MAG & MIS Alliance Password Guidelines & Protection Standards

Mastria Auto Group

Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of resources. All users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

All passwords (e.g., email, web, desktop computer, etc.) should be changed at least every 2 or 3 months.

All passwords should conform to the guidelines described below.

Guidelines

General Password Construction Guidelines

Strong passwords have the following characteristics:

- Lower case characters
- Upper case characters
- Numbers
- Punctuation
- “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)
- Contain at least 7 alphanumeric characters.

Weak passwords have the following characteristics:

- The password contains less than 7 characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "your", "sanjose", "sanfran" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or a phrase.

For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. (NOTE: Do not use either of these examples as passwords!)

Password Protection Standards

- Always use different passwords for your accounts from other non-business access (e.g., personal ISP account, option trading, benefits, etc.).
- Always use different passwords for various business access needs whenever possible. For example, select one password for systems that use directory services (i.e. LDAP, Active Directory, etc.) for authentication and another for locally authenticated access.
- Do not share your passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential business information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the Information Security Department.
- Always decline the use of the "Remember Password" feature of applications (e.g., Eudora,
- Outlook, Netscape Messenger).

Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain Access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOn128Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.