

D-I-Y SECURITY

Guarding Your Data Is Just Common Sense

JASON KRAUSE

SECURITY IS A SHIFTING CONCERN AT Kaufman Law, David Kaufman's Fairfax, Va.-based firm. His work ranges from mundane "mom and pop" legal work to classified government assignments, and the firm's size fluctuates from a solo shop to a team with as many as four attorneys and even more support staff.

Kaufman has some stringent security measures in place to protect the work he does, but he says law office security is most dependent upon common sense. "I'd say 90 percent of having good security is just a matter of having your brain switched on," says Kaufman.

Any solo practitioner, for little cost, can have the same anti-virus protection and anti-intrusion firewall that large corporations have. But truly creating a secure computing environment means not just running the latest software, but knowing the risks and playing it safe.

One secret in the software world is that it is possible to secure your computer for free. For example, Grisoft Inc. makes free versions of AVG brand anti-virus and computer protection software. And Spybot and AdAware, two popular programs used for finding and deleting programs that could compromise computer security, can be downloaded free of charge.

The free versions are very basic, however, and the more advanced versions have price tags. "You can have effective security services set up for free," says Ben Sherwood, a personal security adviser in Milwaukee. "The main disadvantage is that you don't get everything you need in a single suite."

Companies like Symantec and McAfee offer complete

security software suites that feature firewalls, which block outside intruders, as well as anti-virus protection and spyware detection/removal all in one package. But once this software is installed, it is important to make sure you get the latest updates from the vendor's Web site at least once a week.

It's also important to make sure your operating system and security software have the latest patches and updates from the vendor. Most software can be programmed to automatically check for updates, which helps ensure protection against the latest types of hacker attack.

If you keep sensitive client documents on a computer, it is advisable to use the highest levels of security to protect them. Sherwood uses a fingerprint reader for added security on his computer. One simple thing to do when protecting a computer, he says, is to use complex passwords consisting of letters, numbers and keyboard symbols.

For advanced protection, programs like Hushmail make it possible to encrypt e-mail documents so that only the intended recipient can read them. Popular programs such as Microsoft Outlook also make it easy to send encrypted e-mails.

To use encryption in e-mail, all you need is a digital certificate, which Outlook will automatically help you find, and which costs about \$20. In fact, using encryption is something small firms can do better than large ones because it's difficult to keep track of the large number of digital keys used to read encrypted e-mails. "If you're a small firm," says Sherwood, "I feel it's a great way to show clients you value their assets."

SECRET LEAK

ONE THING MANY LAWYERS don't realize is that, even if they're protected against intruders, private information is sometimes being broadcast by their computers

anytime a document is e-mailed. Metadata is information embedded in a computer file about the file itself, such as when it was created, who created it or when it was last modified. A tech-savvy individual can look for metadata to see who last drafted it, or look for versions of earlier drafts.

Fortunately, there are ways to strip out metadata. In Microsoft Word, saving a document in the Rich Text Format, or .rtf, will eliminate such information. Many attorneys have learned to only send electronic documents in a



format like .pdf, which eliminates most metadata, offers security controls and can prevent others from editing the document.

One difficult new security wrinkle is wireless Internet access. For many lawyers, WiFi technology allows them to work in places like airports and coffee shops, dramatically increasing productivity. "I use WiFi a lot. I couldn't live without it," says Kaufman. "But if you don't protect yourself, you're just asking for trouble."

Sherwood says the key with using WiFi is to make sure that you are not an easy target. WiFi hackers can log onto the same wireless hotspot you are using to get online and look for people whose computers are not protected. Because WiFi is a shared network, they might be able to steal documents over the network.

"Make sure you're not the low-hanging fruit," Sherwood says. "If you're paranoid, you shouldn't be using wireless at all. Wireless is inherently insecure."

Common sense will always be important to securing your firm's intellectual property. Take steps to make sure that documents are not left in places where someone can see them. Back up all of your documents several times during the day, and make sure that they are kept where no one can walk off with your entire backup system. But most of all, to be a security guru, a lawyer needs to combine common sense with a little research. Web sites like www.ftc.gov explain the most recent computer scams.

At some point, though, security is out of your

hands. There are limits to what you can do.

"There's not a lot you can do about security risks from your staff other than to run training and make sure everyone understands what to do," says Kaufman. "But there's absolutely nothing you can do about clients. Once a document is out of your hands, you have to just trust that it's being taken care of." ■

Computers can be secured for free by downloading basic anti-virus and computer protection software.



HARVARD LAW SCHOOL

37th Program of Instruction for Lawyers

June 13-24, 2005

Harvard Law School offers five intensive workshops in mediation and negotiation during a two-week period in June. All workshops are taught by Harvard Law School faculty.

Negotiation Workshop: Creating Value in Deals & Disputes

This workshop, by combining lectures, exercises, case simulations and small group debriefs, aims to improve the participant's understanding of negotiation and effectiveness as a negotiator.

Advanced Negotiation: Deal Design & Implementation

This course will explore the inevitable tension between creating and claiming value; structural, psychological and interpersonal barriers that can hinder agreement; and the particular complexities inherent in the lawyer's role as negotiator.

Mediation Workshop

This workshop is currently available via waitlist only. Those interested in Mediation should email their contact information to pil@law.harvard.edu.

Negotiation Workshop

This workshop is designed to provide participants a conceptual framework for analyzing, preparing, and conducting negotiations, and to give them some experience in using this framework.

Advanced Negotiation: Understanding & Managing Difficult Conversations

The workshop offers a systematic approach to diagnosing communication and relationship problems and transforming difficult conversations into learning conversations.

Courses and workshops have been approved for mandatory continuing legal education credits in all states to which we have applied.

Please visit our website for more information or to obtain an application:

www.law.harvard.edu/academics/pil

**Program of Instruction for Lawyers
Harvard Law School
Cambridge, MA 02138**

TEL: 617-495-3187

FAX: 617-496-2869

E-MAIL: pil@law.harvard.edu