

Stump Online Password Hacking Programs with Three Little Words

Security companies and IT people constantly tell us we should use complex and difficult passwords. However, some research has shown that simple passwords can be used more effectively. If the password is something easy to remember but multiple words, it can be more successful.



The work involved in hacking passwords is pretty simple. There are five typical ways used.

1. Asking: Amazingly the most common way to gain access to someone's password is to simply ask for it, usually in connection with something else.
2. Guessing: Most people choose a password that is easy to remember and typically relates to them as a person. Passwords like last name, spouse and children's names and dates of birth, which are easily developed, are common mistakes.
3. Brute-Force Attack: A hacker simply attempts to sign in using different passwords. He will use a program that runs a series of letters until the system eventually breaks your password.
4. Common-Word Attack: This is a simple form of brute-force attack. The hacker will attempt to sign in using a list of common words.
5. Dictionary Attack: This is the same concept as the common word attack using a full dictionary program of nearly 500,000 words.

Automated programs can handle around 100 sign-in requests per second. This means a simple word like sun could be hacked using the brute-force or common-word attack in less than three minutes. However, if your password includes two common words, hacking time increases to two months. Add a third word and the time increases exponentially to more than 2,000 years.

Some web sites require a combination of upper and lower case letters, while others want you to also add a number. These are effective, but sometimes difficult to remember, and experts don't advise that you allow your browser to always remember your passwords.

[- International Risk Management Institute, Inc.](#), October 2010