

Easy things you can do to improve the security of your password

- **Don't share passwords with others;**

Never give your password to anyone including co-workers and family, even by email or over the phone. Do not hint at the format of a password. Before entering your password, make sure no one is watching you.

- **Avoid the obvious;**

Never use your name, the names of family and friends or work-related words in your passwords.

Avoid using dictionary words (i.e. meaningful words including foreign words, slang, dialect, jargon, proper names, words spelled backwards, etc.) as much as possible.

Avoid using common misspellings and substitutions like replacing an "s" with a "5" or an "i" with a "1". Certain easily-guessed words are also commonly used as passwords such as "guest", "password", "secret", etc. and should never be used as passwords.

Include at least one character from each of the following character groups:

- Uppercase alphabetic characters (A through Z)
- Lowercase alphabetic characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (~`!@#\$%^&*()_+={ }[]|\:; "<>',,./)

- **Use more than an 8 character password;**

Using the maximum number of characters greatly increases the complexity of guessing or cracking passwords.

- **Change your password regularly;**

Every time you change your password, try to come up with a new topic and wording, by creating a password that is completely different from the previous ones.

- **Don't write passwords down;**

Don't store them anywhere in your office or computer system. Don't leave your password on a post-it or written down in any other places where someone could find it. Never send them in email, post them to news, leave them online in a file (even in a protected directory), embed them in a script, etc.

- **Use different passwords for different accounts, systems or applications;**

It is always recommended to use different passwords on different systems; if your password is compromised on one system, you can always prevent intruders from gaining access to other systems and data.