

A Good Password Is Hard to Find

Accessing and managing confidential electronic data is paramount in our ability to serve our customers and perform our daily operations. Yet consider what's guarding unauthorized access to this information – YOUR USER-ID AND PASSWORD.

Simple passwords can be cracked with a little time and a computer able to make repeated guesses. Your aim is to create and use a password that takes so long to crack the attacker becomes frustrated and moves on. Avoid using passwords that are easy to guess. These include:

- Words, names or numbers that have some reference to you and can be discovered. For example: Your birth date, pet's names, children's names and birthdays, anniversaries, your agent number or district code.
- A word/phrase that a "shoulder surfer" - someone looking over your shoulder watching you type the password - could easily repeat.
- Words or names that a computer program could match by trying obvious searches, such as:
 - Any word in a standard dictionary
 - Company or organization names (especially Farmers)
 - Famous names
 - Proper names
 - Any of the above written backward
 - Any of the above with a number or single character inserted at the end or beginning
 - Any of the above in a foreign language
- Short passwords, since this lessens the number of tries needed to decipher the word.
- Passwords used as examples in documentation about passwords.
- Passwords that obviously refer to what they are used for, such as "password".
- Simple passwords (such as "farmers1" or "abc123")

Other tips for password management

Even if you've devised a strong password, these common mistakes can still make an attacker's job easy:

- **Writing a password down.** Two-thirds of all computer security breaches are carried out internally so never assume it's safe to leave a note listing passwords on your computer, at your desk, or in a drawer. If you must write something down to help you remember, disguise it by changing the words around in some way. This keeps the password obscure. Never store your user name or other required login information on the same piece of paper or file as the password itself. (If you must write your password, guard it like you would guard your bank card's PIN number)
- **Sending a password where it can be read.** A password sent in an e-mail that is not encrypted can be intercepted and read by an unauthorized person. Store only encrypted passwords on the computer.
- **Change your password on a monthly basis.** Spend 10-15 minutes on the first day of every month changing your password on all of your systems and applications – including the Agency Dashboard and your e-Mail account – instructions for changing these passwords are located on the Agency Dashboard; contact your Personal Lines Growth Coordinator or the Help Desk for more information.
- **Never divulge your password to anyone!** Your password serves as the lock and key to your systems and applications. Divulging your password to someone else is like sharing your identity.

What makes a good password?

People choose and use poor passwords because they're easy to remember. In order to be useful, a good password should be obscure to all but the owner of the account. The best password has these characteristics:

- It can be remembered
- It can be typed easily and quickly
- It won't easily be spotted by a shoulder surfer
- It is long enough to be secure – recommend at least 8 characters
- It is complex enough to withstand multiple guessing attempts
- It has upper and lowercase letters
- It has numerals and/or other non-letter characters

How can you create a password that is obscure to others, yet memorable to you?

A password is only secure while it remains unknown to others. A secure password ensures would-be attackers will find it more appealing to pick on somebody else.

If you're not using a good password you may be putting your agency, customers, employees and Farmers at risk. You could also be putting yourself at risk, as an easily identified password could enable someone to assume your electronic identity.

To test the strength of your password, go here: <http://www.microsoft.com/protect/yourself/password/checker.msp>

An example of a strong password, which is easy to remember, but hard to guess is to:

- Use two words that don't usually go together – such as “yellow” & “frog”, “rose” & “green”, “quiet” & “noise”, or even “blue” and “monkey”.
- Intermix upper/lowercase letters (“BluE”)
- Use a number – such as “16”
- Use special characters – such as the pound symbol (“#”) and/or the at symbol (“@”)

By using these guidelines, you would be able to have the following password “**BluE#16@MonkeY**” – a very strong password (“BEST”), which is not only easy to remember, but also difficult to guess.