Cracking Passwords

This is intended to be a short explanation of why good passwords are important (though the subject of password cracking can be very complex).

There are basically four ways of cracking a password (though techies would give you more):

1. **Guessing** - This is why you're always told not to use common words or numbers: someone who knows you could easily compile a list of words and numbers and try different combinations (Your address, city, pet's or son's names, city, year you were born, etc.). The possible combinations are not that many.
2. **Password Lists** - These are simply long lists of thousands of common passwords available from the Internet. They are generally compiled by major companies who continually see the same passwords. If you search the Internet about most common passwords, maybe you'll get a list of 10 or 25. But, as already said, the lists are in the thousands and are easily available. And with the right setup, a computer could zip through this list in seconds.
3. **Dictionary Attack** - This is just what it sounds like. A dictionary list of different word combinations. It takes longer to go through than a Password List as above, but it is still doable. "treesgrow" is not a good password.
4. **Brute Force** - This is the type of password cracking method that is necessary to crack good passwords. If you hear on the news that the government can crack passwords, they can. But so can you–if you've got hundreds or thousands of years to wait. A brute force crack is where the computer will take all characters from a keyboard, including upper and lower case letters, numbers, and special characters such as *%^$# and try every possible combination.

So what's a good password? It's a passPhrase with odd characters thrown in, such as: mY*8bEst*8fRiend*8iS*8rAlf.

That's not as weird as it looks. It's just:

- "my best friend is ralf"
- the second letter instead of the first being capitalized
- "*8" between all the words
- it's long
- it uses small and large letters
- numbers
- a special character
- and best of all, it's not that hard to remember.

But who's going to guess it?

At a half million guesses a second, this password would take millions of years to crack. More or less.

Too long? Try mY*8bEst*8fRiend. That will still take about 464 years to crack.

You might find this interesting:

number of characters	time to crack at 500,000 attempts a second
1	less than a minute
2	less than a minute
3	less than a minute
4	less than three minutes
5	less than five hours
6	less than 19 days
7	5 years
8	464 years
9	44,531 years
10	4,274,902 years

Of course faster computers will change this ...