



ALPS

Practice Management Pointers

A Password Conundrum

Mark Bassingthwaighte, Esq.

mbass@alpsnet.com

At times, I feel that passwords are to the average computer user what bad tasting medicine is to a sick child. If only we didn't have to take it! Most of us, however, have come to recognize the importance of having a strong password policy (e.g. use of alphanumeric passwords that are a minimum of 14 characters if possible) in the workplace setting. After all, how many times have we all been told, "Never write your passwords on a sticky note and tape it to your monitor?" Unfortunately, holding one's nose to get the medicine down, if you will, can lead to an unexpected problem when it comes to trying to follow through with strong password policies.

Suppose that I comply with my law firm's password policy and have strong passwords in use for various needs. For example, I actually must enter two different passwords on my work laptop, one to enable the boot process and one to initialize the operating system. I do this as one way to further secure the contents of my laptop in the event of a theft. I also have different passwords for my Windows phone, jump drives, network login, online bank accounts, personal email accounts (which I do use for work), and trust me quite a bit more. In fact, I take the security issue so seriously that I regularly change my passwords to key systems or accounts. This is all well and good until the unexpected happens. Returning to the example of my being employed at a law firm, perhaps I pass away or I am an employee who must be fired for some misdeed.

Here's the rub. In many firms, no one would know what my passwords are so getting into the various systems may prove to be a costly venture in both time and money. Key client information stored on my laptop will not be readily accessible because no one will be able to get past the first password. Let's make this even worse. I am the employee who must be fired, my position is network administrator and I have sole and exclusive knowledge of key network passwords. This is potentially a very serious problem because I may simply lock the network down remotely and the firm will be dead in the water.

Now that I have your attention, what is the solution? At its most basic level, anyone's passwords should be available to someone else at the firm in the event of an emergency of some sort. While there is no one right solution, here are a few ideas. Create an Excel spreadsheet of all user passwords and limit access rights to this file to select administrative staff only and make sure that this file remains encrypted at all times. Write down all network administrative passwords and place the resulting document in a sealed envelope. Keep this envelope in a safety deposit box or safe. For the solo attorney, include passwords in the letter of instructions that are to be given to the executor of your estate and/or the

attorney who has been named to administer the winding up of your practice. Update these lists and documents as necessary.

This list of ideas is simply a starting place and not intended to be the best solution for your practice or firm. I am simply trying to raise awareness of the concern. Personally, I use two encrypted password safes for a number of reasons; however, my wife knows how to access the information stored there should I unexpectedly pass away. After all, for all that she has to put up with as my wife, it's the least that I could do. Now, what can you do for your clients and partners?



Risk Management Questions?

Mark Bassingthwaighte, Esq. is the Risk Manager for ALPS Property & Casualty Insurance Company. He is available to answer risk management questions and can be reached at 1-800-367-2577 or mbass@alpsnet.com.

Disclaimer:

ALPS presents this publication or document as general information only. While ALPS strives to provide accurate information, ALPS expressly disclaims any guarantee or assurance that this publication or document is complete or accurate. Therefore, in providing this publication or document, ALPS expressly disclaims any warranty of any kind, whether express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

Further, by making this publication or document available, ALPS is not rendering legal or other professional advice or services and this publication or document should not be relied upon as a substitute for such legal or other professional advice or services. ALPS warns that this publication or document should not be used or relied upon as a basis for any decision or action that may affect your professional practice, business or personal affairs. Instead, ALPS highly recommend that you consult an attorney or other professional before making any decisions regarding the subject matter of this publication or document. ALPS Corporation, as well as any of its subsidiaries, affiliates and related entities shall not be responsible for any loss or damage sustained by any person who uses or relies upon the publication or document presented herein.