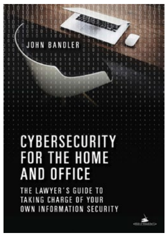
## New in the practicepro.ca lending library:

# Cybersecurity for the home and office:

## The lawyer's guide to taking charge of your own information security

*by John Bandler*


JOHN BANDLER
CYBERSECURITY FOR THE HOME AND OFFICE
THE LAWYER'S GUIDE TO TAKING CHARGE OF YOUR OWN INFORMATION SECURITY

For many lawyers, the divide between "home" and "office" isn't clear-cut. Work is often done in both places and during the trips back and forth. As a result, sensitive client information may not always be protected under the umbrella of a firm cybersecurity system. *Cybersecurity for the Home and Office* can help lawyers understand the threats they face and what they can do to secure their home devices and networks. It is also a great introduction to cybersecurity issues for solo and small firms which may not have an IT department to advise them. The author is John Bandler, who runs a New York state law firm and consulting practice that helps businesses with cybersecurity matters.

Before explaining how to improve your cybersecurity, Bandler gives a very good overview of why your data is so lucrative to criminals and how they can put it to use. It's obvious why trust fund money or sensitive information on clients would be targeted, but that's just part of the picture. Almost any data stolen from your computer can be monetized by criminals. Credit card numbers and email addresses can be sold in huge batches on black market websites. A password to a website that may have no valuable information might help crack a password to more important sites. And your computer itself might be hijacked without your knowledge and become part of a network to help hackers attack websites or hide their illegal transactions. So it's important to take stock of the vulnerabilities in your home office.

Bandler makes the point that any cybersecurity is a compromise between confidentiality, integrity and availability ("CIA"). Confidentiality of client data is generally the most important of the three to the legal profession, and includes strong passwords and encryption. Integrity is ensuring that your data can't be tampered with and is recoverable in the event of a breach or equipment failure. Availability refers to having access to your data when you need it. Compromise comes into play because increasing confidentiality (with, for example two-step authentication or limiting the access of family members) can come at the cost of easy availability. Another way of visualizing your home cybersecurity is a dial of 0 to 10 (or 11, in Bandler's *Spinal Tap* reference to extreme, and probably unnecessary, security measures). Most people will choose somewhere in the middle between reasonable security and ease of use.

The book spends a few chapters going through each component of a modern home network and explaining how each part interacts with the other. This will be very handy to those who usually leave the nuts and bolts of their computer to the firm IT department or their kids. It explains memory, storage (internal and external), devices you can attach to a computer, modems, routers, and both wired and wireless networks. Each is a potential access point for hackers or malware, and Bandler offers tips on how you can best secure them. The advice includes fairly simple security solutions that are often enough for a normal home network, all the way up to more complex arrangements for those who feel they need greater protection and are comfortable making more technical adjustments.

Increasing security goes beyond simply ensuring your WiFi has strong passwords or your storage drives are encrypted. You'll also need to take into consideration the family that may share access with you. Children (highly skilled at computers and getting around security arrangements) and seniors (sometimes not computer-savvy enough to spot a security problem) have their own particular risks you will have to take into account. If you have staff accessing your home office, that can also multiply the points of vulnerability. And when travelling with your laptop there are dangers from theft and connecting to unsecured networks.

The book includes a number of checklists to help you take stock of your cybersecurity situation, including a home device inventory, checklists for decommissioning old tablets and phones and a point-based system for assessing your vulnerabilities.

It's not possible to ever achieve total cyber peace of mind, as the criminals constantly come up with inventive ways to hack or bypass any security system. But that doesn't mean you have to make it easy for them. Many of the suggestions in this book can be implemented by most people with an ordinary amount of computer knowledge, and there is a lot of fascinating information included on how your data makes money for cybercriminals. By investing a little time and effort before there is a problem you can avoid the headache of trying to recover data and deal with the fallout of a security breach.

*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 email. 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 its expense, and you return books at your expense.* ■

**Tim Lemieux is Claims Prevention & Stakeholder Relations Coordinator at LAWPRO.**