

Introduction

Did you know that approximately 60,000 laptops are either lost or stolen each year in the UK¹? A report released by the Home Office also showed that of the students sampled, 33% had been the victim of crime in the last 12 months and almost 12% were the victim of theft².

West Yorkshire Police have reported that 1,500 laptops were stolen in North West Leeds over the last 12 months, with approximately 60% belonging to students³. As most students have a laptop and rely on it for work, then securing it from any form of attack or theft becomes a high priority.

Ask yourself the question; if your laptop were stolen, what would you lose? Music, photos, personal information, coursework, everything? How much would the loss cost you academically as well as financially?

My name is Adam Connell; I am a second year student at the University of East Anglia studying Computing Sciences. During the summer I was on placement with Platinum Squared, an independent information security organisation and was given this assignment to emphasise data security requirements within education. In this paper I will be looking at different scenarios that are incorporated in day-to-day life at a university. I will be discussing disk encryption, backups, anti-virus software, anti spyware software, USB security, as well as physical security and how you can achieve the best practise in security for absolutely nothing.

Backups

Scenario 1: The Importance of Backups

Adam has just finished his final year project and is about to print it off, when his computer suddenly turns off and will not restart. The main risk of not making a backup of his work is that, the project he had just finished will be lost, along with all of his other work, music and pictures. He will, therefore, have to redo his entire project from scratch at a much more rushed pace, meaning that the second piece of work may not be as good as the first and resulting in a lesser mark. Another consequence could be that he misses the deadline and is unable to submit anything at all and fails. Financially, the consequences are that as minimum he may have to repurchase expensive software or much worse still, have to repeat his final year at University, with costs for tuition fees and accommodation and consequential losses because he won't be able to start earning for another 12 months.

To avoid this situation is it advisable to make regular backups of all of your work, while you are working on them and after you have finished them. This will help not only help you recover information if your laptop or computer breaks but also if it is stolen. As well as backing up your documents, you should also make back-up copies of your software and email files because the loss of these can also cause significant disruption.

¹ <http://studentnet.abcolstudents.ac.uk/me/mysafety/Pages/laptopsafety.aspx>

² <http://rds.homeoffice.gov.uk/rds/pdfs2/r194.pdf>

³ <http://www.leedsuniversityunion.org.uk/knowledge/news/>

It is also advisable to save any current work to a memory stick or other portable device rather than on a separate partition on the same computer because keeping the files on the same disk runs the risk of losing everything should the computer be stolen or the disk crashes.

As an extra precaution it is a good idea to keep a full copy of all of your work, personal files and software either on an external hard drive, CDs or onto a computer at home or some other location away from where your laptop is kept. This means that if there is a problem, such as a fire, at your university and the local backup is lost then there is a remote backup at another location that you can still obtain and use.

Where possible store an up-to-date copy of all of your work (completed and currently being worked on) on the university servers themselves so if there are any issues and the main backup is lost there is another copy elsewhere that can be obtained and used.

It is recommended that you should make a local back-up at least once a week, and may be more frequently when approaching important deadlines. Remote back-ups should be made at least once every couple of months.

It is important to also think about the security of the back-ups. See the section on 'How accessible is your data' later in this article.

How to do a backup.

Certain releases of Windows contain a built in backup system, under system tools in the programs list.

To use this program in Windows Vista (for example) go to, start → programs → accessories → System tools → Backup Status and Configuration, then click set automatic file backup and then follow the wizard to choose where to store the backup (CD, external hard drive, partition on your laptop), here you can also choose to have it run automatically so you will always have the most up to date backup.

An alternative method when storing a copy of your documents on a home computer, select the files you wish to backup. Next right-click and go down to 'Send to', and then click compressed (zipped) folder, rename the folder to backup followed by the date, and then transfer the file from your computer to the computer it is going to be stored on, via USB storage device or CD.

How to restore a backup.

To restore a backup made using the Windows tool in Windows Vista, open up 'Backup Status and Configuration' and click restore on the left hand side followed by Restore Files. Then follow the wizard to restore the files from the last backup made. Alternatively if you stored your files in a compressed (zipped) folder on another computer, copy the most recent file back from the computer to your computer. Once transferred right-click the file and click 'Extract All' and follow the wizard to restore the files.

Anti-virus & Anti-spyware

Scenario 2: Infection of a Virus

Emily was researching sources of material for an assignment that she had been set, she went onto an internet site, which downloaded a virus to her computer without her realising it. The virus was used to gain access to her computer and install other programs that record her personal details, such as usernames, passwords, and other important information. It is worth noting that a virus can also delete data from the computer meaning that important data is lost which is another reason for always keeping a back-up of your data.

The consequences associated with this are varied, that important work or data could be lost or stolen due to viruses, or spyware giving a hacker a way into her computer. Most of the work that students do would not be regarded as commercially or politically sensitive, but disclosure of personal information can still expose students to issues as identity theft or even harassment.

As some software can be installed that records what she types into the computer and where she types it, important personal details such as bank or card details can be stolen and used by thieves.

It is essential that you have some form of anti-virus and anti-spyware software on your laptop or computer, as they protect your computer from viruses, spyware, trojans, worms, and other malicious software⁴. There are many free programs anti-virus and anti-spyware programs on the Internet.

For example, AVG free. This is a comprehensive anti-virus program that also has some anti-spyware software built in. The free version also comes with a link scanner to protect you from harmful websites, as well as a resident shield that scans all the files that you use and identifies anything that could potentially be a threat to the system and your work. It is available at <http://free.avg.com/>.

Avast Home Edition is a good anti-virus and anti-spyware program, that also has an adjustable mail and file system shields join the pre-existing behaviour, network, instant messaging, peer-to-peer, and Web shields. It is available at <http://www.avast.com/free-antivirus-download>.

Spybot: Search and Destroy is a free anti-spyware software which, tracks and removes adware, spyware, trojans, keyloggers, and various other types of malicious software. It also has an immunize feature that blocks unwanted malware before it reaches your computer. It is available at <http://www.safer-networking.org/en/spybotsd/index.html>.

Windows Security Essentials is a free windows anti-virus, anti-spyware, and malware protection tool, developed by Microsoft, it protects your computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software by detecting and removing known threats from your computer. It features real-time protection and minimizes interruptions. It is available at http://www.microsoft.com/security_essentials/.

⁴ Collectively these types of software are known as Malware

Data Encryption

Scenario 3: How Accessible is your Information?

Katie leaves her room unlocked while she goes into the kitchen to make dinner. Mean while an attacker enters her room and logs onto her laptop. From this he now has full access to all of the files on Katie's laptop. The attacker can find out personal information about the student such as usernames, passwords and bank account details or steal other data. If the attacker was another student on the same course, the attacker could steal Katie's coursework and submit it as their own or makes changes to the work to cause embarrassment to Katie.

The consequences of this type of account are that Katie could have her identity stolen; she could also have her bank or debit or credit card details stolen and used in various transactions that will affect her financially. If the attacker steals and uses her coursework then Katie could face the issues of being accused of plagiarism or embarrassment if the work has been tampered with.

A simple yet effective way of deterring a casual attacker is to use a password on the account so that they cannot log onto the computer without already knowing the password. In order to make the strongest password possible it is encouraged that you use a mixture of upper and lowercase letters, numbers, and special characters such as @, £, \$, &, !, _ and *.

A weak password would be 'katie'; in contrast a strong password would be along the lines of 'pL4t1num_Squ4R3d!' as this is a much harder password to guess.

A strong password will protect against casual attackers accessing the information on your laptop, but a determined attacker can overcome such defences and it is also important to think about the information you have transferred to other removable devices for example when you have made a back-up.

In order to further protect important information from unauthorised access it is vital that you encrypt the files and folders. Encryption stops unwanted access to your personal files and documents by protecting them firstly with a password that you set, and secondly by transforming the information in each document into an unreadable form to anyone that does not have the key (password).

There are several free encryption tools that incorporate various types on encryption algorithms, on the Internet as well as those built in features for Microsoft Office. A few available programs include:

- Truecrypt, which is available at <http://www.truecrypt.org/downloads>. An open source encryption tool that works on Windows, Mac OS x as well as Linux machines.
- Locknote, which is available at <https://www.steganos.com/us/products/free/locknote/overview/>. This is another open source encryption tool more specifically for text files, however it does make a good tool for storing personal information such as passwords, usernames, bank details and telephone numbers.
- Easy File Locker, which is available at <http://www.xoslab.com/>. This is a small file/folder locking tool that ensures unauthorised users will not be able to open, read, modify, delete, move, copy the locked files/folders, or even not be

able to see it. A password is used to control the application so no one will be able to access the application to change settings or stop the protection or even uninstall the program it without the correct password.

Microsoft Office has built in encryption tools that allow you to create a password for opening the file, as well as creating a password for modifying the document and controlling what modifications can be performed on the file. In order to password protect work/documents in Microsoft Office 2007 you have to go to menu→prepare→encrypt document and enter a password, in earlier versions this is under Tools→Protect Document and enter a password. However it is worth noting that encryption provided as standard by Microsoft Office is not regarded as strong protection and can be easily overcome by a determined attacker.

USB Security

Scenario 4: Losing your USB device

Max stores his work on his memory stick while he is working in the computer labs; he goes to the toilet and leaves his memory stick and other personal items unattended. When he returns his memory stick is missing. The immediate consequence is that Max will have to buy a new memory stick as a replacement for the one that was stolen, but the much greater risk is that the person who stole his memory stick can access the files on the memory stick.

In order to stop people from accessing the files on your memory stick it is important to encrypt your USB device. This will ensure that only you will have access to your files. A few of the encryption tools, for example Truecrypt, in the above section can also be used for encrypting USB devices. It is also advisable that if you are to leave your computer unattended, for whatever reason, either leave your memory stick with a friend, or take the memory stick with you.

Securing the BIOS

Scenario 5: The Power of Control

Michael leaves his room unlocked when he goes to a lecture. A passer by enters his room and turns on his laptop; while it is starting up he enters the BIOS of the computer and changes settings in the BIOS so that he is able to gain access to your system without needing a password. This could lead to data on the computer being stolen or removed, as well as programs being installed without Michael's knowledge.

To stop people from changing the BIOS settings and from accessing your system, you should set a start-up (BIOS) password that has to be entered before the computer is able to start up. If you do not have this password then you are not able to start the computer up.

Getting to the BIOS password varies depending on the manufacturer of your laptop, but generally turn on or reboot your computer, after a short time a message similar to "Hit the <X> key to enter the BIOS setup program" will appear, when the message appears press the required key or keys and a main menu screen will appear. Go to the security tab. Under this tab the number of passwords that can be set differs between types of laptop, however the most common one is Supervisor. Select Supervisor; you will be prompted to enter a password; unfortunately you are often limited to eight characters, however it is recommended that you use all of the eight characters for the best security. You will then be prompted to confirm the password,

enter the same password again. To set your system so that it asks for that password every time it boots, select the Password Check option and change the setting from setup to always. Now navigate to Save & Exit and select Exit & Save changes. Your machine will then reboot and you'll be prompted for the password. Often some machines only allow you to set a user password once the supervisor password has been set.

User Level Accounts

Scenario 6: It Came From the Internet

Fraser loved his new laptop and used it for everything, coursework, downloading music, watching films, sending joke emails, and chatting to his friends over instant messenger. This was until a couple of months later when his computer started to become sluggish and performance severely reduced. He took the laptop back to the company where he was charged for the technical support guys to look at his laptop and assess the problem. On inspection his laptop was found to contain hundreds of viruses, as well as other malicious software. Fraser then had to pay extra for the removal of the viruses on his laptop and he lost a significant amount of data.

Most people only have one account on their laptop or computer that they use for everyday usage, this makes your computer easier to break into and more susceptible to viruses or trojans. This is because the account has full administrator privileges and therefore if broken into can be used to install an array of programs, viruses and other malicious software all designed to break or damages your system, impede work progress and processor speed by clogging it up with useless processes, or record your personal details for future attacks and theft.

The problem can be reduced by creating one account that has full administrative properties and is used for carrying out system updates, such as installing new programs and hardware, as well as other administrative operations, and then having a second user account that is used for everyday purposes such as checking your emails, writing reports, and general day to day activities. This can reduce the infection success rate of a large number of virus attacks, trojans and malware, as under the user account you are not able to install new programs or access sensitive areas within the operating system.

However for a more effective result it is advised that you incorporate this method in conjunction with anti-virus and anti-spyware programs.

A web page that explains how to set up the user account, use extra features, and contains a very brief but precise question and answer section, is:
<http://www.microsoft.com/hk/protect/computer/advanced/useraccount.msp>.

Physical Security

Scenario 7: Locking your door

Tom leaves his room to go to the kitchen and socialise with his flat mates and ended up going to the bar without locking his room. The risks here is that a thief could walk into the flat and see that his door is unlocked and enter his room, this means that the thief could steal his laptop. Even if the laptop has been encrypted and therefore of no value to the thief, it would still result in Tom losing his work and having to buy a new laptop.

It is always good practice to keep your laptop in a locked room or cabinet when it is not in use. Another tip is to write your name and address on your laptop in a hidden place with an ultra violet pen, so that if it is stolen and recovered again then the police can return it to you. A cheap and secure way of locking a laptop to a desk is to use a lock cable, these are fairly cheap to buy and use a combination lock, which is harder to break through than normal locks.

Conclusion

To conclude, with theft being a particular problem for students the need to secure your laptop against any form of attack or damage is highly important. Using the techniques explained in this paper will help you to protect your personal files and documents, with only a small cost in terms of your time and little or no financial outlay.