

SECURITY - *Now ...more than ever!*

Cyber Security - Disaster Recovery - Continuity of Government



DTI eSecurity News - You wouldn't share your toothbrush...don't share your Password

Why do I need a "strong" password?

Passwords are used for a wide variety of applications, to provide a means of authentication. E-mail, ATM machines, your voicemail, and online bank accounts all require a password in order to verify your identity before providing access to their resources. The resources are locked until you provide the correct password which unlocks them for use.

If a password is easy to guess, too short, or too simplistic, malicious users can easily gain access to all of the important information it protects, including financial information. With password-cracking tools easily available on the Internet today, weak passwords can be cracked in seconds, while stronger passwords can take much longer.

Remember that your password is your personal key to your workstation, network, and data. Strong passwords make it harder for attackers to gain access.



How do I choose a password that is strong *and* easy to remember?



Many people choose passwords that are based on personal information because it makes them easy to remember. The problem is that these passwords are easy to crack by guessing. Hackers also "brute force attack" your password by using software that repeatedly attempts to guess the password, using a dictionary of common words and numbers, until it finds the right one.

The best passwords are at least eight characters long and contain a combination of both upper and lower case letters, numbers, and special characters such as !, #, \$, @, etc. Alternating numbers, letters, and special characters to form your password makes it difficult for hackers to crack your password. But these passwords are difficult to remember!

Don't defeat the purpose of a strong password by writing it on your desk or taping it to your computer. A better method is to use a mnemonic or passphrase to assist your memory. An example of a strong password is 'l8&8@MDs'. In this case, the mnemonic is the phrase 'I ate and ate at McDonald's'. Another example is 'SBchampNYG08', a passphrase for 'Super Bowl Champions New York Giants 2008'. These techniques make the password strong, and easier to remember.

Tips for keeping your password secure

- Don't base passwords on personal information.
- Use different passwords on different systems.
- Don't use dictionary words.
- Longer passwords are more secure.
- Passwords should not be a user ID in any form.
- Avoid password saving utilities.

Questions or comments?

E-mail us at

eSecurity@state.de.us