What's Your Pass Phrase?

Everyone needs a Strong Pass Phrase

The most basic level of good security is a good password. But the various hacking tools and robots make cracking basic passwords too easy. You should create **pass phrases** (more than one word) that are **strong**. A strong pass phrase contains at least three of the following:

- Uppercase letters (e.g., A, B, C)
- Lowercase letters (e.g., d, e, f)
- Numbers (e.g., 1, 2, 3)
- One or more spaces (that's what makes it a phrase)
- Special Characters, which can include:
  { } [ ] , . < > ; : ' " ? / | \ ` ~ ! @ # $ % ^ & * ( ) _ - + =

It's the space that makes remembering your strong pass phrase easier: It becomes a sentence or phrase that's meaningful to you. For example:

This is a Pass phrase?
L0ggin on now… (note that that's a zero in loggin)
Don't run with scissors 8<
Kick b*tt, take names!
Smiling 2004 ;-)

Your pass phrase should be at least **6 characters**. It should **not** contain any part of **your name**, your user-name, or your email address. It should change 8-12 times per year. And it must not be any single word that can be found in any dictionary (of any language). Hint: Misspelled words are good.

The first thing robots do to crack passwords is to run a dictionary against your username. If your pass phrase is a single word, you lose.

We can also help you with:

- Password Policies
- Privacy Policies
- Acceptable Use Policies
- And more

KPEnterprises Business Consulting, Inc.

Our job is to help manage your computer net-works so you can focus on **Your Business**.

Let us help you create the systems and policies that will make your company more successful.

KPEnterprises
Business Consulting, Inc.

916-928-0888
www.kpenterprises.com

Microsoft CERTIFIED Partner