SAFEGUARDING YOUR EMAIL ADDRESS

Back in the early days of the internet (circa 1981), AOL and other services like it (Yahoo, Excite, Hotmail, etc.) were the trailblazers for combining internet access with email. It was a revolutionary way in which to communicate with others and literally started the evolution of email as we know it today. People were able to send messages and receive responses immediately, which almost replaced the facsimile machine entirely. Attaching documents to emails facilitated an exchange of information that had never before been possible.

However, as with all new forms of technology, it had it drawbacks and "bugs" to work out. The free email providers offered this service with very little security protections. In addition, when you used these free email accounts, the only way you could access them was to use your internet browser. People were drawn to these accounts for their convenience and ability to access them from anywhere in the world. Unfortunately, they brought along their own form of security issues; namely, hackers decoding your password and gaining access to your address book. Because the free email accounts were "internet-based," anyone surfing the web could easily locate your email address and hack it. Thus, at any point in time, your free email account could be hijacked and spammed within a couple hours.

Using free email accounts in a law practice is a very dangerous decision. For the reasons mentioned herein, your email is extremely vulnerable to hacking attacks, causing your sensitive contact information (clients, opposing counsel, third-parties, etc.) to be exposed to the internet universe. Recently, there has been a new wave of spam emails in which someone spoofs (when the header information of an email is altered to make the message appear to come from a known or trusted source) an email address and then sends a bogus email to the person's entire address book claiming that they are stranded in London with no money. For those of you who are relatively savvy, you will immediately notice in the "to" box that it is sent to "undisclosed recipients." This is a dead giveaway that the email address has been hacked. Unfortunately, for those who are not quite so savvy, they may actually take this email seriously and fall prey to the scammer, believing that they are in fact responding to their attorney.

In addition to the address book issue, you also have the risk of your attorney-client privileged emails, as well as all email communications saved within your email account, being exploited by the hacker. Once again, because your free email account is internet-based, the hacker has the ability to hack into your email account thereby exposing all of your email communications, privileged or otherwise, to a nefarious third-party. Would you want the entire Solo/Small Firm listserv to know that you planned to subpoena a party in a case? I doubt it but that information could very easily be shared on the listserv if it fell into the hands of a hacker.

Many solo and small firm practitioners are so overwhelmed with starting their law practice and acquiring all of the nuts and bolts that they do not give a lot of thought to websites and email protections. It is understandable that this would be low on your priority list when deciding whether to take on more cases or develop a website. However, the decision does not need to be that time consuming nor that difficult.

The secret to obtaining a secure email address is as simple as choosing a domain name and reserving that name with a web host company. The difference between an "internet-based" free email account and a "web hosting" email account is very simple: the web hosting company does not store your email information on the internet. Web hosting companies store your files on their password-protected, local servers from which your email program downloads your emails. Many web hosting companies will provide you with a browser-based program that will allow you to check your email from anywhere in the world. However, you are still logging into the local server – not openly using the internet like the free email account services.

Securing a domain name with a web hosting company will not break your bank. Go Daddy offers very basic, easy domain registration for as little as $4.95/month (long-term commitment required). Others services which do not require long-term commitments and are as inexpensive are very easy to find. Your best resource, however, is to ask the members of your MSBA section via the listserves to see who everyone else uses as their web hosting company. You are guaranteed to get a lot of referrals and ideas for securing your domain.

In addition to the security a domain-based email account provides, there is one more important feature that I must point out: it looks professional. This email address shows that you are a professional: john.smith@jsmithlaw.com. This one does not: johnsmith327@aol.com. As the old addage goes, you do not get a second chance to make a first impression. If you want to project a polished, professional image to the outside world, make the minimal investment of securing a domain name and then set up your secure, domain-based email address. Your clients will appreciate your effort!