What About Passwords?

Passwords are a computer version of a "key".
Would you set up all your locks on your house, office and cars to use the same key?
Would you make that key just a blank key? (like a blank password)
Would you make that key with just a single notch in the middle (like a very simple password "1234")?

Probably not, eh?

So the same principles apply to computer passwords.
You should likely use different ones for each access.
You should use passwords that are "complicated enough" to discourage hackers.

Here is a pretty good set of recommendations:
http://www.makeuseof.com/tag/create-strong-password-forget/

Go to this website: http://www.passwordmeter.com/
or: http://howsecureismypassword.net/
Both are helpful in their own ways. So I suggest you try them both.
Compare your old password with some new ones you like.

Please understand that entering passwords into computers is assumed to be automated. A computer does the entries as fast as possible. If the entries are by hand then it will take a lot longer. That doesn't mean you should assume that the only method possible is by hand - because it isn't.

Here is what I often do:
Come up with some phrase or phrases like: donaldson or inthecity
Then augment it with numbers like 21141: 21donaldson141
(You could use donaldson21141 but that may be a bit obvious).
Then maybe change the "o" to a zero "0": 21donalds0n141
Then make some of the letters upper case:
21d0NaLdS0n141 ... which simply alternates between lower and upper case ignoring the 0s.
And, to make it harder to crack and a bit harder to remember would be to break the sequence of alternation:
Instead of LULULULUL (lower-upper-lower……..)
you might use LULLULULUL (lower-upper-lower-lower-upper …..)

Here's the desired result:
The structure should be easy to remember.
You need to remember (in this case) that the letters start with lower case first.
You need to remember that the "o" is a "0"

Another trick that may work for you is to combine a standard part with a site-specific part to create different passwords:
donalds12hotmail
donalds12bankofthepacific
or
DoNaLdS12hOtMaIl
DoNaLdS12ThEbAnK
etc.
The notion in all cases is to not use things like birthdates nor obvious names.

Password math:

How many different passwords does a hacker have to try?

- Start with 3 or 4 lower case letters:
There are 26 lower case letters in the English alphabet.
So I have to try a-z for the first one.
For each of those I have to try a-z for the second one.
That's 26 times 26 to get the first two right or 676 possibilities.
If there are 3 letters then 26 times more for 17,576 possiblities.
If there are 4 letters then 26 times more for 456,976 possibilities.

That sounds like a lot doesn't it? Well not really because:
- on the average it will take half the tries to get the right combination.
- computers are *very* fast and might deal with millions of combinations each SECOND!
- hacking programs can use dictionary words first

But, what if we use both upper and lower case letters and add the numbers 0-9?
Now we have 62 characters instead of 26.
That's 62 times 62 to get the first two right or 3,844 possibilities.
If there are 3 letters then 26 times more for 238,328 possiblities.
If there are 4 letters then 26 times more for 14,776,336 possibilities.

This is why most reasonable password systems require 8 characters minimum, use of upper AND lower case AND numerals.
The result is 218,340,105,584,896 possibilities and would take 106 years for a desktop PC to crack according to http://howsecureismypassword.net.

Mitigating in your favor are a couple of things:

1) the hacker likely doesn't know the length of the password. So, the number of possibilities increases.
2) the hacker may have to wait a long time to see if a password works or may get shut out after some number of tries. This increases the time tremendously.