

Using secure passwords

Introduction

Many individuals look upon the requirement to use and change passwords regularly as an evil inflicted by the Information Technology (IT) industry. What users should be aware of is that a password is no different than the combination to a safe and should be protected in the same way. Although you may believe your company and personal data would be of little or no interest to hackers, this often has no bearing on which sites are targeted. A large percentage of hackers are opportunists out to create petty vandalism and cause damage. Other hackers may be more interested in using your site to relay emails (spam) or viruses to others, thereby protecting themselves and implicating you. These are good reasons for making passwords difficult to crack or guess. This will make your site much less interesting to casual hackers and much harder for targeted hackers to infiltrate and abuse your computer systems.

Best Practice

There are many ways to crack or break passwords. For this reason it is essential all passwords be chosen with care and changed regularly. There are a number of industry 'Best Practices' which can help ensure the safety of the organisations data.

- All passwords should be at least 6 characters
- All passwords should contain at least one number
- Passwords should be changed regularly (at least every three months).
- Passwords should not be in the dictionary, names, dates or phone numbers
- Each password change should introduce a new password, which should be substantially different from all previous passwords (e.g. the password should not remain the same and just have a new number tagged on the end)

If possible these rules should be enforced by software to ensure compliance and the security of the organisation.

Do

- Use a password with mixed-case characters (e.g. aLEx54)
- Use a password with non-alphabetic characters, e.g., digits or punctuation.
- Use a password that is easy to remember, so you don't have to write it down
- Use a password that you can type quickly, without having to look at the keyboard. This will make it a lot harder for someone to steal your password by watching over your shoulder

Don't

- Use your login name in any form
- Use your first or last name in any form
- Use your spouse's or child's name
- Use other information easily obtained about you. This includes license plate numbers, telephone numbers, the brand of your car, the name of the street you live on, etc.
- Use a password of all digits, or all the same letter. This significantly decreases the search time for an intruder
- Use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Use a password shorter than six characters

Some Selection Ideas

Often when people choose a random password it is then easily forgotten, although passwords can usually be easily reset, this can cause an overhead on the system administrator and waste valuable time. One popular way of choosing passwords that can be remembered is for the user to select a two syllable word, divide the word in half, reverse the order, and insert a number. For instance, the word

SUMMER and the number 2 become MER2SUM. This becomes an easily remembered password (all the user must remember is SUMMER 2 and the rule), while still being difficult to crack or guess.

Switching letters for numbers is also a good method. Start with a normal word, say 'computing' and replace the i's with 1's and the o's with zeros, so the password would become 'c0mput1ng'.

Use word abbreviations to create small simple phrases that are easy to remember. For example, "you too can be safe" would turn into "u2canbsafe".

Taking a short phrase and using the first letter of each word can also be a good method. For example, 'I like the beach in the summer' would become 'iltbits'.

Summary

The basic key with passwords is after avoiding all the common mistakes like using your name etc. It must be something you can remember. If you can't remember it then you will write it down which is a big no-no. Second to remembering it is: the password should be easy to type.

Marc George & Simon Griffiths

Document copyright © 2001
All Rights Reserved
Technology Solutions – www.techs.co.nz