TECHNOLOGY UPDATE

# Good Passwords—The Solution or Bane of Existence for Digital Assets

*By Joseph G. Hodges, Jr., Esq.*

The past two years have seen a significant increase in the interest of our clients in using and maintaining good but easy to remember user IDs and passwords for all of their digital assets, not just e-mail or commercial accounts. We are sometimes surprised at the breadth and scope of what are considered password protected digital assets these days. Here, from one of law Professor Gerry Beyer's (Texas Tech Univ. School of Law) sample estate planning digital asset inventory matrix charts, are just a sampling of the diverse categories of digital assets that have to be considered: electronic devices (such as PCs and voice mail), e-mail accounts, domain names, online storage (*e.g.*, Dropbox and Google Drive), financial and tax software, banking, brokerage, income taxes, retirement assets, insurance (health, life and property), credit cards, debts (mortgages, cars, loans), utilities, commercial businesses, social networks, digital media accounts (*e.g.*, Netflix, iTunes, YouTube, Kindle), loyalty programs (*e.g.*, airlines, Target, Amazon, Best Buy), and other miscellaneous accounts (such as Skype, Flickr, and on line medical records). See Beyer, "Estate Planning in the Digital Age" (2013), http://ssrn.com/abstract+2255623. A similar matrix has been developed by attorney James D. Lamm as part of his work on a Uniform Digital Assets Act and can be found in his Blog at www.digitalpassing.com called "My Digital Audit: Passwords, Online Accounts & Digital Property" (2013).

*...according to data developed by security-focused developer SplashData, up until 2013 the word "password" was the most commonly used and worst password.*

Given the depth and breadth of these potential digital assets, it is no wonder that the passwords that protect access to them have become so important. Given that importance, let's now take a look at what are considered to be some of the worst and best passwords. Not surprisingly, since having a great variety of different easy to remember passwords is so difficult to remember and maintain, recent studies have shown that users tend to use more secure passwords for digital assets that really matter, such as for computers and other electronic devices or online banking or brokerage or commercial transactions, and a variety of simpler "throw-away" passwords for sites that do not retain any of the user's sensitive or credit card information, such as a Facebook or Linkedin accounts or ones that require you to have one just for return access or tech support. Within those broad parameters the selection of good passwords is all over the place.

**Mr. Hodges** is an attorney in Denver, Colorado, and formerly served as Co-Chair of the American Bar Association's Real Property, Probate and Trust Law Section Technology Committee. He currently serves as a member of that Section's Communications Committee and the Technology in the Practice Committee of The American College of Trust and Estate Counsel.

Believe it or not, according to data developed by security-focused developer SplashData, up until 2013 the word "password" was the most commonly used and worst password. In 2013 the equally bad password "123456" took over first place. Another one in the top 25 was "adobe123." Still another was "photoshop." Some additional bad ones were (and I am not making these up): 12345678, abc123, letmein, 111111, iloveyou, trustno1, 123123, welcome, ninja, 000000, shadow, sunshine, password1, and qwerty. Moreover, while somewhat novel, passwords such as "letmein" and "trustno1" are hardly unique or novel, let alone all that difficult for a hacker to crack.

To better protect a client's digital assets without also having to memorize myriad strings of nonsense numbers, letters and symbols, SplashData recommends passwords that contain random words separated by spaces or characters such as trolls_need_jobs. Personally I do not think this goes far enough and would recommend that your clients also add at least one more word for good length and add somewhere in the sequence of those words a mix of numbers and symbols that is unique to all of their accounts, plus at least one or two capital letters either in the words themselves or as a preface or suffix that is indicative of the name of the site such as "MS" for Microsoft. An approach such as this is essentially one of balancing the benefits with the dangers and finding a happy medium that works for your clients that they can live with. Whatever you do, don't let your clients use such things as birth dates or social security numbers, or easily recognized family names, or words commonly found in dictionaries. In fact, here is an excellent place where misspelled words you can remember as such can often come in handy.

If you still have doubts about how easy it is to have your user IDs and passwords hacked, just consider the recent hack job that hit Target Corp after the holidays, when the information of as many as 110 million customers who shopped there during the holiday season had their private data compromised. This incident was followed by similar breaches of the computer systems of other well known retailers. In fact, Hold Security, a research and online security firm reported in Yahoo finance on 2/26/14 in an article entitled "*360 Million User Names and Passwords*" that the sheer amount of data about people's private online information that was available for sale by criminals had reached a staggering 360 million credentials by early 2014. In October of 2013 a cyberattack was launched against Adobe that exposed the Adobe customer IDs and encrypted passwords and credit card information for some 38 million active accounts. What is really sad about this particular incident is that, while many customers said the password they used on the Adobe site was not important to them, nearly 2 million of those customers were using the exact same password, the same being 123456. Sound familiar?

Another step-up option to consider for generating good and safe passwords is to use a site like http://passwordgenerator.net. iPassword Generator is a free, lightweight and portable Windows application that is designed to create a strong and unique password for each of your applications or online accounts from the keyfile you selected using a technology called Tabula recta. In addition, you are allowed to encrypt and hide your keyfile inside any other file with the AES-256 (Advanced Encryption Standard) algorithm. The main difference between iPassword Generator and other password creators is that the passwords created by it look like random strings, but they are not. The passwords can only be recreated if you selected the correct keyfile and entered the correct password if it is encrypted, but if you lost the keyfile, no one can retrieve the passwords back.

Alternatively, Norton has had an Internet Security tool for years that now contains an Identity safe tool that keeps personal data and sign ons in a secure vault on your PC. Gmail also has a password storage tool under the Tools/Options/Security tab. Just click on "Saved Passwords" but make sure you use a Master Password to access it.

Once your client has developed a list of passwords, the next question is where is the best place to store them for safety and convenient recall. Generally keeping them on a PC, hopefully with some sort of encryption device, is not recommended due to the dangers of someone gaining access to that list or your having a system crash. Another option is to write them down or record them, hopefully in an easily updateable spreadsheet format, and then keep that list as a file that you store in a safe place. Still another option is to download that spreadsheet file to a

UBS drive that you can carry around with you separate from your PC and access remotely as and when needed. Probably the best option is to invest in one of the many available password manager software programs or cloud services. While many of us have a favorite password manager we use, it is not the purpose of this column to promote any one password manager in particular, as studies have shown that the use of any of them will likely elevate the level of password security above what it presently is. However, in the interests of trying to pass along some suggestions for password manager programs to consider, below is a listing of several of these that I gleaned primarily from reading user comments in various articles I read while preparing this column. See also "*Why You Should Use a Password Manager and How to Get Started*" at http://www.howtogeek.com/14150/.

*InformationWeek* (www.informationweek.com) published a list of the top 10 password managers on 4/30/13. The ones on that list are:

- LastPass (www.lastpast.com);
- Password Genie (www.securitycoverage.com);
- SplashID Safe (http://splashid.com);
- RoboForm and RoboForm Everywhere (www.roboform.com);
- Dashlane (www.dashlane.com);
- mSecure (www.msevensoftware.com);
- KeePass (http://keepass.info);
- DirectPass (www.trendmicro.com);
- Norton's Identity Safe (https://identitysafe.norton.com); and
- MyLOK Personal (www.mylok.com or www.hsn.com ).

Not to be outdone, *PC Magazine* published a list of what they considered to be the six great password managers on March 11, 2011, listing:

- Kaspersky Password Manager (www.kaspersky.com);
- LastPass and LastPass Premium;
- IronKey Personal (www.ironkey.com); and
- RoboForm Desktop and Everywhere (www. www. roboform.com).

That list was expanded in a January 28, 2014 article by *PC Magazine* entitled "*The Best Password Managers*" that lists LastPass and LastPass Premium, Dashlane, RoboForm Everywhere and Desktop, Keeper, MyLOK Personal, Norton Identity Safe, plus the following:

- PasswordBox (www.passwordbox.com);
- 1Password for Windows (www.http://agilebits.com);
- Password Genie (www. securitycoverage.com);
- F-Secure Key (www.f-secure.com); and
- my1login (www.my1login.com).

For what it is worth, out of this group, the PC Magazine Editors selected as their Editors' Choice for 2014 LastPass, as being more powerful and flexible than almost all of its competition, LastPass Premium, because it adds mobile support, and Dashlane, because it is also feature packed, plus they felt it has an attractive and user-friendly interface. *One additional program* that was mentioned a lot was Password Depot (www.password-depot.com) as it was rated 5-star by CNET in 2009, although some users found it to be too cumbersome and complex to use effectively.

While the above is a daunting list of choices, many good ones are provided for your further exploration and testing so you can increase the security of your client's user IDs and passwords and thereby help them give lasting value to their digital assets.