

I'VE BEEN INFECTED!

Ellen Freedman, CLM
© 2016 Freedman Consulting, Inc.

Two recent articles in ABA Journal entitled "Lawyer resigns himself to paying ransom for release of computer files" and "'Ransomware' software attacks stymie law firms" made their way to the Solo & Small Firm Section listserv. As you might imagine, they created quite a stir. Several members contacted me off-list to make sure their safeguards were adequate. One member asked me whether PBA might be of any help.

These threats originate mostly outside the U.S. They are well-designed (e.g. socially engineered), in order to get past modestly cautious computer users. Aside from the practical information I can depart, the truth is that the PBA is powerless to assist you. In fact, the ABA can't help. The FBI can't help. Even the governments of the countries in which some of the threats originate are powerless to help. For every criminal who is caught, two arise like a Hydra with the head cut off.

Ultimately, your best defense is a combination of software and educated precautions. It's a dangerous computing world and we have to be vigilant all the time. This article includes some of the suggestions from the ABA articles, plus those I have learned the hard way from the breaches I have experienced.

I know, you're thinking that I teach and write about this stuff. How could I possibly get infected? Read on. Two were preventable. One was not. All were learning experiences.

Let's start with security measures. Some of these are basic. You may need an IT person to help on others:

1. Use quality anti-virus and anti-spyware software, and have it update not less than once a day. Once an hour is preferable.

2. Block executable files (like .exe) and compressed files (like .zip) from reaching a user's inbox.

3. Keep your operating system, browser and plug-ins, and application software fully updated.

4. Program hard drives on the computer network to prevent any unidentified or unauthorized user from modifying files. If you have only one computer, create a separate user logon for day-to-day work. Only log on as administrator when changes to the system need to be made.

5. Utilize two methods of automatic daily backup. For example, external hard drive and cloud-based. Keep multiple generations of backups. Ideally, do an extra full back-up once a week to a separate external hard drive which is NOT connected to the internet, and isn't overwritten. This will ensure you always have a pre-infection clean back-up.

6. Use strong passwords everywhere. A strong password includes upper and lower case letters, numbers and at least one special character. Don't use the same password in multiple places. Don't use names of children, pets, or part of your address or phone number.

   If you're like me and can't remember what you had for lunch, use a password vault that holds all your secure passwords, and synchronizes automatically to laptops and other mobile devices. I have been using LastPass for years with great results. PC Magazine reviews the top options for 2015, which you can find easily with Google.

My first infection came from someone I connected to on LinkedIn long ago. I knew the person. I got a private message a day later from my new connection which read "Ellen, look at what this person posted about you" followed by a link. Since I knew the person before we ever got connected, and they referenced the link, I clicked without hesitation. It took me to a web page which didn't reference me at all. But there was nothing apparently sinister about it. I closed it, fully intending to reply to the sender to find out if the link was bad.

The next morning, I opened my inbox to discover about a dozen messages from business contacts telling me "You've been infected! There are spam messages from you all over the place." Sure enough, it looked like I was sending out spam through my various social media accounts on diet aids, and many more

embarrassing products. Because I used the same password (albeit a decent one) for all my social media and many other accounts, most had been hacked.

Recovery from this first hacking wasn't too difficult, and actual damage was really just the embarrassment and time spent changing all the passwords and apologizing to people. It could have been a lot worse.

The second infection was more difficult. Again, an email from someone I knew and with whom I regularly exchanged documents. I got an email that said "Please look this over for me." And there was a PDF attachment. I opened it, and it was just a picture. This time I picked up the phone. "Oh, I'm so sorry," she said, "I've been infected. I didn't send that. Don't open it!" Too late. I shuddered. What was going to happen now?

At first nothing happened. A few days later there was a glitch in one of my programs, and it wouldn't open. Then another, and another. Slowly, one software application at a time, my workhorse computer became lamer and lamer, until it wouldn't fire up. Of course, the technician was onsite by that time; it took only 48 hours to total meltdown once the problems started.

The infection was so bad the technician had to take my computer into the shop to clean it, and reinstall several software programs. That didn't work. He had to completely wipe the hard drive, reinstall the operating system, reinstall all the applications, and move my data back. That worked. But I was without a computer for 3 days.

From that point on I added this additional security measure: any email which arrives which has a link or attachment, even from someone I "know," gets verified before I open attachments or click on links.

If I'm in an active work phase with someone and expecting the link or attachment, I don't verify. If the email totally explains what the link or attachment is and why it's sent, I don't verify. That leaves a whole lot of emails that wait 24 hours for my verification email to receive a response. Oh, and let me add that I don't "reply to sender" for the verification. I use "forward" and get their email address from my address book, just in case they've been spoofed.

This has turned out to be the best strategy. Probably 90% of the time the response is "Don't open it . . .it's not really from me!"

The last time I was infected was a doozey. I had been using the free version of Malwarebytes for years with no problem. All of a sudden it would not update. I thought at first this was caused by a glitch in a software update, so I waited for the next update to fix the problem. It didn't. That's when I found out that the problem with "free" software is that you don't get the support available to those who use paid versions.

I went to the Malwarebytes web site. I searched high and low for a way to get directly in touch with support, but that was only for those with the paid version. My only option was to send an email. I did. Within 2 hours the phone rang. The person on the other end had a heavy accent. He stated that his company, Repair Street, handled all the support calls for the free version of Malwarebytes. He initiated a remote connection to my computer so he could "fix me right up."

Shortly after he took control of my computer, I became alarmed. He was moving quickly from one screen to the next, making changes everywhere he touched. I tried to get him to slow down and explain, but he only worked faster, and explained less. About 30 minutes into the call I insisted that the connection be severed, and disconnected on my end. He called back over and over trying to convince me to re-establish the connection. He stated he found all sorts of security issues which probably happened while Malwarebytes was not functioning, and had to complete the repairs. I wanted none of it.

I searched the internet frantically for a way to get in touch with Malwarebytes. I found their twitter feed, and sent a post asking whether the company which contacted me was really their designated support company. They were not. When I read the response my heart sank. I was the victim of an inside job. My email had been intercepted and routed to the "bad guys" by someone at Malwarebytes.

My computer was thoroughly destroyed. It had to be trashed and replaced. Worse, it had corrupted my backups, rendering them useless.

Now I have an independent 3rd backup which is not overwritten or vulnerable to the internet. I use paid versions of most software so I can get to real support. And I always ask alleged repair technicians to provide verification when they call.

It's a dangerous world out there. Learn from my mistakes, and the mistakes of others. Be hyper-vigilant. Stay informed on the new threats that keep cropping up. Keep reminding all your staff as well. Don't think it can't happen to you.

© 2016 Freedman Consulting, Inc. The contents of this article are protected by U.S. copyright.. Visitors may print and download one copy of this article solely for personal and noncommercial use, provided that all hard copies contain all copyright and other applicable notices contained in the article. You may not modify, distribute, copy, broadcast, transmit, publish, transfer or otherwise use any article or material obtained from this site in any other manner except with written permission of the author. The article is for informational use only, and does not constitute legal advice or endorsement of any particular product or vendor.

Freedman Consulting, Inc.
(215) 628-9422