# Unit 242 it security for users

Law, Security

[242] IT security for users [242. 1] Select and use appropriate methods to minimise security risk to IT systems and data Assessment Criteria | 1. 1| | Describe the security issues that may threaten system performanceThe possible threats to system performance may be: unwanted e-mail (‘ spam’), malicious programs (including viruses, trojans) and hackers.

Security precautions can be taken beforehand such as use of access controls. We can configure anti-virus software, adjust firewall settings, adjust internet security settings; backup; store personal data and software safely; treat messages, files, software and attachments from unknown sources with caution; download security software updates. | | | | | | 1. | | Describe the threats to system and information security and integrityThe possible threats to information security may be: from theft, unauthorised access, accidental file deletion, use of removable storage media; malicious programs (including viruses, trojans), hackers, phishing and identity theft; unsecured and public networks, default passwords and settings, wireless networks, Bluetooth, portable and USB devices. | | 1. | | Keep information secure and manage personal access to information sources securelyProtect systems and data: Access controls: Physical controls: log-in details should be treated as credit card information and not to be left lying anywhere with an easy access, locks, passwords, access levels. | | 1. 5| | Describe ways to protect hardware, software and data and minimise security riskThere are steps to prevent threats to system and information: access to information sources should be allowed with Username and password/PIN selection.

The system set up on password strength; how and when to change passwords (monthly); online identity/profile; Real name, pseudonym; what personal information to include, who can see the information; Respectconfidentiality, avoid inappropriate disclosure of information. | | | | | | 1. 7| | Describe why it is important to backup data and how to do so securelyData backup involves the storing of files from your computer in another location. In this way, if there is ever any loss of data on your primary machine, you still have your data in backup in order to restore those files.

Read thisChapter 2 – Why Security is Needed

In order to maintain the integrity of stored data, project data should be protected from physical damage as well as from tampering, loss, or theft. This is best done by limiting access to the data. Manager should decide which members are authorised to access and manage the stored data. Notebooks or questionnaires should be kept together in a safe, secure location away from public access, e. g. , a locked file cabinet. Privacy and anonymity can be assured by replacing names and other information with encoded identifiers, with the encoding key kept in a different secure location.

Ultimately, the best way to protect data may be to fully educate all members of the team about data protection procedures. As a way of protection data and confidential information in Trust Royal Marsden Hospital there is mandatory Information Governance training yearly for every employee. Theft and hacking are particular concerns with electronic data. Many research projects involve the collection and maintenance of human subjects data and other confidential records that could become the target of hackers.

The costs of reproducing, restoring, or replacing stolen data and the length of recovery time in the event of a theft highlight the need for protecting the computer system and the integrity of the data. Electronic data can be protected by taking the following precautions: * Protecting access to data. * Protecting your system by keeping up-to-date software and if using connection to the Internet, use a firewall. * regularly back up electronic data files and create both hard and soft copies.

Data storage and backup is important because: * Properly storing data is a way to safeguard your information. * Data may need to be accessed in the future. * | | 1. 8| | Select and use effective backup procedures for systems and dataTo have an effective back up you will need to create a procedure for how you will back up data and restore your data in the case of loss. You will need to have a plan in place that details the steps to take when an emergency situation occurs. You will need to plan for each possible type of disaster and how you would recover from it.

You will also need to decide who is responsible for restoring files and which files have highest priority, and have acommunicationplan to keep everyone informed of the restoration process. At my workplace there is a following procedure in place: each employee has been created a personal U: drive to store confidential information which can be accessed by logging in with individually created nickname and password (that requires change monthly). And on each PC each employee can perform under Microsoft system tools - back up which can be stored on a server. In future the backed up data can easily be restored if needed. |