

Information Security - More Important Now Than Ever



By Barry Kouns, Vice President of Information Security Risk Assessment

As attention shifts to the ever increasing challenges around us the bad guys are turning their attention to how to take full advantage of any situation.

The number of organizations reporting data breaches has increased dramatically. The average cost per compromised record is now \$243 for first time offenders and the total cost averages \$6.6 million per breach. The financial industry accounts for half of the total number of exposed records each year and there are no signs that things will be getting better soon.

So how do we respond to the increased threat to the security of our information assets with fewer resources and a reduced budget from last year? In a phrase, “We need more deputies.” Credit unions must ensure that every employee knows how and is doing the following on a regular basis - especially those employees with computers that access, store or transmit nonpublic personally identifiable information.

1. **Set strong passwords/pass-phrases** – Weak passwords are one of the most common flaws in computer security. Make sure you use a minimum of eight characters combining letters, numbers and symbols. Consider using a pass-phrase to create a strong password. Create a phrase that is easy for you to remember, but no one else would attribute to you. For example; ‘Today was too cold and snowy for skating!’ could be used to remember the following password; ‘2Dw2cas4s!’

2. **Protect confidential information from unauthorized access at all times** - Do not share your user-ids and passwords or other forms of electronic authentication. Do not use your personal credentials to provide other people with access to any information system. Enable screen savers with locking passwords for all computer systems. Position monitors and printers so that confidential information is not on display to be seen by the general public.

3. **Only transmit confidential information via secure channels** - Confidential information should not be sent over the Internet or via e-mail unless encrypted or otherwise secured. Talk to your security professional or call Southeast Corporate if you have questions about the security of your communication channels.

4. **Remove all unnecessary files that contain confidential information** - First identify the data you have stored on your computer. Confidential information should not be stored on your computer unless it is absolutely necessary and in that case it should be encrypted. Identify any confidential data you no longer need and then follow your security professional’s guidelines for securely deleting these files.

5. **Delete without opening, all executable or unfamiliar email attachments** - Use caution when accessing e-mail and do not trust any unexpected e-mails. Never open an unexpected e-mail attachment without first verifying its type and checking it with an antivirus program. If in doubt, delete it, and/or verify with the sender before opening it.

6. **Avoid downloading files from the Internet** - Only download files from Web sites that you trust. Be cautious, certain file types are less safe because they are known for carrying viruses. Some file types to avoid include program files with extensions such as .exe, .scr, .bat, .com, or .pif. Be careful, often a dangerous file can be disguised because it has two file name extensions such as, filename.txt.exe.

7. **Report all suspected security incidents** – Always be alert to security vulnerabilities, threats and potential breaches to information or information systems. If you observe or suspect information security has been breached, stop work, isolate the system as best you can and do not transfer any files to other computers. Do not attempt to test or prove a suspected weakness. Immediately report any observed or suspected incidents to your supervisor.

8. **Maintain computers per company policy** – Employees are granted access to information and information systems in order to perform their job responsibilities. You must understand, agree and comply with all acceptable use policies pertaining to the use, maintenance and protection of information systems including user responsibilities in support of anti-virus, firewall, spyware and set automatic updates to install the latest antivirus signatures and security patches.

9. **Be security wise** – Year after year security surveys report that computer users are the weakest link in information security. Users represent the largest threat because the bad guys know how to take full advantage of our human nature, bad habits, inherent trust, and willingness to help when asked under most situations. Be a student of security. Make yourself wise to the latest vulnerabilities and always be on the lookout for attempts to gain unauthorized access to confidential data. Don’t be so trusting when it comes to computer security.

10. **Limit computer access** – Unauthorized access to your files, Internet sessions and applications can be greatly reduced if you log out, shut down, or lock the system when leaving your computer unattended. Do not leave laptops, PDAs or portable storage devices unattended at any time.

The current economic climate is causing many to question the safety and soundness of our financial system. Let’s do our part in building member confidence in our dedication and ability to protect the privacy of their personal information.

As always - Remember, Think Security – Act Smart.

