



Rev A

May 8, 2001

Guidelines for Secure Password Selection

© Jamcracker, Inc., 2001 - Proprietary and Confidential

Status: Final

Page 1 of 4

The information contained herein is the property of Jamcracker, Inc. The possessor agrees to maintain this document in confidence, not to reproduce, copy, reveal or publish it in whole or in part.

Context

It is extremely important that users change the passwords associated with their computer accounts frequently, and that they change them to something that cannot be guessed by someone else. This is because the password is the way the computer verifies that someone logging in with your account number (also known as your login or user ID) is really you. If someone else obtains your password, they can use your account to peruse your private data, including electronic mail; alter or destroy your files; and perform illegal activities in your name. And, in such cases, it is difficult to find out who the culprit is. In a digital world, the password is often the first line of defense that protects the person's integrity. It must be kept secret at all times, much like a PIN for the ATM, and there is absolutely no good reason to share it with anyone such as a colleague, a system administrator, even your boss. **EVERY ACCOUNT IS IMPORTANT, including yours!**

Guidelines

The following guidelines will guard against someone finding out your password and using your account illegally:

- **Make your password as long as possible.** The longer it is, the more difficult it will be to attack the password with a brute-force search. Always use a minimum of 7 characters in your password (most Microsoft Windows systems at Jamcracker allow up to 14 characters and some applications, such as PGP, allow more).
- **Use as many different characters as possible when forming your password.** Use numbers, punctuation characters and, when possible, mixed upper and lower-case letters. Choosing characters from the largest possible alphabet will make your password more secure.
- **Do not use personal information in your password that someone else is likely to be able to figure out.** Obviously, things like your name, phone number, and address are to be avoided. Even names of acquaintances and the like should not be used.
- **Do not use words, geographical names, or biographical names that are listed in standard dictionaries.**
- **Never use a password that is the same as your user name.**
- **Do not use passwords that are easy to spot while you're typing them in.** Passwords like *12345*, *qwerty* (i.e., all keys right next to each other), or *nnnnnn* should be avoided.
- **Change your password on a regular basis.** Changing your password every 30 days is a good rule-of-thumb, and you should never go longer than 90 days before picking a new password. Do not reuse any previous password you have used. You must change any password given to you (sometime known as default password) as



Rev A

May 8, 2001

Guidelines for Secure Password Selection

© Jamcracker, Inc., 2001 - Proprietary and Confidential

Status: Final

Page 2 of 4

The information contained herein is the property of Jamcracker, Inc. The possessor agrees to maintain this document in confidence, not to reproduce, copy, reveal or publish it in whole or in part.

soon as you logon to the system for the first time. If a system you are using does not allow for a password change, either voluntary or induced by the system, you must notify the system administrator of this problem so that corrective actions may be put in place.

- **If you are having difficulty picking a good password, one good method is to use the first letter of each word in a phrase you can easily remember.** For example, "McDonald's is your kind of place" would be *miykop* (this is known as a passphrase). Another method is to intentionally use misspelled words, or words with a number or punctuation mark suffixed. Examples include: *braekfast*, *kite276*, and *weather.* (the period at the end is part of the password).

Good passwords:

- Have both upper and lower case letters, digits and/or punctuation.
- Are easy to remember, so they do not have to be written down
- Are at least seven or eight characters long
- Are even longer and are actually passphrases, a whole sentence which is NOT a common citation.

Here are some guidelines about what secure passwords should NOT include:

- Your name
- Your spouse's name
- Your parent's name
- Your pet's name
- Your child's name
- Names of close friends or coworkers
- Names of your favorite fantasy characters
- Your boss's name
- Anybody's name
- The name of the operating system you're using
- The hostname of your computer
- Your phone number
- Your license plate number
- Any part of your social security number
- Anybody's birth date
- Other information that is easily obtained about you
- Words such as *wizard*, *guru*, *gandalf*, and so on.
- Any username on the computer in any form (as is, capitalized, etc.)
- A word in the English dictionary
- A word in a foreign dictionary



Rev A

May 8, 2001

Guidelines for Secure Password Selection

© Jamcracker, Inc., 2001 - Proprietary and Confidential

Status: Final

Page 3 of 4

The information contained herein is the property of Jamcracker, Inc. The possessor agrees to maintain this document in confidence, not to reproduce, copy, reveal or publish it in whole or in part.

- A place
- A proper noun
- Passwords of all the same letter
- Simple patterns on the keyboard, like *qwerty*
- Any of the above spelled backwards
- Any of the above followed or prepended by a single digit

What is a passphrase?

Most people are familiar with restricting access to computer systems via a password, which is a unique string of characters that a user types in as an identification code. A passphrase is a longer version of a password, and in theory, a more secure one. Typically composed of multiple words, a passphrase is more secure against standard dictionary attacks, wherein the attacker tries all the words in the dictionary in an attempt to determine your password (there are a lot of computer programs that do just that and dictionaries covering almost every language and specialty!). The best passphrases are relatively long and complex and abide by the same standards as passwords (contain a combination of upper and lowercase letters, numeric and punctuation characters, etc). They must NOT be chosen from the citations of famous characters (ex: “To be or not to be : that is the question” is a poor choice, whereas “T0 Bee or not 2 bE : that 1s the Qu3sti0n” – notice the use of numbers in place of letters or whole words – is a better choice, although it is harder to remember) or well-known sentences that are easy to guess from your work environment (a sentence on a poster, or your company slogan).

Although passphrases are harder to break than password one must keep in mind that most systems only allow for passwords that are shorter than 14 characters. Still, you may create a hard to guess password by using portions of a passphrase, by taking the first letters of your hard-to-guess passphrase and putting them together (see example in previous section).

Why all the fuss?

Although it is humanly impossible to attempt to break into a system by systematically trying all the combinations of, say, 14 characters (26 to the power of 14 combinations would require about 26,455,978,787,195 years!), many password crackers exist today to carry out this task. A password cracker is a special computer program that attempts to break into a computer system by trying every possible combination of characters or by trying a pre-defined list of words (a dictionary) to check if one would work. The latter, also called a dictionary attack, is remarkably fast since the computer doesn't waste time trying some “weird” words. It is also very efficient because it exploits a key vulnerability



Rev A

May 8, 2001

Guidelines for Secure Password Selection

© Jamcracker, Inc., 2001 - Proprietary and Confidential

Status: Final

Page 4 of 4

The information contained herein is the property of Jamcracker, Inc. The possessor agrees to maintain this document in confidence, not to reproduce, copy, reveal or publish it in whole or in part.

in the human being, our memory (we use “easy to remember” words to make sure we do not forget them). Still, a computer (or a human being, given enough time) will undoubtedly succeed with a brute-force attack: trying every possible combination of characters. Typically, a password cracker attempts around 1 million different possibilities by second (on a PC equipped with an Intel Pentium™ III running at 450 MHz) and it takes typically between 30 seconds and a few weeks to find every password on a computer using this technique!

As soon as a password is known, a computer system stands a very high probability to fall under the attacker’s control, no matter which individual (or role) the compromised password belongs to. EVERY PASSWORD IS IMPORTANT and every password compromise is a very serious security incident that needs to be reported.

