TopLawyerCoach.com
"UNWAVERING FOCUS ON RESULTS"

Email Loopholes Spell Danger!

Posted by Coach • January 22, 2010 • Printer-friendly

12 Ways to Avoid Costly Email Mistakes - and a Future Malpractice Suit

It seems all of us have some sort of love-hate relationship with our email inboxes.

We hate the time management issues associated with **email overwhelm**, yet we can't *bare* to live without our accounts.

We love email simply because it's the easiest and fastest way to communicate with clients and colleagues.

Unfortunately, though, it can also be **DANGEROUS**.

There are **email security loopholes** that may very well put you and your firm in ethical hot water.

Before you hit Send - here are 12 ways you can guard against costly email security dangers.

Top Lawyer Coach, LLC
601 Penn Street
Fort Worth, TX 76102

817/992-6711
newman@toplawyercoach.com

1. Be aware of metadata.

When you create or edit just about any document on your computer (like Microsoft Word, MS Excel or Corel WordPerfect files), hidden information about you and the edits you make is automatically created within the document file. This information is called metadata—which can be simply described as **"data about data."** It is dangerous because it can include past edits, deleted text or tracked changes, and information about others who work on the document—the kinds of things you likely don't want the client or opposing counsel to see. Thus, if you are emailing documents in native format to others, you may be unwittingly sending confidential information to them.

2. Know how to remove metadata from documents.

Converting files to PDF with Adobe Acrobat or other PDF creators will usually strip out most metadata. For this reason, many firms have adopted a practice of **sending only locked PDF documents** to clients or opposing counsel, especially if the recipient doesn't need to edit the document. Also, newer versions of Microsoft Office include features that can identify and strip metadata from documents created in Office applications.

3. Don't share or compromise passwords.

You wouldn't give your house key to a complete stranger, so don't do the same with your passwords!

4. Beware of email address Auto-Complete.

Having your email software automatically fill in recipients' addresses is certainly helpful when it comes to saving a few keystrokes or having to remember an e-mail address. But it is also a recipe for disaster.

Too often we are hurried and do not confirm an address that the software has filled in before hitting Send. Just about everyone who has used the Auto-Complete function will tell you they've accidentally sent an email to the wrong person. Save yourself the potential exposure to a confidentiality breach by turning Auto-Complete off.

5. Who is james007@aol.com?

When adding email addresses to your contacts list, you want to enter full names so it is obvious who a message is going to, since the contact's full name will then appear in your "To" line.

Top Lawyer Coach, LLC
601 Penn Street
Fort Worth, TX 76102

817/992-6711
newman@toplawyercoach.com

6. Double-check before you hit Send.

Before you touch that Send button, you should make it a practice of always checking and verifying that the email addresses in the "To" field.

7. Check your spam box daily.

Spam filters are essential for keeping junk mail out of your inbox. But they can be dangerous, too, because they can erroneously catch a message from your client, opposing counsel, the court or the like. This is called a **"FALSE POSITIVE."** So if you don't check your spam box daily, you could miss an important message.

Most spam filters let you create a **"WHITE LIST"** of parties you know and trust so messages from them will never be stopped.

8. Don't assume that an email was delivered.

In addition to spam, there are a number of reasons why your email may not be delivered - email server problems, a wrong email address, or the message went through but the person didn't open it, just to name a few.

You should always follow up on important messages that you send, and you should always reply to important messages sent to you (even if it is just an initial acknowledgment of receipt). This way everyone involved knows that critical emails have been safely received.

9. Don't use the "Remember Me" feature.

It is so tempting to let Windows and other computer applications remember **YOUR LOGIN NAMES AND PASSWORDS**. However, while it may make sense for your **Twitter** access, you should never have Windows or other programs remember your password for access to any program or system that has sensitive or confidential information in it (as in your computer login, accounting systems, bank accounts, practice management software access and so on).

In the law firm context, this is especially **critical for those who use the family computer at home.** Letting Windows remember a username and password gives anyone sitting at that computer full access to the program and all the data in it.

10. Never use a public computer to log on to your firm's network.

Public computers (like those in libraries and hotel business centers) often have **SPYWARE** on them that surreptitiously captures login names, passwords and other data typed in by people

using them. That information can be used to compromise the integrity of your network and leave you open to breaches of attorney- client confidentiality. **For this reason, typing user names, passwords or other confidential information on a public computer is an absolute do-not-do.**

11. Screen remote users.

A compromised computer that has remote access credentials can bypass firm security and let bad guys or malware get on to your firm network. Require all remote users to have the same level of Internet security on their computers as the law firm has on itscomputers. Any computer seeking to access your network must use firewalls, anti-virus software, anti-spyware protections and the like.

12. Enforce and update your technology use policy.

Every law office should have an up-to-date and enforced technology use policy. The policy should clearly state what people can and can't do when using office computers and when working on client matters on computers outside the firm's walls.

Remember, technology can be our best friend or our worst enemy.

Don't let yourself, your data, or your firm fall victim to a costly email mistake!

These simple steps are your best protection against future malpractice headaches.

Adapted from: Costly Technology Gotchas - A Dozen Tips for Email Security and More, Law Practice Magazine (March 2009), Dan Pinnington & Reid Trautz

Top Lawyer Coach, LLC
601 Penn Street
Fort Worth, TX 76102

817/992-6711
newman@toplawyercoach.com