RIA WorkSpace

Creating Hacker-Proof Passwords

How many passwords do you have? If you're like most people, you probably have more than 10 and possible closer to 20. How many different systems do you have to log into just to get your day up and running at your RIA firm? It's hard to remember them all and as a result people tend to use passwords that are easier to remember and therefore - easier to hack.

Your passwords are like the keys to your life. They control access to your banking information, your email, the network in your office, your social network, online purchasing sites etc. None of this should be taken lightly. An effective password policy for you personally and for your RIA firm is important and here are a few recommendations to help you along that path.

Creating Passwords

Complex

A password should be a minimum of 5-8 characters and should contain a combination of upper and lower case letters, numbers and special characters. Some people use phrases as passwords which can also work as long as they are not common phrases from a movie or song that might be easily guessed.

Unique

If a password you're using is on the list of SplashData's Worst Passwords you need to change it. You want passwords that are not easy to guess by hackers so shy away from the most common passwords. And if hackers can gain insight into who you are, the use of personal information like your spouse or child's name or the numerical sequences of your birthday are bad moves as well.

Confidential

Your colleagues, friends, children or spouse do not need to know your passwords. This is especially important inside the RIA firm where employees should be reminded that they are responsible for all access – authorized or not – that is done using their password.

Exclusive

Do not use the same password for multiple websites or applications. Recycling passwords makes it easier for hackers to gain wider access to your life and network.

Changing

Your RIA firm should adopt practices that require frequent changes to passwords. Setting expiration date of 45-90 days means that if hackers have figured out a password, they won't be able to use it once it's expired. Users should be required to make significant changes to passwords not just a change to one character which can be easily guessed by hackers.

Some Helpful Tools for Your RIA Firm

Storing Passwords

To help you keep track of your passwords, and to get rid of the page of scribbled passwords sitting next to your computer, you can consider a few options. A simple solution is having users create an encrypted file that contains their passwords and is saved in a secure location. Password managers are also available and offer many different features. They can automatically capture your password, fill in web forms and many offer two-factor authentication. PC Mag did a side-by-side comparison of paid password managers and free password managers that can help if you're trying to decide what to adopt at your RIA firm.

Two-Factor Authentication (2FA)

Logging into a system with a username and password is single-factor authentication. Two-factor authentication (2FA) includes a second step and while it might require slightly more effort by the user, it can improve security. 2FA is not new. You use it when you go to the bank machine to take out money. The bank card you use is one form of authentication, and your PIN code is the second. To help with password logins, the second authentication can come via a phone app, a one-time-password (OTP) token of FOB which can provide a unique pin code that changes continually and has a limited use-ability time.

Single Sign-On (SSO)

Single Sign-On (SSO) is becoming common place for RIA firms, especially for those who have moved to the cloud. SSO allows a user to use a single username and password to access multiple systems and applications on the network. Your SSO will review an employee's credentials when they log in and verify what they can and cannot access. You may choose to require additional login credentials for access to some of the more sensitive areas of your network where security is paramount.

SplashData's 2014 Worst Password List

Rank	Password	Change from 2013
1	123456	*No Change*
2	password	*No Change*
3	12345	*Up 17*
4	12345678	*Down 1*
5	qwerty	*Down 1*
6	123456789	*No Change*
7	1234	*Up 9*
8	baseball	*New*
9	dragon	*New*
10	football	*New*
11	1234567	*Down 4*
12	monkey	*Up 5*
13	letmein	*Up 1*
14	abc123	*Down 9*
15	111111	*Down 8*
16	mustang	*New*
17	access	*New*
18	shadow	*Unchanged*
19	master	*New*
20	michael	*New*
21	superman	*New*
22	696969	*New*
23	123123	*Down 12*
24	batman	*New*
25	trustno1	*Down 1*