Can Marketing Make Your Law Firm Vulnerable to Cyberattacks? Absolutely.

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

The objectives of marketing and cybersecurity are not the same

On the one hand, you want to get the word out about your law firm, its lawyers and its services. Inevitability, that means giving away information that might be used by a cybercriminal. Every piece of information you give a cybercriminal may be weaponized. The more sophisticated the attacker, the more they will ferret out information (especially in wire fraud cases!) to use against you.

The marketing objective is to get clients. The cybersecurity objective is to keep your data safe. Those two objectives are often at odds with one another.

Law firm websites

Take a hard look at your law firm website. Not every element below will be on every law firm website, but a lot of them will be. Think about the ramifications of each element.

Typically, law firms give a glowing description of their practices, including history, number of attorneys, and some list clients. There has been a real shift in the last few years from making prospective clients fill out a contact form to having attorney emails included on their bio page. We did an informal survey of law firm websites, including those of BigLaw and were amazed at how many included the email address of their lawyers.

Make no mistake about it – they are right to do that from a marketing point of view. Law firms will receive many more emails from prospective clients with an email address listed. It's instantaneous contact with a lawyer – which is what prospective clients wants.

We do the same thing – because it works.

Many sites have extensive bios which give away all kinds of information about a lawyer's education, former employers, firm phone number, listings of honors and recognitions, and sometimes, in an attempt to humanize lawyers, personal information, including the names of wives and children, hobbies, etc. Attorney photos are customarily posted – and have been known to be hijacked to create phony profiles or websites. Law firms often post videos or podcasts rife with information useful to a cybercriminal. We think it's marketing but in the cyber world, it's called advanced reconnaissance.

What are you doing about security?

Have you had your network security (including the security of your website) professionally assessed? Law firm web applications can be a way to steal your data or exploit vulnerabilities in your network. The harm that can be done does not bear contemplation. Yet again, another reason to host your firm's website somewhere not connected to your network.

For most law firms, a security assessment will suffice. If you are big enough, you may want a penetration test in which "good actor" act like "bad actors" to see if they can penetrate your network and what damage they can do. Penetration tests are far more expensive than assessments, so we generally recommend them only for larger law firms.

There are a lot of ways to fail an assessment – and they will all be identified in a report, but here are a few to think about. If you don't encrypt emails with sensitive data, have two-factor authentication enabled, an endpoint detection and response solution and a way to monitor for attacks, you will fail the assessment – the good news is that you will have identified all critical vulnerabilities and can address them immediately, while you figure out how and when to address the lesser vulnerabilities.

Reviews and testimonials on your website

Reviews and testimonials praising your work can be very useful marketing tools. Law firms often seek client testimonials for their website, understandably, but unless they are carefully vetted, they may give a criminal information which would help them target your clients. Not at all what you intended, but a real danger in today's world. If they impersonate your email address and target your client, the consequences could be serious.

Email signatures

Signatures have grown in size in many cases. Lawyers list many things about our firm, the firm's physical address, the areas of law we practice in, honors and certifications, our social media handles, our email addresses, the firm's social media sites, etc. Today, this constitutes good marketing.

Someone who is targeting you or your law firm, especially in a sophisticated cyberattack, will gather information from your email signature, hoping that some of it will prove useful in attacking your firm.

Law firm and lawyer social media marketing

More attorneys use LinkedIn than any other social media site. There you will find much of the information cited above in the firm website. Should you accept a contact invitation, that person (by default) will be able to see your other contacts. And, the contact invitation may be bogus, to maximize the chance that you will accept the invitation.

Commonly, lawyers list licenses and certifications, as well as list their skills and recommendations from others. Then there are their publications, their honors and awards, their interests, etc.

Of course, you may be using Facebook, Twitter (which is steeply declining) or other social media sites. No matter what social media you use, think about what you are posting and any possible damage that could result from your posts.

Remember that social media accounts of lawyer firms and lawyers have been compromised by criminals, so that they can see all your connections and even impersonate you to send phishing messages trying to trick the clients into clicking on a link or attachment. Commonly, if they have an email address, they will send your client a bill.

If they get useful information, they may sell it to other cybercriminals on the dark web.

Final words

Law firms exist in a dangerous world – they are a one-stop shop. Successful attackers will reap the data of many clients in addition to that of the law firm. So what are you to do?

- Establish and enforce a social media usage policy
- Train your employees, especially marketing employees, on cybersecurity, especially phishing and wire fraud
- Monitor the security of your email and your network
- Have a security assessment (at a minimum) at least once a year
- Stay up to date on cybersecurity – threats and defenses against them change with unnerving speed!

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* snelson@senseient.com

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* jsimek@senseient.com

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* mmaschke@senseient.com