



DTI eSecurity News - What if the grooves on your keys were easy to reproduce?

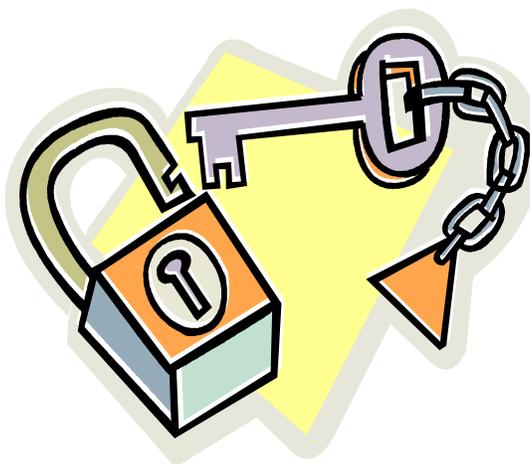
Why do I need a “strong” password?

Passwords are used for a wide variety of applications to provide a means of authentication. E-mail, ATM machines, your computer, your voicemail, and online bank account management systems all require a password in order to verify identities and provide access to their resources. The resources are locked until you provide the password to unlock them for use.

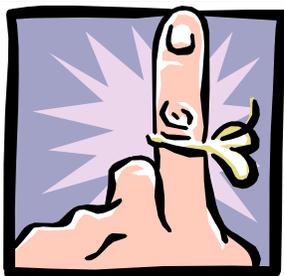
People are the weakest link concerning passwords. If a password is easy to guess or too simplistic, malicious users can easily gain access to all of the important information it protects, including financial information.

It may seem that access to your personal e-mail or voicemail is no more than an inconvenience and breach of privacy, but it could be much more dangerous. Attackers could use the information they find in e-mails and voicemails to steal additional information or launch additional attacks.

Strong passwords make it harder for attackers to gain access to sensitive information.



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



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

The strongest passwords contain a combination of both an upper and lower case letter, numbers, and special characters such as !, #, \$, @, etc. Alternating numbers, letters, and special characters to form your password make it exceedingly difficult for hackers to crack your password. The passwords should also be at least eight characters long.

The problem is choosing strong passwords that are easy to remember. Many people defeat the purpose of their strong password by writing it on their desk or taping it to their computer. Anyone that has physical access to the computer then has full access right in front of them.

A method is described below that is both easy to remember and secure. An example of a strong password is: 2JazE-4u. The password was formed by using a mnemonic, which is something that is intended to assist the memory. In this case, the mnemonic is the phrase “too jazzy for you”. The strong password (‘2JazE-4u’) was created from that phrase utilizing 1) phonics 2) lower and uppercase letters 3) a special character and 4) replacing the words ‘too’ and ‘for’ with the digits ‘2’ and ‘4’. This combination makes the password strong yet easy to remember.

Tips for keeping your password secure

- Don’t base them on personal information.
- Don’t use dictionary words.
- Use different passwords on different systems.
- Avoid password “saving” utilities which may be insecure or hacked leaving your password vulnerable.

Questions or comments?
 E-mail us at
eSecurity@state.de.us