



## Security 101

We recently placed our home on the market. In doing so I had to have an additional key duplicated for the Realtor's lock box. While getting this key duplicated, it struck me how similar the basic security devices for my house are to those of a network environment.

In a house, to gain entrance you need a key. To gain entrance to a network, you need a password. With this concept in mind, I consulted with one of my Internet gurus, Jeeves, and found the average lock has 5 tumblers and each tumbler can have 8 positions (or depths of cut on the blank). This gives a possibility of 32,768 variations for a key. Do you realize that most password controls I have reviewed mandate a minimum of 4 characters? Given this and knowing that a number of people will use their PIN (all numeric) with a variation in numeric order gives me 10,000 possibilities. At this point my house is 3 times more secure than my network; just imagine having to carry 32 thousand keys. The 7 in my pocket are bad enough. Just how long will it take a computer hacker to try all 10,000 possibilities? Not too long.

What if we add letters into the mix? Now my 4 character password is up to over 1.5 million choices. But still, a number that large can be hacked by brute force relatively quickly. I normally recommend a 6 to 8 alphanumeric password. Let's look at 7 to make it simple. If I use an alphanumeric password and mix upper and lower case letters, I have a password that is unique out of 3,521,614,606,208 possibilities. That's going to take a little longer to hack. But how do I remember 7 characters? One trick is to use a pass-phrase, something you can remember, like Nap2Day. I'm sure many of you have seen various prestige license plates that meet the requirements of a strong password. Nap2Day meets the length of 7 characters, utilizes both alpha and numeric characters, as well as a mix of upper and lower case letters, plus, it is something that I would like to do. But is this really secure? In addition to brute force attempts, many of the password cracking utilities rely on huge dictionaries to speed up the cracking process. Human nature is to use

something familiar, something that would be found in a dictionary. Based on that theory, the pass phrase Nap2Day can be broken into three pieces, Nap, 2, and Day, possibly easier to crack than others. So how can I make a pass-phrase strong? Let's take another example, Hello2U. This uses both upper and lower case letters while incorporating numeric characters; however, Hello is still vulnerable to a dictionary attack, so let's scramble it some more. Since my weakest point is Hello, let's replace the letter l with a symbol !(exclamation point). Let's also replace the letter o with the number 0 (zero). Now my password reads He!!02U; UPPERCASE lowercase symbol symbol numeric numeric UPPERCASE. This is a strong mix but still relatively easy to remember.

**“In a password utopia, all passwords are extremely strong and are never written down.”**

First and foremost a password policy should be established and communicated to the staff. In password utopia, all passwords are extremely strong and are never written down. Let me caution you here, as computer users we have passwords for everything and many with different rules. If you “lock-down” the system so tight and enforce strong passwords to the nth degree, your users will write them down. I have found numerous passwords on sticky notes under keyboards, under mouse pads, and in various spots on the desk. If users aren't trained to develop a password or pass-phrase that is easy to remember, it will get written down and possibly compromised. Be tough, but assist your users.

As I was filling out the realtor paperwork I had to note that there is an alarm system in the house. Our A/C repairman can attest to the fact the Sheriff's department responds quickly to a triggered alarm. How many networks are monitored this well? In my neighborhood if 100 people stopped

by a nd knocked on my door in one day someone would notice. Do you know if 100 people on the Internet have “knocked” on your door, or more, many more? As credit unions you are responsible for the assets of thousands of members. Shouldn't you at least go to the same lengths to protect their assets as you do at your own home? An Intrusion Detection System (IDS) either monitored by a third party or monitored by your staff provides you with this level of protection. Not only can an IDS alert you to those unwelcome guests that are knocking at your door but many times can ignore them so they go away and possibly let you know where they are coming from. In these days we must take whatever precautions necessary to ensure the security of the assets that we have been entrusted with. Just so you don't get the wrong idea about the neighborhood in which I live, one of the primary uses of our alarm system is to let me know when one of the children has left the house. An IDS can be configured in a similar fashion, not only to monitor external attacks on the network but internal as well. While we may not want to admit it, internal fraud or theft is a severe problem and the one from which we are most at risk. An IDS can monitor areas of the network that have been designated as sensitive and can alert the appropriate individuals when someone has entered this area.

This is a good place to discuss access rights or levels. There is information on the network that should not be available to everyone. You control the availability to this information through some sort of access level for each staff person. Each function in the credit union should be identified along with the areas that require access. This can be folders on a network drive or it can be functions within the core system. These access levels should be reviewed periodically to ensure they are appropriate and necessary for each staff person's job duties and responsibilities. When staff are promoted, access levels may need changing.

*Continued on page 2*

A staff person might be given additional access to cover for someone else temporarily. The only way to ensure access levels are assigned appropriately is to have a guide in place that outlines the functions, their access rights, and a periodic review. This review should be done by someone that is not involved in the day to day assigning of rights, to maintain independence, and to just simply have a fresh set of eyes looking at them. For an IDS to work there must be a set of rules defining who can go where and do what. Without pre-determining or classifying the data, there would be no set of rules for the IDS to enforce. Without a set of rules to enforce, there can be no exceptions. Nobody is doing or seeing anything wrong because no one has determined what is right or wrong.

With just the three steps above great strides can be made in securing your network. Passwords have been made stronger, monitoring for both internal and external attacks has been implemented, and we know who is supposed to have what access. Sleeping tonight will be easier. Of course, these are just a few of the things that need to

be done to secure your network and the valuable data it holds. The NCUA has a whole section and Appendix that addresses information security and the required security program. How does your credit union's security program compare? Has it been updated to reflect the changes in technology and the required technology aspects?

In a nutshell, the requirements of NCUA Regulation 12 CFR Part 748 are that the security program must:

- ▶ Apply to both physical and electronic (or logical) environments,
- ▶ Be written and include administrative, technical, and physical safeguards appropriate for the size and complexity of the institution, and
- ▶ Be certified in compliance annually.

The objectives of the security program are very basic. The security program is designed to:

- ▶ Ensure confidentiality of information
- ▶ Protect against threats to the integrity of information
- ▶ Protect against unauthorized access

- ▶ Assist in identifying who commits these acts
- ▶ Prevent destruction of vital records

While this can be achieved through various means, the presence of the following elements provide a strong foundation for your security program:

- ▶ Involvement of Board of Directors
- ▶ Identify and Assess Risk
- ▶ Management of Risk
- ▶ Service Provider Oversight
- ▶ Security Program Adjustment
- ▶ Board Reporting

There is a lot to cover and depending on your staff this could feel intimidating. If you have any questions as to your Credit Union's Security Program's compliance call us. We can work with you in determining compliance and can make any recommendations necessary.

In the next newsletter find out why my children think I have a pet hippopotamus at the office. ♦

*Jay Simonton, CISM, CNE, CNA  
Information Technology Manager*