Chicago Daily Law Bulletin®

Volume 162, No. 176 Serving Chicago's legal community for 161 years

Your firm may be small, but don't think you are safe from cybercrime

Still using that old "my-name-law@yahoo.com" e-mail address for your solo firm? Do your online accounts have easily remembered passwords such as a pet's name or a significant date? Ever conduct business on public Wi-Fi at the local coffee shop?

If you think hackers stalk only large law firms, think again. Internet predators are working 24/7 to steal information belonging to lawyers and their clients. Sole practitioners who lack proper safeguards can be prime targets.

Data breaches may lead to monetary and reputational losses, and under the recently promulgated disciplinary Rule 1.6(e), lawyers can be sanctioned for not taking reasonable steps to prevent unauthorized access to client information.

Longtime practitioner Michael Hannigan, a member of Konicek & Dillon P.C., defends lawyers accused of professional negligence and triages the damage caused by cyberattacks. Hannigan explained that most self-employed attorneys do not have data security specialists on staff and thus must be extra vigilant in anticipating and avoiding security lapses.

Wire transfer schemes, 'ransomware'

Although cyberschemes constantly evolve and adapt, Hannigan described two emerging online frauds that could paralyze a solo practice: diverted wire transfers and "ransomware" that locks down your computer.

Wire transfer swindles single out attorneys whose clients move money electronically. The fraudster hacks the lawyer's e-mail account and monitors upcoming transactions. When the lawyer e-mails wire instructions to the client, lender or transmitting bank, the e-mail is intercepted and replaced (or "corrected") with false instructions to a rogue account.

By the time the scam is discovered, the funds have been withdrawn and the thief has disappeared.

Ransomware is malicious software unknowingly downloaded from seemingly innocuous websites or contained in e-mail attachments that may masquerade as PDF files. The self-installing program encrypts or locks down the victim's computer, which can only be opened with a password supplied by the attacker, in return for substantial payment.

Your grim choices are to pay the hefty ransom — possibly more than once — or lose all access to your system.

Thwarting hackers, securing data

Hannigan cautioned that all sole practitioners should hire a qualified IT security consultant, who can implement appropriate safeguards for your particular practice. In the interim, there are basic measures that may keep web intruders at a distance.

1. Verbal confirmation for wire instructions. When it comes to electronic fund transfers, low-tech security is best. Require the transmitting bank to obtain your verbal confirmation for all wire transfers.

SOLE SPEAK

GLENN E. HEILIZER

Glenn E. Heilizer is a veteran litigator and sole practitioner based in Chicago and is the founder of the Sole Practitioners Bar Association of Illinois. He handles commercial disputes in the federal, state and appellate courts in Illinois and Wisconsin. He welcomes all questions and comments, and he can be reached at glenn@heilizer.com.

Data breaches may lead to monetary and reputational losses, and under the recently promulgated disciplinary Rule 1.6(e), lawyers can be sanctioned for not taking reasonable steps to prevent unauthorized access to client information.

2. Security suite programs on all devices. The traditional firewall-antivirus programs now have more expansive protections that avoid malicious websites and screen potential downloads for security threats. Whether you choose Norton, McAfee, Kaspersky or another product, make sure all your computers, tablets and smartphones are protected and download the updates regularly to stay current.

3. Password manager. Your online accounts require random, complex passwords that meet today's security protocols. LastPass has a free version that will generate secure passwords, maintain them in a "vault" in the cloud and even autofill when desired for ease of use. If you prefer a password manager-generator that resides only on your desktop, Password Safe is a free program that can fit the bill.

4. Two-factor authorization. Many web-based services offer a further layer of security beyond the typical username and password, by texting an additional required code to your phone. For an unofficial list of companies that offer two-factor authorization, check out twofactorauth.org.

5. Back up your data. Avoiding the damage of a ransomware attack is just one of many reasons to back up your data. Although many firms choose the cloud storage option, local backups can be made to physical external drives as well. Each method has its pros and cons, but regardless, backing up your data is a must.

6. Avoid open source e-mail accounts. The FBI warns that free e-mail services may carry an increased risk of attack. If you are still using AOL, Yahoo or Gmail for your solo practice, it is time to acquire a unique domain name for your firm and establish e-mail accounts under that domain.

7. E-mail encryption. E-mail encryption is an ultra-safe way to communicate with clients, but it does require the exchange of digital signatures with recipients to decrypt messages. ProtonMail offers a free option with limited storage and use of the protonmail.com domain, or for $5 per month, users receive ample storage and can import their own domain.

8. Web-based, attorney-client portals. For a one-stop option that packages a number of the above safeguards, consider a web-based program designed for lawyers. For example, MyCase offers a client communication, document management, billing and calendar system, where attorneys and clients securely store, share and download information about their cases. With a monthly fee of $39 per attorney, the service is well-suited to sole practitioners and a free, no-obligation 30-day trial is available.

Hannigan's parting advice to sole practitioners? Develop a mindset that makes data security an absolute priority, and be proactive. Hackers are attempting new invasions every day. Lawyers cannot afford to be complacent. Stay informed and incorporate updated security measures into your practice as they come along. And, for goodness' sake, avoid public Wi-Fi.

(For more information on these and other strains of cyberfraud, or to report one, visit the FBI's Internet Crime Complaint Center at ic3.gov.)