SCHULTZ COLLINS
INVESTMENT COUNSEL

Online Security

(December 4, 2019)

As we head into the holiday season, we remind you that this time of year, more than ever, it is important to be diligent about securing your identity in your interactions with financial institutions. Taking a few simple precautions can make a huge difference. A word, then, about some of the more important measures you can take to protect yourself.

Secure Your Password(s)

For all financial web sites (investments, banking, insurance, etc.) it is recommended to use very secure passwords: a minimum of 10 characters long, with upper case and lower case letters, numbers, and special characters. While this may seem complicated, it's quite simple to do. For example, take a favorite phrase and change a character or two from letters to symbols or numbers. For example, if your phrase is blueboat, change it to Blu3b0aT5%. The position of the keys on a keyboard makes it easy to substitute the numbers on the keys just above certain letters and then add a special character by hitting shift for a second strike of a number key. It speeds the typing and makes remembering the password easier.

Other general guidelines for passwords: never use the same password across sites, and change your password every six months (ninety days is even better). Many institutions are already mandating changes to passwords after set time periods.

One way to help keep passwords secure and organized is to use a password tool (RoboForm and Lastpass are just a couple of examples). These tools will help you keep your passwords organized, and can help generate secure passwords. Many such tools also analyze your current passwords and tell you how secure they are.

It's also a good idea to take advantage of Two-Factor Authentication whenever you can. The two factors in question are first your regular log in credentials – user name and password – and second a unique key code for each new log in. Such key codes can be generated in several ways. In one, the website sends the key code to the email address or cell number of record once the first authentication test – the correct log in credentials – has been passed. Alternatively, a site can work with an Authenticator App (several are available for most smart phones) to request that it generate a code. Both of these methods add an extra layer of security.

Two-Factor Authentication is becoming the de facto standard for most financial institutions, so even if your current vendor doesn't use it today, they probably will very soon.

SCHULTZ COLLINS
INVESTMENT COUNSEL

Be Careful Where & When You Click

As a general rule, don't click on links in emails from financial institutions. It's much safer to go directly to the institution's own website, and log in there to see if the message of the email is legitimate. Many phishing emails these days are well crafted and appear quite genuine. But when you really look at the links they contain, you can see that that pleasant looking enquiry from your bank is in fact a nefarious attempt to steal your information.

When using search engines, visually inspect the links before clicking on them to see if they appear valid. If a link is to www.microsoft.com.xyx instead of www.microsoft.com, it's a pretty safe bet that it's going to send you to a bogus site.

Inspecting links can be done in email messages, too. Just hover your mouse pointer over a particular link without clicking on it and at the bottom of the window, or in a small pop-up, the underlying link will be displayed. If it doesn't match what you're expecting then the link is probably not good.

Keep Your Computer Safe and Secure

You should always run Anti-Virus software on your computers or devices used to access financial platforms. If you don't already have some sort of security program installed, make sure you get one. There are paid and free versions. The free versions are often almost as good as those that charge a subscription fee. The primary difference between many paid and free versions are that the paid versions will automate many scan and check routines

You should also make sure that all security patches are up to date on your devices. Many of the exploits that hackers use can be prevented with the latest security patches.

How Does Schultz Collins Protect Our Clients?

For SCI clients, we have recently implemented two programs: Trusted Contact and Secret Word.

The Trusted Contact Rule directs brokerage firms to obtain the name and contact information for a "trusted contact" for all accounts that are newly opened or updated. The Rule, as espoused by FINRA, enables a firm to communicate with the designated trusted contact whenever there are concerns about a client's financial management decisions. Such communications will not violate investor privacy or account confidentiality restrictions. Under current standards, the trusted contact does not have any management authority over client assets – unless he is also appointed attorney in fact.

While not yet a widespread practice in the financial industry, the Secret Word will probably become the norm within a few years. The Secret Word comes in handy when someone calls an advisor representing that he is a client, but no one present in the office is familiar with the client's voice. If the caller can provide the Secret Word, even a new employee who has never met him can feel confident that the caller is indeed the client.

It has been a longstanding SCI policy to call to confirm all requests regarding financial transactions with our clients directly. So, if we see an email stating “Hi there, I need $50,000 ASAP,” we’re going to call to confirm that this is in fact a legitimate request. The Secret Word is the way we shall do so henceforth.

Conclusion

These are just a few ways that you can protect yourself, not just during the upcoming holiday season, but all year round. Some of them may sound a bit laborious (securing passwords), but once you get into the practice, you’ll find that you’ll feel more secure in your interactions with all your financial institutions. However laborious these steps may be, a stitch in time saves nine. We urge you not to neglect them.

Very truly yours,

Kenneth S. McMurray
SCI Information Technologist

Post Script

A few weeks ago we published a lengthy article on Financial Exploitation that discussed a few of these same topics in more detail, as well as highlighting other recent regulations and practice changes. We encourage you to visit our site and read the article if you haven’t already done so.