Computer Security Basics

Email is not a letter, it's a postcard.
Vulnerability: Email messages are passed from computer system to computer system on the internet until they reach their destination. At each hop on the journey, email is susceptible to easy, undetectable snooping, just like a postcard. The same thing applies to chat and instant messaging. This is a particular concern in countries with government surveillance of electronic communication.

Encryption is a method of securely encoding data so it can only be read by its intended recipients.

Countermeasure: Either encrypt sensitive information or just don't send it via email. Some office suites have built in support to encrypt documents; attach personal data to your email as an encrypted file. Alternately, use a program like PGP to encrypt your email directly. This is convenient if you frequently send sensitive info, but requires that your recipient has a similar program to decrypt. Don't send sensitive information over chat or IM.

Sensitive information is anything you wouldn't want to post on the wall at a coffee shop. Be particularly careful with anything you might use to verify your identity over the telephone, like SSNs or or maiden names.

You are never secure in an internet café.
Vulnerability: Public wifi hotspots are a leap of faith – you can't tell which one you're connected to or the motives of the person providing it. The internet café owner could monitor all your internet communication or substitute a duplicate of your bank's website to grab your password. If you are using a computer provided by the café, hidden software could record everything you type, make a copy of every file from your flash drive, or infect your flash drive with a virus.

Countermeasure: Just don't do it. At least, not banking or anything important. If you have no other option, weigh your risk of compromise against your need to communicate. Mitigate your risk with good security practices – always run up-to-date antivirus and anti-spyware software at home, take browser security warnings seriously, don't give private information to insecure websites (look for the lock icon).

Your worst loss when your laptop is stolen is your identity.
Vulnerability: Computers manage our finances, store personal, medical and contact data, and handle our online identities. Physical access to a laptop goes a long way to circumventing security precautions; a thief with your laptop in hand can easily bypass your login password or boot password by removing the hard drive and adding it to a different computer, for example.

Countermeasure: Invest in a full disk encryption utility like PGP Whole Disk or TrueCrypt, which will encrypt and password protect everything on your computer seamlessly and (pretty close to) impenetrably. Also, be aware of the physical security of your computer, like locks and cables, at home and traveling. To paraphrase Mark Twain, if you've put all your eggs in one basket – **watch that basket!**

Consider using a passphrase instead of a password – they're more secure and easier to remember. A good passphrase can be an obscure quote from a book or or the punchline to your favorite joke.

The *second* rule about data backups is making sure they work. Restore files from your backup to confirm the software is configured correctly and the backup media are in good condition, and to become familiar with the process so you'll be able to do it quickly in an emergency if necessary.

USB flash drives are just as dangerous as floppy discs.
Vulnerability: They have more storage capacity, but are easy to lose, so your chances of accidentally leaving lots of personal data in a taxi are higher. And they're particularly good at contracting and transmitting viruses, since most computers automatically install them, and may even automatically run programs on them when connected.

Countermeasure: Buy a spare to use in less trustworthy computers and keep it free of personal info. Put your flash drives on a sturdy lanyard or keychain and encrypt any personal data, or the whole drive, with software like PGP or Truecrypt; some flash drives come with built in encryption options. Consider disabling your computer's autorun feature.