the event that your systems are used to hack a third party. Many policies have been extended to include first-party costs to comply with breach notification laws in different jurisdictions. Finally, cover can also be included for voluntary security breach notification which will help mitigate an impact upon the company's brand or reputation.

Coverage has also evolved to take into consideration the outsourcing of data storage to third-party cloud providers. While this endorsed coverage is still in its infancy, there are some insurers that are able to consider this type of risk.

Canadian Underwriter Magazine recently reported on a 2011 research study from NetDiligence, which found that the average cost of a data breach was $3.7M. The study found that the largest component of the costs related to the legal damages, with the average defence costs being $582,000, and the average cost of settlement being $2.1M. The implications of not handling a breach properly, measured by way of reputational harm to your organization, are costly. If that client trust is lost, it will certainly impact the gross revenue of your firm in terms of lost clients. With client acquisition being far more costly than client retention, having a plan in place to mitigate that reputational risk is very important.

Cyber and network liability policies have built in a solution for these types of situations. Many policies commonly offer limits of coverage for crisis management. The costs associated with hiring public relations consultants and costs to conduct advertising or PR activities are all things that can be built into a cyber policy.

Traditional insurance policies may offer a limited amount of coverage for cyber-related exposures, but it is important to understand the implications of relying on coverage that is not necessarily designed for a specific exposure. Property policies may not cover the loss of "data" because it may not be considered real or personal property. General liability policies are intended to cover bodily injury and property damage scenarios, and would not extend to cover network implications. Finally, in addressing these exposures, you should take into consideration liabilities that will fall outside the coverage offered by LawPRO's cybercrime sublimit.

As legislation changes and the breach notification requirements in Canada evolve, so too will the costs associated with damage from hackers, breaches, cyber extortion, and other cyber-related crimes.

Don't underestimate the costs your firm might incur in the event of a data breach. Reinforce the long-term security of your firm by ensuring it has taken adequate precautionary measures, has contingency plans in the event that something does occur, and has appropriate insurance in place to transfer and avoid the financial risks of a data breach. ■

Greg Markell, FCIP, CRM is an account executive with Jones Brown Inc. (gmarkell@jonesbrown.com)

While there are variations from provider to provider, insurance companies that offer cyber risk policies may include coverage for:

Lawsuits or claims relating to

- **inadvertent disclosure of confidential information**
- **intellectual property and/or business secrets infringement**
- **damage to reputation**
- **liability related to damage to third party systems**
- **impairment to access to systems or information**

And/or costs related to

- **privacy notifications, if required**
- **crisis management activities**
- **online and/or electronic business interruptions**
- **electronic theft, communication, threats and/or vandalism**

LawPRO FAQ

Reporting changes to information and changes in status to LawPRO and to the Law Society of Upper Canada (LSUC)

Q. As of last month, I have left private practice to become a law professor. I advised the Law Society of this change, and have been advised that I will be eligible to pay the non-practising lawyer membership fee. However, I continue to receive emails from LawPRO reminding me to renew my professional indemnity insurance. I thought that as an educator, I was exempt from the insurance requirement. What's going on?

A. It appears that you have not notified LawPRO of your change in practice status. If you're changing firms, contact information, or changing your status (going into or out of private practice), you should be sure to notify both LawPRO and the Law Society separately of these changes. LawPRO and LSUC maintain completely separate information databases and, in keeping with their respective mandates, generally do not share information that lawyers may consider confidential or proprietary. If you meet the exemption criteria, you should amend your status by completing an Application for Exemption, and forward it to LawPRO for processing.

More information

For more information about insurance requirements, exemption eligibility, run-off coverage, and other insurance issues, please visit the FAQ section of the LawPRO website at lawpro.ca/faqs

If you have any questions regarding your coverage or practice status, please contact LawPRO's customer service department by email at service@lawpro.ca, or by phone at 416-598-5899 or 1-800-410-1013.

Be ready

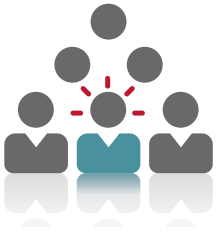
with an Incident Response Plan

Because a cybercrime attack can cause irreparable harm, law firms should be prepared to take action immediately. Being able to do this requires an Incident Response Plan, or IRP.

An effective IRP can put a firm in a position to effectively and efficiently manage a breach by protecting sensitive data, systems, and networks, and to quickly investigate the extent and source of the breach so that operations can be maintained or promptly restored. Many firms design IRPs so that they address inadvertent breaches as well – for example, a lost USB key, or a misdirected email. An IRP can help avoid many of the pitfalls of an ad hoc response, such as slow containment (leading to more widespread impacts and damage), lost productivity, bad press, client frustration, and even malpractice claims or discipline complaints.

A complete IRP addresses the detection, containment, and eradication of a cyber breach, recovery of normal operations, and follow-up analysis. When creating your plan, we encourage you to address the following issues:

Build an IRP team.



The size and composition of the team will vary depending on the size of your firm, but teams of all sizes should have a leader. If the firm employs IT staff, they will be key members of the team. There should also be representation from senior management, from the firm's main practice groups, and from the communications and human resources departments, if these exist. Roles and responsibilities for all team members should be documented in the firm's plan. Where necessary, team members should be trained in the procedures required under the plan.

Establish priorities.

In the event of a cyber attack, what should the firm's first priorities be? Presuming no staff are in physical danger, a firm's first priority is often protecting the confidentiality of client information. Identify and rank your priorities (be sure to include the need to notify LawPRO and/or your cyber risk insurer), and design your response accordingly. For example, the IRP may specify the order in which servers and services will be restored. Ensure that business objectives and priorities are met while negative effects on users are minimized.

Be ready to investigate.

To be able to respond appropriately, you will need to understand the nature and extent of the cyber attack or breach. If you have an IT department, there may be individuals on your staff with sufficient knowledge of forensic investigation to isolate the problem. Firms without an IT department should identify, in advance, the provider that would be contacted to investigate a breach, and record this contact information in the IRP.

Remember – non-IT staff may be the first to discover a cyber incident. Encourage your staff to report indications of trouble. See "How to recognize your computer is infected with malware" on page 16. In the event that a third party (for example, a client) detects a problem – for example, by receiving a phishing email – you should ensure that it's easy for third parties to identify the appropriate contact person to whom to report the issue.

Have a communication plan.

Prompt and effective internal communication is essential to an effective incident response. The IRP should have a "call tree" with current contact information that will govern communication between staff should an incident occur when many are out of the office. Contact information for outside IT and other service providers should be documented in the plan and kept up to date. It is useful, where the firm is trying not to immediately tip off the intruder, to avoid email communications – in these cases, phone, text, BlackBerry Messenger, or fax communication should be preferred.

It is useful to have a list ready in advance of outside parties who should be notified, along with current contact information. These parties may include the police, clients, insurers, credit card companies, a public relations firm, and your Internet service provider (be sure you have a current contact list saved outside your usual system).

Be technically prepared. While the details of breach prevention protocol are beyond the scope of this article, some of the basic protective steps firms can take are:

- create an inventory of computing resources;
- back up systems and data daily;
- create an offsite record, updated regularly, of client and service provider contact details;
- create a software archive and a resource kit of tools and hardware devices;
- create redundancy capacity for key systems;
- prepare a checklist of response steps;
- log and audit processes;
- use automated intrusion detection systems and a secure firewall; and
- use secure mechanisms for communication.

Have a containment plan.

As soon as a problem is identified, be prepared to make decisions about how to contain damage. IRP team members should have authority to lock down accounts and change passwords, to determine whether and which systems need to be shut down or isolated, and how to decide when it's safe to restore operation. It is useful for IRP members to document events and responses as they unfold – this record will be invaluable for the analysis of the attack once it's over.

Effectively eradicate threats.

Once the damage is contained, the firm will need to be prepared to resolve the incident by identifying and correcting all breach points, and eradicating all intruder leavings (malware, etc.). This is a complex and sometimes tedious process that may require external help.

Analyze the incident and the effectiveness of your response to help prepare for the next event.

Once the threat has been contained and then eradicated, the incident should be thoroughly analyzed. How did the intruder get in? What was he/she looking for? What did he/she accomplish?

You should also review the effectiveness of the firm's response. If there were any areas of confusion or parts of the plan that didn't work well, consider how those aspects of the IRP might be improved, so you'll be better prepared for the next attack when it happens.

While it takes some time and effort to create an IRP, being ready to respond to an incident in a coordinated and effective way can reduce damage to records and systems and minimize the impact of a cyber attack on your firm's productivity. Because the panic associated with a crisis can lead to errors and missed steps, it is much better to have thought these issues through calmly beforehand. ■

Nora Rock is corporate writer and policy analyst at LawPRO

techtip

Keeping your passwords strong and secure

Computer passwords are the keys that "unlock" our computer and network systems. We all have more passwords than we can remember. This tends to make us a bit lazy. We use obvious and easy-to-remember passwords – even the word "password" itself. Or worse: we don't use them at all. Bad password habits are often one of the weakest links in data security schemes. Cyber criminals know and exploit this fact.

For this reason it is critical that all lawyers and staff in a law office use passwords, and use them properly. This article reviews the steps you need to take to protect the confidentiality of your passwords, and how you can create passwords that are harder to guess or determine.

QUICK FIX Many of the password best practices mentioned in this article are very easy to implement – review them with your lawyers and staff.

Can you keep a secret?

Passwords don't work if they aren't secret. Unfortunately, people get careless and don't always keep their passwords confidential. These are the things you can do to keep your passwords secret.

Never ever tell anyone your passwords: This includes your IS support person (they can force a reset if they really need to access your account). And, make sure no one is looking over your shoulder when you are typing a password. If more than one person knows about a password, it isn't a secret anymore.

Never write down your passwords, especially on your monitor: Is this not the same as leaving the keys for your car in the ignition? Take a walk around your office and see how many passwords you can find on little notes taped to monitors or keyboards. If you absolutely have to write down some of your passwords to remember them, don't write them out exactly. Write without an obvious reference to the account they apply to, and so they have to be translated in some way. Add or delete a character, transpose letters, or vary them some other consistent way which only you can figure out.

Don't save passwords on your computer hard drive: It is not uncommon for people to create a document with all their passwords in it on their computer. This file can be located in seconds with a hard drive search, especially if it is called password.doc or if it contains the word "password" or other related terms like "username."

Use a password manager: If you must store passwords on your computer or smartphone, use a password manager. These handy programs remember and enter passwords for you and they are stored in an encrypted form so that they can't easily be accessed. Widely used password managers include 1Password, LastPass, and Robo-Form. Some password managers let you sync and use your passwords on multiple platforms and devices across the web. Very convenient, but depending on your personal preference and the work you do, you may want to be cautious about putting your passwords in the cloud. Make your password manager password extra complex! (And make sure you don't forget it.)

Use biometric scanners: Some laptops and the most recent iPhone have built-in biometric scanners that give you access to a device or other logins with a swipe of your finger or by facial recognition. These scanners help you avoid the need to remember passwords.

Don't use the same password for everything: This is very tempting, but is also very dangerous as anyone that figures out your password can get easy and instant access to all your other accounts. Use a unique password for each program, especially for very sensitive things like your network logon, remote access to networks or bank account logons. You also shouldn't use the same passwords for home and work purposes or on the administrator and user profiles on the same computer.

Change passwords on important accounts on a regular basis: For critical things like your computer and bank account, you should change your password every 60 to 90 days. This will foil a lurking hacker that has your password unbeknownst to you.

Change any compromised password immediately: Do this even if you only suspect a password has been compromised. Again, this is to foil a lurking hacker.

Don't use the "remember password" feature: Be wary of dialog boxes that present you with an option to save or remember your password. These can appear in your web browser and for remote access. By selecting this option you give unchallenged access to accounts to anyone sitting down at your computer.

Use two-step authentication

Using two-step authentication on sites that offer it will help to increase the security of your online information. Two-step authentication is a process involving two stages to verify the identity of someone trying to access online services.

You are already using two-step authentication if you withdraw money from an ATM. To access an ATM, you need two things: the ATM card and a personal identification number or PIN. If you lose your ATM card, your money is still safe; anyone who finds the card cannot withdraw money if they do not know your PIN. The same is true if someone knows your PIN and does not have the card. This second layer of security is what makes two-step authentication more secure.

More and more websites are offering two-step authentication, including Google, Facebook, Apple, Dropbox, Twitter, Microsoft, Amazon, Evernote, WordPress and Yahoo! Mail. You should enable two-step authentication if you are using one of these services.

Many of these sites have also added a feature that notifies you by email or text message if your configuration has been changed. In some cases you have to confirm the change for it to remain in effect. This protects you in the event a hacker gets into your account. If the hacker changes your password or other settings on the account, you get an email or text message notifying you of the change and you have the ability to prevent it from happening. Enabling this feature on any of your accounts that have it will help prevent those accounts from being taken over by a hacker.

Creating "strong" passwords

When you pick a password, you can't just use any password. It shouldn't be anything obvious and easy to guess, either by a human or a computer. Password-cracking tools continue to improve and they use one of three approaches: intelligent guessing, dictionary attacks and automation.

Intelligent guessing involves using words, phrases and key combinations that people commonly use as passwords. Intelligent guessing works reasonably well because most people use simple and obvious passwords (e.g., password, 12345, qwert, etc.). Dictionary attacks cycle through a complete list of words from one or more languages. Automated (or "brute force") attacks try every possible combination of letter, numbers and other characters. Given enough time, the automated method can crack any password. The computers we have today are much more powerful so passwords that used to take months to crack can now be cracked in days or hours.

So, your challenge is picking a password that is hard to break because it isn't short, obvious or a common word. This is called a "strong" password. For a password to be strong it should:

- Not contain your name or your computer user name;
- Not be a word associated with you (e.g., your spouse or child's name, street name, etc.)
- Not be a common word, name or phrase;
- Be significantly different from any passwords you have used previously;
- Be at least 12 characters long, and longer is even better;
- Have at least one symbol character in a position other than the first and last;
- Contain at least one character from each of the following four groups:
  a. uppercase letters A, B, C, ...
  b. lowercase letters a, b, c, ...
  c. numerals 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
  d. symbols (all characters not defined as letters or numerals, including: ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /

The best practice is to create a unique, complex and random password for every service you use. There are online tools that will create passwords with totally random characters. While these will be stronger, you will likely have to use a password manager to remember them.

Passphrases can help you remember complex passwords

If you follow the advice in the previous section, your password will be an unreadable mix of letters, numbers and characters. While good for security, they will be hard to remember. Consider using a "passphrase" to remember complex passwords. A passphrase is a mix of letters, numbers and characters that has a translation that makes it easier for you to remember the correct sequence. Here are some sample passphrases:

QUICK FIX

- !am@#1DJ!nuSSr "I'm a number one DJ in Russia"
- Rm@j0risKrayz "Our major is crazy"
- l@wPR0!sgr8! "LawPRO is great!"

Using strong passwords can help you better protect the confidentiality of client and firm data and systems. Encourage everyone at your firm to make sure all their passwords are strong and secure. ■

Dan Pinnington is vice president, claims prevention and stakeholder relations at LawPRO.

Could this happen to you?

Would you take the bait on a phishing scam?

"Phishing" is one of the most common scams that cyber criminals use because it can produce spectacular results with very little effort or expense on the part of the hacker. Phishing involves the use of an email, text message or phone call that appears to come from a trusted source or institution, vendor or company, but is actually from a third-party impostor. Phishing messages are intended to trick you into giving cyber criminals your information by asking you to update or confirm personal or online account information. Personal information and identity theft and/or payment scams are the motives behind most phishing scams. Thousands are phished – criminals only need one or two dupes to make it pay off.

Cyber criminals do their best to make phishing messages look official and legitimate. They will mimic real communications from the company or entity they are supposedly from by using the same layout, fonts, wording, message footers and copyright notices, etc. as official messages. They will often include corporate logos and even one or more links to the alleged sender's real website.

To make it more likely you will fall for the scam, phishing messages commonly involve urgent scenarios. They may suggest that you must reset your password because your account has been compromised by hackers or they may request that you login to your account to review an invoice or deal with an outstanding payment. Another common phishing scam is a call from someone claiming to be from Microsoft who will tell you your computer is infected and that you must go to a special website to download an update that will fix the problem. Phishing scams can also be a request to complete a survey or to give information to collect a prize you have won. They can also be requests for money supposedly from someone you know (see the "stuck in London" example on the next page).

Many phishing messages will include a link or attachment that you are asked to click so you can update your information. After doing so, the webpage or attachment you will see (which will also have text and logos to make it look official) will prompt you to enter your name, account number, password and other personal information – thereby giving it to cyber criminals.

To make matters worse, clicking on links or attachments in phishing messages often causes malware to be downloaded to your computer as well.

Could it happen to you? Would you fall for a phishing scam?

As you consider these questions, see the next page for some sample phishing messages.

How to spot phishing messages

Phishing scams work because some people are gullible. If you get a phishing message from a bank and you don't have an account there, you aren't likely to fall for the scam. However, if you have an account at that bank, the message may look legitimate to you and you are more likely to fall for the scam. Here are some clues that can help you recognize a phishing message:

- The link you are asked to visit is different from the company's usual website URL (see the next paragraph).
- The main part of the sender's email address is not the same as the company's usual email address.
- Bad spelling and poor grammar.
- Nonsensical or rambling content.
- The promise of receiving money or another big prize.
- Anyone asking for money – even if you know them (see the "stuck in London" message on the next page).

QUICK FIX

Checking the link you are asked to go to is one of the best ways to confirm that a message is a phishing scam. Place your mouse over the link you are asked to go to (but don't click on it!) and look at the taskbar in your browser window (usually at the lower left). It will show you the URL of the link. It should start with the proper characters in the proper website (e.g., lawpro.ca) and not a URL that appears unrelated (e.g., http://12.67.876/aed/1234/bnklogin). An unrelated URL virtually guarantees it is a phishing scam. Watch for small differences: "lawpro.com.tv" seems close, but is different!

QUICK FIX

Never respond to "phishing" requests for personal information in the mail, over the phone or online. Most importantly – this is probably the most common way that personal information is stolen – never ever reply to unsolicited or suspicious emails, instant messages or web pages asking for your personal information (e.g., usernames, passwords, SIN number, bank account numbers, PINs, credit card numbers, mother's birth name or birthday), even if they appear to be from a known or trusted person or business. Legitimate businesses should never send you an email message asking to send your username, password or other information to them in an email message. If in doubt, call the company yourself using a phone number from a trusted source. Don't use the number in the email – it could be fake too! ■

Dan Pinnington is vice president, claims prevention and stakeholder relations at LawPRO.

Sample phishing scam messages

A message pretending to be from RBC re hacked account

From : RBC (service@rbcanada.com)
Subject : Account Alert !

Actions for current recipient :

Dear your email address

Your password was entered incorrectly more than 5 times.

Because of that , our security team had to suspend your accounts and all the funds inside.

Your account access and the hold on your funds will be released as soon as you verify your information.

Review Your Account Activity

We are sorry for this inconvenience but this is a security measure which we must apply to ensure your account safety.

If you have already confirmed your information then please disregard this message

Thanks for choosing Royal Bank of Canada

The RBC Security Team

Copyright © 1999 – 2013 RBC. All rights reserved.

A message pretending to be from a debtor re payment request

From : Ann Tara <office@schaechle.com, herira7@aol.com>
Subject : Invoice Payment Confirmation

Actions for current recipient :

Hello

My name is Ann Tara , i was asked by my boss to send you the payment been made Earlier today.

Kindly see the attached payment slip for confirmation. Thus acknowledge the receipt of payment been made.

Thanks

Attachments
PaymentCopy.zip, 192330 bytes

A message pretending to be from Wells Fargo

From : alerts@notify.wellsfargo.com
Subject : Wells Fargo: Changes to Your Membership Checking Account

Actions for current recipient :

Important changes coming to your Membership Checking Account

There are important changes coming to your Membership Checking account that will take effect November 7, 2013.

Please sign on to view a secure message about these changes.

Thank you. We appreciate your business.

Sincerely,
Wells Fargo Online Customer Service
wellsfargo.com | Fraud Information Center
Wells Fargo Bank, N.A. Member FDIC.

Please do not reply to this automated email.

A message pretending to be from PayPal re account correction

From : PayPay l Inc.account@ppl.ca
Subject : Restore your account.

Dear PayPal Customer,

During our regularly scheduled account maintenance and verification procedure we have detected a slight error in your Paypal account.

This might be due to the following reasons:

1. A recent change in your personal information (ie. change of address, email address)

2. An inability to accurately verify your selected option of payment due to an internal error within our systems.

Please fill in all the details that are required to complete this verification process. To do this we have attached a form to this email. Please download the form and follow the instructions on your screen.

Please understand that this is a security measure intended to help protect you and your account. We apologize for any inconvenience.

If you choose to ignore our request, you leave us no choice but to temporary suspend your account.

Sincerely,
PayPal

Please do not reply to this email because we are not monitoring this inbox.

Copyright © 2013 PayPal, Inc. All rights reserved.

Attachments:

Restore.your.account.html, 11036 bytes

A message pretending to be from a friend via Google Drive

Google Drive. Keep everything. Share anything

Please check the document I uploaded for you using Google docs.

CLICK HERE just sign in with your email to view the document it's very important.

Thank You.

—

Someone you know
Street Address
Toronto, Ontario
Postal code

A message addressed to you from someone you know "stuck in London" asking for money

[Note: If you are getting this message, it likely means the person that it is from has had their email account hacked, likely by a phishing scam they fell for.]

Subject: Please help me

Hello,

I'm sorry for this odd request because it might get to you too urgent but it's due to the situation of things right now.

I'm stuck in London, England right now, I came down here for a short vacation then i was robbed, worse of it is that bags, cash and cards and my cell phone were stolen at GUN POINT, it's such a crazy experience for me, I need help flying back home, the authorities are not being 100% supportive but the good thing is i still have my passport and return ticket but currently having troubles paying off the hotel bills and also getting a cab to take me to the airport.

Please i need you to loan me some money, will refund you as soon as i'm back home, i promise.All i need is ($900 USD) but dont know how much you would be able to spare..we will be waiting to hear back from you on how you can get the fund to me please

Thank You

practicetip

Draw clients a roadmap to avoid communication claims

Our readers should now be well aware that problems with lawyer-client communication are the number one cause of malpractice claims. Managing communication takes patience and effort: at one extreme of the spectrum, responding to calls and messages from clients who want constant contact can be frustrating; while at the other end, trying to get absentee clients to update instructions or produce necessary documents can be time-consuming. How can you get the lawyer-client exchange off on the right foot from the beginning of a retainer, so that you don't feel either bombarded or ignored?

It helps to remember that the reason clients may communicate too much – or too little – can be that you've left them in the dark about how their matter is likely to proceed.

As lawyers, we sometimes forget that many clients have no frame of reference – other than movies or television – for what will happen in a typical legal matter. They may not know what the steps are, how long it will take, or how much it will cost. Common assumptions that lawyers make based on experience – for example, that the chance of an action going to trial is less than 20 per cent (or whatever it might be, in your practice area) – are not common knowledge to many clients. It's not surprising that, when the progress of a matter turns out to be slower, different, or more complicated than the client had expected, the phone starts to ring or the inbox to bulge.

You can improve your communication with clients and at the same time avoid malpractice claims by making the effort, at the beginning of each retainer, to provide the client with an overview or "roadmap" of how the matter can be expected to proceed. A good overview includes the following information:

- The typical steps and stages involved in the particular type of matter. Remember that a client may have had occasion to obtain legal services before, for a completely different type of matter, and may be assuming that this one will work the same way. You may find yourself explaining that a labour grievance is as similar to estate litigation as a goat is to a gorilla… they're both mammals, but beyond that…;
- An explanation of with whom the client will work at each stage. For example, if your legal assistant typically assists in the data-and-document-gathering stage of matters, let the client know that she will be hearing from the assistant; or if you handle family law agreements but refer away cases headed for trial, make sure the client knows this;
- A description of the assistance and participation you will need from the client (will she need to obtain documents from her employer? Undergo a medical examination? Attend at discoveries?);
- How long *on average* it takes to complete each stage in the particular kind of matter – as well as what the short and long ends of the range might be – and whether there are delays the client should know about (for example, clients may not know that a court can reserve a decision at the end of a trial, and may be shocked that they won't know the outcome until weeks or months later);
- Information about the impact of certain strategic decisions on the complexity, duration, and cost of a matter. Make sure that a client understands that time is money, and he should take into account the costs savings associated with early settlement when assessing the adequacy of settlement offers;
- The difference between fees and disbursements, and the general range for the expected overall costs (but be careful – many clients may hear and remember what you say about the lower end of the range more clearly than they remember the high end!); and
- The fact that, in a litigation matter, an unsuccessful party may be required to pay part of the successful party's costs.

This is just a suggested list, and deciding what belongs in the roadmap you draw will necessarily vary depending on what kind of legal work you do. For clues about what you need to include, pay attention to what kinds of questions you find yourself answering over and over in your communications. If you do legal work that follows a fairly predictable pattern (for example, residential real estate), you may even want to commit portions of this roadmap discussion to writing, in the form of a client handout – as long as you realize that handouts can never replace personal communication. A handout eliminates some opportunities for clients to raise important questions, and skimping on personal communication may make a client feel ignored – a recipe for trouble. For an example of a client handout precedent, see Hon. Carole Curtis' (former family lawyer, now a Justice of the Ontario Court) "Administrative Information for New Clients," available at practicepro.ca.

Finally, regardless of the content of your overview, you can improve the quality of your communication with clients by remembering to communicate just two pieces of information at the conclusion of every communication. No matter the reason for the call, visit, or email, always be sure that by the end of the contact, the client knows the answer to these two questions: 'what happens next?' and 'when will I hear from you?' Even if the answer is merely 'now, we wait; you'll hear from me when the other party makes a move', knowing where things are going reduces uncertainty, leaves the impression that a strategy is unfolding, and reaffirms that the lawyer will be in touch. ■

Nora Rock is corporate writer and policy analyst at LawPRO.

bookreview

The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals

Jill D. Rhodes and Vincent I. Polley

"There are two types of firms: those that know they've been (cyber) attacked and those that don't," says Jill Rhodes, co-author along with Vincent Polley of the *The ABA Cybersecurity Handbook*. The book is an initiative of the ABA Cybersecurity Legal Task Force that was created in 2012 to bring together the legal community and private sector to help secure law firm computer systems.

As described throughout this issue of *LawPRO Magazine*, law firms (as well as government and in-house lawyers) are tempting targets because of the wealth of confidential information they have about their clients, such as strategic business data, proposed mergers and acquisitions, intellectual property and information obtained through e-discovery in the course of litigation. And it isn't just hackers that can cause these breaches: it could be disgruntled or duped employees, lost mobile phones with lax passwords, or accidental damage (e.g. a flood) to computer hardware resulting in a malfunction of security systems.

This book was written as a resource for lawyers in all practice settings to help them develop a cybersecurity strategy. There is no single solution for every firm, and developing measures to increase security and respond to breaches requires balancing legal requirements, firm resources, staff training, investments in technology and client needs.

The authors first look at why firms are vulnerable and what steps they should be taking to increase their cybersecurity. The underlying problem is that lawyers are experts on law, not technology, and often don't have the kind of security arrangements big businesses or governments do. Data that was created in a secure environment can become exposed when it moves into the hands of a law firm with inferior security systems. Firms are under pressure to find efficiencies such as outsourcing, cloud storage and mobile devices, and each of these ways of dispersing client data adds another potential breach point. Lawyers and staff may also resist new security arrangements and the inconveniences these can bring.

At the same time, the authors point out that lawyers fundamentally understand the importance of client confidentiality, and that's a good starting point to make them embrace the importance of improved cybersecurity. Also, clients will increasingly press firms to have security systems as strong as their own.

The book describes how firms should do a risk assessment and develop plans to not only prevent security breaches, but also deal with them when they happen (and firms should make the assumption that breaches *will* happen). This assessment would cover all of a firm's data usage policies and the ways in which staff use and access confidential data. How to have a conversation with clients about data security (in terms of potential added costs and what to do in the event of a breach) would also be considered.

The next section of the book is an in-depth look at the legal and ethical obligations lawyers have to protect clients' data. As the book was written for a U.S. audience, the rules and laws described apply to American lawyers. However the basic principles would apply to Ontario lawyers, who will want to consider the Law Society *Rules of Professional Conduct* and bylaws as well.

The remainder of the book looks at how firms of various sizes can implement cybersecurity strategies. Small firms will have the flexibility to adopt new technologies and practices quickly, but may struggle with the costs, while large firms would have the opposite challenge. The authors also address how government and in-house lawyers can improve their levels of security.

For many firms, issues of cyber and data security have crept up on them in recent years, but recent high profile breaches of client information have added a sense of urgency. This book is a good resource for firms wanting to start a discussion with staff, clients and technical support providers about their own state of preparedness for a cyber attack or data breach. ■

Tim Lemieux is practicePRO coordinator at LawPRO.

About the practicePRO Lending Library

The practicePRO Lending Library has more than 100 books on a wide variety of law practice management topics. Ontario lawyers can borrow books in person or via e-mail. A full catalogue of books is available online (practicepro.ca/library). Books can be borrowed for three weeks. LawPRO ships loaned books to you at our expense, and you return books to us at your expense.

We have books on these topics:

- Billing & financial management
- Law firm management & administration
- Marketing & client relations
- Law office technology
- Career issues
- Wellness & balance issues
- Solo & small firm issues

For full descriptions of these titles, including downloadable tables of contents, go to practicepro.ca/library.

LawPRO has a corporate LinkedIn page, does your firm?

LawPRO has had a corporate LinkedIn page for almost two years now. We find it a useful tool to connect with lawyers and other legal profession stakeholders. It allows us to easily share LawPRO-related information with LinkedIn users.

As well as giving us a corporate presence and the ability to post updates, we have customized the "Products and Services" tab. On this tab we list seven items including: E&O insurance for Ontario lawyers, our practicePRO risk management program, TitlePLUS title insurance, excess insurance, *LawPRO Magazine*, our corporate social responsibility program, and the AvoidAClaim blog. Each item has a brief description; together they give a good overview of our mandatory and optional insurance program options and our risk management materials and resources.

If you don't have a firm page on LinkedIn you should consider creating one. LinkedIn highlights and shares information about the staff and lawyers from your firm that are on LinkedIn – and those that have left, as well – so it is a good idea to have a page for your firm. Did you know that if any one of your employees has a LinkedIn account and has added your company as an employer, LinkedIn will automatically create a generic business page? With over 225 million users on LinkedIn, there's no better time to claim that page and customize it to start promoting your firm, the lawyers and staff who work there, and the services you offer. LinkedIn can also be a helpful recruiting tool.

Don't forget! Connect with LawPRO:

Victoria Caruso is communications coordinator at LawPRO.

Social media profile: Kathleen Waters

Kathleen Waters
President and CEO

When asked how Kathleen has seen social media shape the industry she works in, she responds:

> **Social media allows us to be closer to our insureds and other influencers, and what could be better than that? We can see what they are interested in and they can see what we value as reflected in our posts. I receive more direct feedback from insureds about my social media efforts than any other aspect of my work at LawPRO.**

Time at LawPRO: 16 years

Kathleen has been active on Twitter and LinkedIn for the past two years.

Target audience:
- lawyers and paralegals
- real estate industry
- political stakeholders
- insurance regulators

Topics of interest:
- professional liability insurance for lawyers, including risk management and global insights
- LawPRO updates, primary, excess and TitlePLUS programs
- real estate issues in Canada and the U.S.
- insurance industry updates
- lawyer and paralegal education
- charity initiatives of interest to lawyers
- occasional updates of interest to feminists

LawPRO®
Lawyers' Professional Indemnity Company
lawpro.ca

practicePRO®
Risk management
practicepro.ca

LawPRO eXcess™ Insurance
Additional professional liability insurance
lawpro.ca/excess

TitlePLUS®
Title insurance
titleplus.ca

CANADA POST POSTES CANADA
Postage paid Port payé
Publications Mail
40026252

Return undeliverable Canadian addresses to:
LawPRO • 250 Yonge Street • Suite 3101, P.O. Box 3 • Toronto, Ontario M5B 2L7

AvoidAClaim.com

LawPRO

@LawPRO
@practicePRO
@TitlePLUSCanada

LawPRO insurance

TitlePLUS Home Buying Guide – Canada

< PREVIOUS