Securing your Password

Today, a business person or resident hears of databases containing private information being stolen from universities, companies and individuals. Sometimes your username and password to access data files is taken by programs called "Spyware", code that can copy the exact keys being pressed on your computer keyboard, saved in a file and then sent to the perpetrator of this crime via the Internet. Another technique that I have found which is easier to penetrate a user's account is to locate the area where the employee has written down their password. While inspecting organizations over the years, we are discovering passwords written on paper and placed under keyboards, desk drawers, and on calendars. These smart passwords are easy to identify since the collection of characters contains letters, numbers and special characters, and they do not conform to any other format of messages we can expect to see in a work cubicle. Once we log onto the individual's computer using the provided entry key, we have access to many of the company's files and can carry them away with a small Flash drive. So using passwords that are difficult to remember to control the right of entry to a server defeats the purpose when the user has to write their code down to remember them.

The most successful method of picking a password is to extract the characters from a phrase that is easy to keep in mind, since a short string of words are easy to remember. A password based on a passphrase can be formed in a variety of ways. One of the most common ways is by taking a memorable saying or line from a song and uses the first two letters of each word replacing the vowels with numbers or special characters. For example:

Get At Me = Ge@m3

Notice that the passphrase does not have a phone number or birth date that can easily be traced to the user. Also this combination can not be found in a dictionary, which if was present allows the code to be broken by a criminal in hours using a dictionary attack. Whatever method the associate chooses, remember the password should be hard to guess, but easy for the user to remember.

Many companies set up their servers and can set the password length to be at least eight characters long, and then they check the password complexity requirement and the user's entry code now needs to be a smart by incorporating three of the four elements.

- Password should have one or more uppercase letters
- Password should have one or more lowercase letters
- Password should have one or more numerals
- Password should have one or more special characters

We do not want to see passwords like the following:

287Parma or **Francis1986**

Since they can be the street address of the employee or the name of the birth year of a child. Passphrases should be smart, built from your favorite saying or line from a much loved song. When built, they are easy to memorize and they are not found written in a work space.

Melissa Price, Gahanna, Ohio