It's Time to Change Your Password

DAVID B. LOEPER, CIMA
CHAIRMAN/CEO

It is time to change your password...

The confidentiality of an investors' personal financial information is of paramount importance. Investors need to have confidence that their personal information is secure. The media have been covering this topic for some time, and publicity about malicious hackers breaking into everything from confidential military systems to databases of credit cards have made headline news.

The Internet has created a lot of confusion and anxiety about security. The Internet is a virtual "world" and many people, having lived in a physical world for so long, have a very difficult time conceptualizing the level of security in this new virtual world. There seems to be an assumption that if the data is on the Internet it is somehow less secure than in our more traditional physical world where we can "see" our security.

We would like to help investors and advisors understand the similarities between the virtual world and physical world and also recognize some of the differences.

First, a general rule of thumb about security...any information is only as secure as its weakest link. The biggest holes in security come from information access points that have no real barriers to access. In the physical world there are many difficulties in securing information. Something as simple as your brokerage statement that you receive in the mail each month is extremely insecure, yet contains extremely sensitive information.

To design highly secure data systems, security specialists walk through all movements of data, inputs, retrieving or viewing of information and physical access to systems to identify "holes" and then design a means of blocking access by people that should not have the information. Let's look at the path your brokerage statement takes....

A few days after the end of each month, giant printers at the brokerage firm start printing reams of paper statements that are automatically sorted, folded and stuffed into envelopes. We will assume the people in the brokerage firm that are running these large print jobs have appropriate security clearance and that the brokerage firm delivers these statements to the postal service in armored trucks with armed guards. How secure is the information once it reaches the postal service? Could any one of the dozens of postal workers that will be handling your statement use that information maliciously? Let's say that keeping their jobs is enough of a deterrent. Are postal workers armed? How many times have you seen the door open on a mail truck? How is your information protected when the mail truck door is open and the postal worker is fifty feet away delivering or picking up a package?

The statement makes it to your mailbox. There it sits with no barrier to access other than respect for the law. Maybe you are out of town and Susie, your neighbor's teenager, is feeding your fish and bringing in the mail. Do you trust Susie (pierced nose and all) with your confidential information? Once the mail makes it from your mailbox into your home, do you keep it secure? We will assume that you have an alarm system for your home. Does your mail ever sit in a pile "to be opened" in your kitchen or home office? Who has physical access to your home? Your teenager's responsible friends...the cable repairman...the exterminator...housekeeper...your spouse's bridge club? Unless you immediately put the statement under lock and key as soon as it enters your home there are several "holes" in your security.

What do you do with statements after you are done reading them? Do you file them in a locked file cabinet? Toss them in the trash? Run them through a shredder and then toss them in the trash? Put them in your recycling bin after they are a couple of years old? Think about all the potential unrestricted access points to your confidential information.

If you don't think any of these risks are serious or ever happen you would never be employed as a "security specialist." Have you heard about the credit card offers that are stolen from mailboxes or trash? These are real security breaches that happen every day. They don't make the headlines simply because they only affect one person at a time.

Let's move to the security of your information stored on "local" PCs or file servers. This still isn't a virtual world because you know that the information is physically stored either right there on your PC or on a file server down the hall in your office. This "feels" nice and safe just like knowing that your paper statement is in the locked file cabinet. Do you have DSL or a cable modem? Do you have a firewall or proxy server to protect your information? It is unbelievable the number of people who have their computers online 24/7 that have their whole file system totally open to the public, should someone want to look there.

Is your PC screen saver password protected? If so, how many minutes does it take for the screen saver to be activated? What about physical access to the equipment? Is the file server in a locked room? Who has keys to the file server closet? Do cleaning personnel have physical access to your PC or File server? What precautions are in place to prevent the physical removal of the equipment with all of this personal information?

If you have a laptop with confidential information on it you may feel safe, just like carrying around paper statements. Do you have any idea how many laptops are stolen each year from airports, hotels and offices? There is another security risk.

What software tools and systems do you use? If you use Microsoft Excel, do you password protect the worksheets? Is the data encrypted in other applications? If the application is password protected that doesn't necessarily mean that the data the application uses is encrypted.

Then there is email. The primary rule here is to send nothing confidential via email because it isn't secure. If you are sending file attachments via email this is the electronic equivalent of posting the information on the Internet with no password protection for everyone to peruse. Delivery of user names and password via email is a great convenience, especially if you forget your username or password, but do you change your password on the system once you receive it in the email?

The thing that security professionals focus on is plugging all the access points using reasonable security measures. There is no way to guarantee a creative, malicious criminal won't get to your confidential information. Anyone that tells you otherwise is lying to you.

Security is a matter of using more than reasonable precautions to protect information. Things like shredding statements before sending to the trash or recycling is just a reasonable precaution. Encrypting data is a reasonable precaution. Using firewalls or a proxy server is a reasonable precaution. Password protecting is a reasonable precaution. Securing physical access is a reasonable precaution. Having armed guards and barbed wire fences around facilities that house a computer is a reasonable precaution (when there are large amounts of data to be protected, it is practical too, as is often the case in an Internet hosting facility).

Here is where the concern over Internet security has been ignored. Although safe deposit boxes require two keys to open and they are in a safe, there have still been bank robberies where safe deposit boxes have been looted or destroyed by fire. (Yes, security means protecting against the loss of data too. How often do you make backups? Are the backups protected under lock and key in a separate building?)

While everyone is very concerned about security, the fact of the matter is most people do a very inadequate job of protecting their confidential information. Imagine if you could password protect that brokerage statement that sits in open mail trucks, in your mailbox, on your desk or in the trash. That would be far better security, would it not?

So, while we are all concerned about security, the fact of the matter is in all likelihood, data stored on financeware.com is safer than you would ever protect the data yourself. You don't need to worry about your screen saver password because we automatically log you off if you go too long on our system without activity. The data is physically stored on servers (not unlike the one in your office) that are in a facility that has 24x7 security guards, biometric scanners and/or electronic key access, motion detectors and continuous video surveillance both inside and outside the facility. Documents stored in finance file manager are encrypted as they are passed to and from our servers. We use 128 bit SSL for the passing of information to your screen. We have firewalls to protect access to our computers. Backups are run nightly and tapes are stored in separate facilities under lock and key. You can change your password at any time, and through this communication, we are encouraging you to do it regularly. Our servers never sit in hotel rooms or airports. We run background checks on new employees for both criminal and credit histories.

So, while the physical world may feel safe and it is nice to know that your data is right there with you that doesn't necessarily mean that it is safe. How safe is your data? Are YOU using all the precautions we are with your computers that have confidential information? Are these precautions applied to both the access to and prevention of loss as we do? How much time, effort and inconvenience does it take for you to provide this security? Wouldn't it feel better to know that all these precautions are taken every day and that all you have to do to deliver this level of security is change your password once a month.