



UU Security Policy

Personal Computer Security Advice Note

Author:	Harry Young
Approved by:	IICTSC
Version:	2.0
Date:	1 June 2006
Status:	Agreed
Classification:	Public
Enquiry point	Harry Young Network Manager University of Ulster Phone: 028 90366488 Email: h.young@ulster.ac.uk
Policy effective from:	1 June 2002
Policy review date:	1 May 2007

Change History

Version	Changes	Date
1.0	Initial document	1/6/02
2.0	Included BS7799 reference Included section on identity theft	1/6/06

Contents

UU Security Policy	1
Personal Computer Security Advice Note	1
Change History	2
Contents	2
Personal Computer Security Advice Note	3
1. Introduction.....	3
2. Password Protection	3
3. Virus Protection	4
4. System Vulnerabilities	6
5. Personal firewall	6
6. Accidents and other risks	7
7. Identity Theft.....	7
8. Further Information	8
9. BS7799 Reference	8

Personal Computer Security Advice Note

1. Introduction

Computer security is the process of preventing and detecting unauthorised use of your computer. User education is an essential first step to protecting systems against data corruption and intentional misuse by intruders. The purpose behind this advisory note is to highlight best practices, thus enabling users to secure their systems against attack and data corruption. It is the responsibility of each personal computer user to take reasonable precautions to safeguard the security of their computer and the information contained upon it.

Some security issues arise from the possibility of intentional misuse of your computer by intruders via the computer network or Internet connection. Other risks can arise even if you are not connected to the network. Typical examples of this category would be hard disk failures, power supply failures and unprotected operator access.

We all depend on computers for everyday use and would find it very difficult to work if we were denied access to or lost the data on our computer. While we may not consider the data on our computers as “top secret”, the last thing you would want is an intruder accessing your computer to read personal information, corrupting information or using your computer to attack other computers.

It is impossible to guard or protect against every risk. But, if the best practices highlighted in this advisory are followed, your computer should be protected from most of the common intentional and accidental risks that you are likely to encounter. Remember this is not a “one off exercise”, but requires continued vigilance and system housekeeping to maintain system and data integrity.

2. Password Protection

Unless a computer is being used for purposes, which have no security implication, access should be restricted through password protection. There are several levels at which passwords can be used to help protect personal computers from unauthorised access. For information on passwords users should read the Password Policy.

Power-On Passwords

To prevent unauthorised access to your computer, power-on passwords should be set. This will prevent unauthorised people switching on or rebooting your computer in your absence. If this is not set, your computer can be switched on and the information accessed or programs installed without

your knowledge. If you have a screen saver password set and no power-on password set, rebooting your computer will by-pass the screen saver allowing access to your system.

Screen Saver Password

Most computers provide screen saver functions that have password protection. Once the screen saver has engaged, a casual viewer can no longer see what is on the screen. Additionally, the password protection prevents opportunistic access to your computer if it is left unattended for short periods. It is also advisable to assign a shortcut to your screen saver. This allows you to invoke the screen saver before you leave your desk.

Remote access

Staff may have information stored on their system to which other staff have access. Typical examples of this would be File Sharing under Microsoft networking or via Peer to Peer configurations to collaborate on shared documents. Database access over the network to information stored on your computer would be another common use. Where remote access to sensitive information or files stored on your computer is required, this access should be controlled via password protection. Access should also be restricted to the application or to the directory that contains the shared files. Only files that you intend for public access should be stored in this directory. Users should refer to the system manuals supplied with the applications for information on how to secure these services. It should be noted that adding services to your computer (e.g. ftp, remote logins ..etc) may turn it into a server and the conditions covered in the Server Connection Policy will apply.

Emergency Access

If critical data is stored on your computer, then there should be a process to enable selected staff to access this data in your absence. A recommended process would be to write your password down and place the paper in a sealed envelope. This envelope should be given to your line manager and stored in a safe place; typically a safe or locked cabinet with restricted access. In an emergency the envelope may be opened, by selected personnel, and the password used to gain access to critical information stored on the computer. Once the envelope has been opened, upon your return, new passwords should be allocated and the procedure repeated.

3. Virus Protection

Computer viruses are a continuing problem for many organisations. A computer virus is a piece of software which can be transferred between programs or computers without the knowledge of the user. The virus software contains instructions that when activated will either display a message, delete

or corrupt files, allow access to your computer or infect other programs or computers by exploiting the power residing in the computer.

It is strongly recommended that anti-virus software be installed on every computer. Anti-virus programs provide facilities for running constantly in the background, monitoring for unusual behaviour and are able to detect and alert the user of a possible virus attack.

In order to ensure the continued effectiveness of such products, it is important to keep them up-to-date with current virus and attack signatures supplied by the original vendors. Many anti-virus packages support automatic updates of virus definitions and engines. New viruses are discovered daily, so it is important to update these definition files regularly. For information on the current recommended University anti-virus program, contact the helpdesk on extension 66777.

Don't open unknown e-mail attachments

Before opening any e-mail attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognise. Be very wary of e-mails from unknown sources. Malicious code is often distributed in amusing or enticing programs.

If you must open an e-mail attachment before you can verify the source, the following process should be adopted,

1. be sure your virus definition files are up-to-date
2. save the file to your hard disk
3. scan the file using your anti-virus software
4. open the file

Don't run programs of unknown origin

Never run a program unless you know it to be authored by a person or company that you trust. Do not send programs of unknown origin to your friends or co-workers simply because they are amusing; they may contain a virus program. Always scan programs from unknown sources before running them. Likewise, always scan and check floppy/zip disks and memory sticks for viruses prior to using them.

Disable scripting/auto-run features in e-mail programs

Some e-mail programs are set to auto-run attachments whenever you click on the e-mail message. This allows the attachment to be auto-loaded and previewed before you have a chance to check the attachment for any hidden viruses. This feature should be disabled.

4. System Vulnerabilities

Keep operating systems and applications patched

Intruders are always discovering new vulnerabilities to exploit in computer software. The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems. When these holes are discovered in systems or applications, intruders are quick to utilise these vulnerabilities to attack or gain access to your system.

When vulnerabilities are discovered, computer manufacturers will usually develop patches to fix the problem. However, it is up to the user to download and install these patches or service packs. Most attacks are possible because users do not keep their systems patched to the latest revision. Some of the recent attacks are based on vulnerabilities that are several years old and could have been prevented if computers were kept up-to-date with the latest patches. These patches or service packs can be downloaded from the manufacturers' web sites. If available, systems should be configured to automatically download updates from the manufacturers' web sites.

Turn off/remove unused network services

Unused network services should be turned off or removed. The more network services installed on your computer the greater the risk. Unfortunately programs install, as default, all network services that may be required. For example, installing the Microsoft client will install NetBEUI and File and Print sharing. These applications, by default, allow unauthorised access to your computer. These unprotected features can be used to store or run programs on your computer without your knowledge. Users should check with their technical staff or documentation on what network clients are actually needed and remove those services not required.

Change default passwords

Default installations can create several risks. Attackers often gather knowledge about system vulnerabilities based on their copies of the same software. The first step is to change all default passwords for known user names, especially for administrative user names.

5. Personal firewall

It is recommended that a personal firewall software package be installed on your computer. This is specialised software that provides the ability to control the services, which are, permitted access to and from your computer.

Intruders are constantly scanning networks for systems with known vulnerabilities. Personal firewalls can provide you with some degree of protection against these attacks and alert you to the fact that you are being attacked or scanned. However, no firewall can detect or stop all attacks, so it is important to continue to follow safe computing practices.

6. Accidents and other risks

Make regular backups of critical data

In addition to the risk of data lost through attack, the data stored on hard disks are also at risk through hard disk failure. Hard disk crashes are a common cause of data loss on personal computers. Important files should be copied to removable media such as floppy disks, ZIP disks or recordable CD-ROM disks. Regular system backups are the only effective way to guarantee that lost or corrupted data can be restored. Several versions of the backup disks should be stored in a secure location away from the computer. The backup data should be regularly tested to ensure that it can be relied upon when needed.

Recovery CD

Computers are delivered with a recovery CD. This would be used to restore the operating system for your computer and to aid in the recovery from a security breach or hard disk failure. This CD together with any other driver CDs and licence numbers should be kept in a safe place and handed over in an emergency to aid the recovery of a damaged operating system.

7. Identity Theft

Identity theft is the stealing of a person's credentials to gain access to accounts and information. One of the fastest growing forms of identity theft is phishing. Phishing uses social engineering skills within bogus emails and web sites to trick the user into providing financial or personal information. These emails and web sites provide a significant resemblance to a tried and true online brand and due to the sophistication of the fraud sites and emails, it is becoming increasingly difficult to distinguish between a legitimate or an illegal site. The victim is usually tricked via an email to follow a link to a web site, where they will be asked to provide sensitive information into an online form. Once the fraudster has access to this information he can pretend to be you and could have authorisation to transfer all funds out of your bank account. Be very wary of unsolicited emails that ask you for personal information. Never following web links in these emails. Legitimate companies will never ask for account information and pin numbers on the same form. If in doubt, go direct to the company's web site and follow the links from their home page or contact the company by phone and query the email.

8. Further Information

Password Policy
Server Connection Policy

9. BS7799 Reference

A 3.1.2	Review and evaluation
A 4.1.3	Allocation of information security responsibilities
A 6.2.1	Information security education and training
A 8.3.1	Controls against malicious software
A 8.4.1	Information backup
A 8.7.4	Security of electronic email
A 9.3	User responsibilities
A 12.2.1	Compliance with security policy