IT Security - Guidance for Staff and Students.

Passwords and Accounts.

Your password protects your account from unauthorised access.

- Do not let anyone else know your password.
- Do not store your password in a file on your PC.
- Do not write down your password or leave it stuck on your desk or PC.
- When changing your password (which you should do regularly) do not re-use an old password (the system will prohibit this).
- Ensure that your password has a minimum of 7 characters where these characters are a mixture of letters, numbers and other characters (such as #@[] etc).
- Use a password that is not in the dictionary.
- Passwords will automatically expire once per year and you will be asked to change your password.
- After three attempted failed log-ins you will not be able to log-in again for a further 10 minutes. This discourages the automatic password detection programs.

Viruses/Malware etc.

You will read and hear about new viruses in the media – viruses can be particularly disruptive to your work and the work of your colleagues. You could easily become the unwitting vehicle for the circulation of viruses if your do not take precautions:

- Ensure that you have the University's virus checker installed on your PC and that it is set to check files regularly and that it updates itself each evening.
- Ensure that you have your home PC protected as well – Microsoft Security Essentials and AVG are available free for home use.
- Ensure that you have the latest Operating System Security patches installed on your computer.

ITD will not connect a computer to the University computer network that does not follow these guidelines and will disconnect any computer found to be in breach of this guideline.

Applications.

Most of the applications that you will need are available as part of ITD supplied set. These applications have been checked to ensure that they work correctly in the University environment. You need to be very careful about loading application programs from the internet or programs that your friends may give to you (they may even be infected with viruses).

- Do not download applications programs from the internet unless there is a clear need for you to do so and you trust the source/server that is providing it. Be particularly careful with respect to entertainment programs such as games etc.

- Ensure that you conform with any software licensing agreements for the application programs that you load onto your PC.

E-Mail.

Remember that it is easy for email to appear to come from someone you know when in fact it has been falsified. Also you cannot trust that even though you are sure of the source of the email that it doesn't contain (unwittingly) a virus.

- Do not open email attachments unless you are expecting them. If in doubt check with the originator of the message. Be especially careful of .EXE attachments .

Back-ups.

If your computer should become compromised then it is quite likely that you will lose all your data. You could also lose all your data through a hardware fault (such as a disk failure).

Back-up your computer at least once a week to a CD-writer, external disk, memory stick and store the resulting disks securely. After writing the back-up ensure that you can read back from the back-up.

Use the M: drive to store your data – this is backed-up each evening by ITD.

Memory Sticks.

Be particularly in the use of memory sticks. Don't put someone-else's memory stick into your computer unless you really have to. Always scan memory sticks for virus and malware before using them.

Physical Security.

When you leave your desk/office ensure that your lock the office, if this is not possible then log off of the PC or use a password protected screen saver. Terminate any active sessions to University servers (such as the Student Administration server).

PC Sharing.

Sharing files from your own PC to other staff or students (particularly students) opens your PC to a potential hacking risk.

Do not share out files from your own PC to students – use the E-learning environment SULIS or a fileserver provided by ITD or by your department instead or.

ITD Access to Your PC.

No implicit access to a staff computer is possible from ITD or elsewhere. If a staff member requires ITD to diagnose or fix problems on their PC it is expected that a staff member would grant ITD staff explicit access.

ITD staff accessing a staff member’s PC will abide by the following guidelines:

- Regulation - Access to an individual's computer by ITD staff

Gordon Young.
IT Director,
ITD
University of Limerick.
7th Sept 2010.