*KEVIN MITNICK'S

10 Rules for Passwords

1. Don't tell your passwords to anyone!
2. Avoid simple dictionary words, names, key dates, and personally identifiable information.
3. Use passwords at least 12 characters long
4. Use a passphrase: A string of unrelated words is more secure than a regular password.
5. Use a unique password or passphrase for every website.
6. Change your passwords for sensitive websites every 60-90 days, and remember, no easy to guess patterns!
7. Change your password immediately if you feel you have been informed of a breach.
8. Answers to security questions must be as hard to guess as your password.
9. Use MFA (multi-factor authentication) whenever possible!
10. Use password procedures that your organization requires you to use.

pcc corp
We make I.T. easy

***Kevin Mitnick** is a hacker turned good guy, computer security consultant. He is best known for his high-profile 1995 arrest and five years in prison for various computer and communications-related crimes.

CHOOSING AN EFFECTIVE PASSPHRASE

5 Easy Steps

Random passphrases provide the best combination of memorability and security.

1. **User 5 or more words you can easily remember, separated with a special symbols (spaces are symbols)**

2. **A good passphrase should be at least 25 characters long.** Ex) coffeewishesparakeetspeed

3. **Make sure that your passphrases are easy to remember but isn't a common quote, lyrics, or any group of words that can be easily guessed by someone that knows you.**

4. **Use a passphrase: A string of unrelated words is more secure than a regular password.**

5. **Ensure the complexity of your passphrase meets the necessary requirements.**

The passphrase '**logic finite eager ratio**' would take approximately 189,658,722 centuries to crack!

pc corp
We make I.T. easy