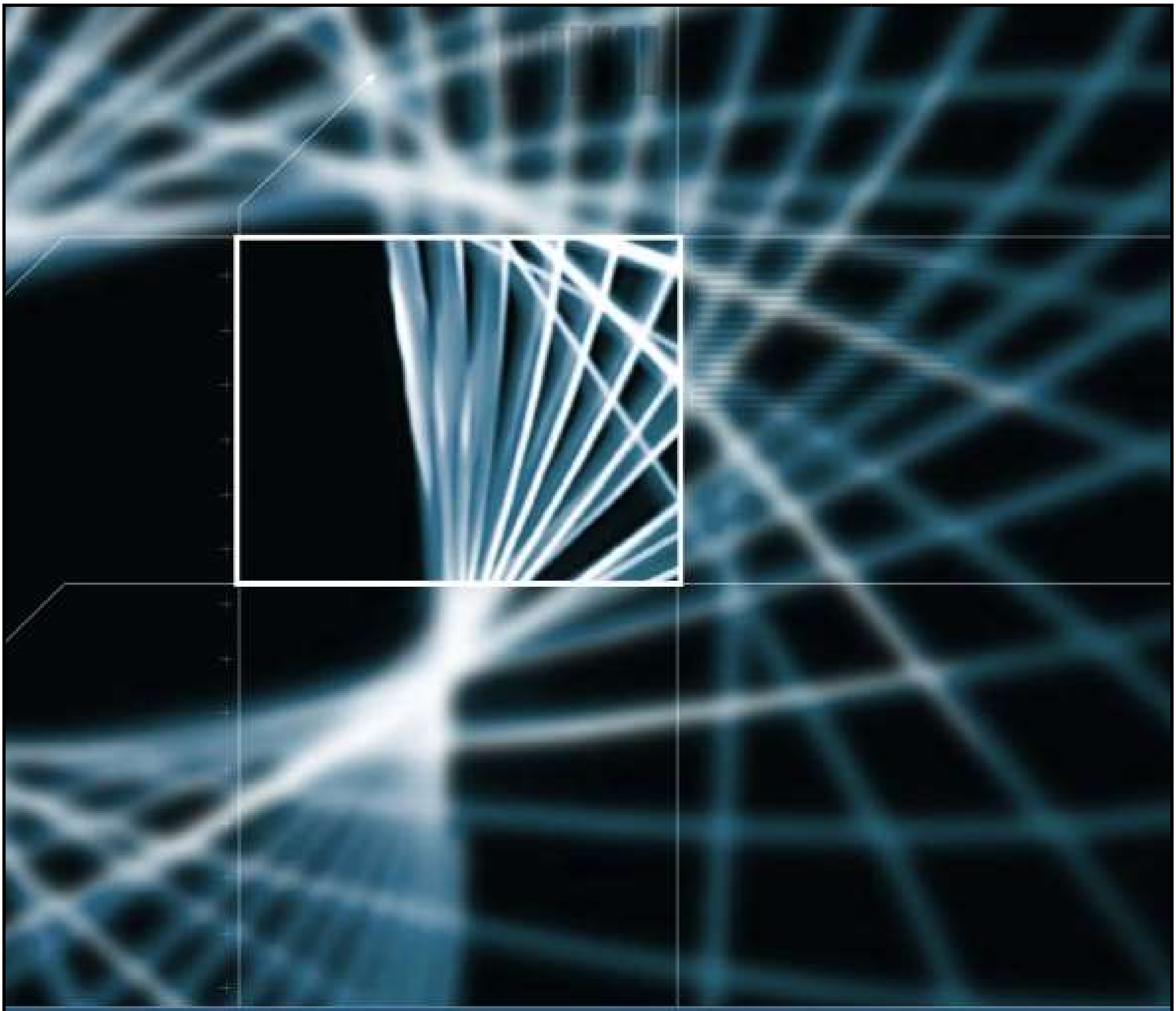


INTERNET SECURITY ASSESSMENT OF BEECHASH GROVE LIBRARY

Written by Jeffrey Farnan

INTERNET
SECURITY
SOLUTIONS

TABLE OF CONTENTS

INTRODUCTION

The management of Beechash Grove Library has requested Internet Security Solutions to analyse their computer systems and produce a report, after some problems have arisen with their operating systems and Internet Security. Internet Security Solutions is a full-service information security consulting firm which offers a comprehensive range of services to help businesses protect their valuable assets.

Information security is essential in order to prevent potentially costly and embarrassing security lapses. Internet Security Solutions will provides detailed assessments of the libraries entire security infrastructure to identify and eliminate any vulnerability. Internet Security Solutions bring their unique experience and the latest technology to address any vital security needs.

Internet Security Solutions will work closely with the management of the library to address each any security concerns without disrupting their ability to do business. Internet Security Solutions services are not limited merely to identifying and recommending effective countermeasures such as patching existing security vulnerabilities. Rather, the company is dedicated to helping the library to develop and maintain an integrated security infrastructure that can prevent and minimize the effect of future security lapses. Following its vulnerability assessment, this detailed written report will advise the management of Beechash Grove Library what systems were tested, and what vulnerabilities were detected, and recommendations for improving security.

OUTLINE

A brief outline was provided to me by the librarian stating relevant information and the incident s which accorded:

- Beechash Grove Library was awarded thirty-five computers in 2007.
- The computers were installed and set up by a local group.
- Apart from the local community, the dominant users are the senior citizens club and primary school teachers and children.
- The computers began slowing down, and still ran slow after shutting them down.
- The solution to this problem was to reinstall the operating system.
- The second incident was a child accessed a site containing pornographic material.
- This most recent incident caused a great deal of distress and anger from concerned parents, they requested to know what safeguards were in place, what policies and educational aims were in force for their children.
- The solution for the time being was to shut down all computers, and hire a professional in the I.T sector to assess the situation, provide an extensive and explanatory report which will be submitted to the meeting of the parents and concerned locals.

This report will demonstrate the safeguards that can be put in place but and they can work to secure their children online and a plan for the future maintenance of the local Beechash Library IT service.

The procedures /strategies that will be employed.

I will spend a day examining the computers and network system in the library, where I will:

1. Check each computer to find out what are the problems.
2. Identify the problems.
3. How bad are the problems.
4. Explain how these problems came about in the first place.
5. What can be done to solve the problems (Software needed).
6. Preventing these problems happening again.

The sections my report will have:

- Background – Here I will examine the pre-analytic data.
- Analysis – I will give exact details to the causes of the problems.
- Intervention / Recommendations – How to fix the problems and my recommendations.
- Conclusion – Briefly revisit the main points in my report.

Summarise my recommendations.

At the end of this report I will summarise my recommendations and any simplification needed will be readily made available.

BACKGROUND

Beechash Grove Library is responsible for providing library and internet services to its local population. The Library was awarded thirty-five computers in 2007, which purpose was to develop and enrich the I.T. skills of the various community groupings within the parish of Beechash. Many various groups, senior citizens and the local primary school benefit from the use of the internet, the senior citizens and the primary school being the dominant users of the internet.

Here is a full account of what was reported to me by the librarian.
A local voluntary group of 'mechanically' gifted people took responsibly for installing and setting up the computers on a network and connecting them to the Internet. All had been relatively well, until Patrick, the librarian, had a couple of incidents with the computers, the first had no specific date of onset but rather evolved over time. He noticed the computers began slowing down, became sluggish, Patrick, who does not know much about computers, simply turned off the computers and started them again hoping they would return to normal. This solution did not seem to solve the problem but over time the problem kept getting worse. After getting a number of complaints, Patrick asked the a few members of the voluntary group who set up the computers, what is causing this problem and how to go about solving this issue. After much debate to the cause and the potential solution, Patrick was told the best solution was to reinstall the Operating System using the CD that came with the computer. Patrick thought this would be the best solution so, he put an 'out of order' sign on each computer and set about the tedious task of reinstalling the operating systems. After two weeks the computers were up and running again as normal as ever.

The second incident, happened when the primary school children were having an internet class. Some children began shouting and laughing at something that appeared on a screen, when the teacher went to investigate, she found one of the boys had accessed a site containing pornographic material. The other children began looking for this material also, the teacher quickly asked the class to shut down the computers, while she searched for the librarian looking for an explanation. Patrick found himself in a very difficult position as he was simply unable to explain how this had happened.

A meeting was called by the concerned parents, who were deeply distressed and angered over the recent incident. They requested to know what safeguards were in place, what policies and educational aims were in force for their children, etc. Patrick had assumed that the children were completely protected, and he had never conceived of the danger, so he suggested hiring a professional in the IT sector to assess the situation, everyone at the meeting agreed. Until then all Patrick could do was turn off the computers and call Internet Security Solutions to solve the problem.

Summary of these Incidents and other Difficulties the Library was having:

1. Computers became extremely slow and the operating systems were reinstalled.
2. Children accessed sites of pornography and thus other groups were exposed to this material as it was still on the system following the children.
3. There was a recent deletion of all library records. How could this have occurred.
4. The use of chat rooms by children has led to a few overly friendly online ‘children’ wanting to meet.
5. Information being received by e-mail that was never requested is confusing some older groups.
6. The secure transfer of data from the Local Library to the County Library is sensitively discussed, how this could be protected.

ANALYSIS

This is an Analysis of all the problems which occurred.

1. Computers became extremely slow and the operating systems were reinstalled.

When the operating system was reinstalled it means I will never know what was causing the particular problems because the computer has been wiped clean, but I do know why computers slow down in general and they are:

1. Malware.
2. Data Storage.
3. Computer Misuse.

• Malware.

Malware is a term used to describe a wide range of malicious software that includes viruses, worms, or any other program that attempts to infiltrate or damage a computer without the owner's informed consent. In the Beechash Grove Library the general public spend a good deal of time on the Internet to visiting popular Web sites such as social networking sites and search engines, they were unknowingly opening the door to different types of Malware. Examples of malware include:

1. Viruses - A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc. A properly engineered virus can have a devastating effect, disrupting productivity and doing billions of dollars in damages.

2. E-mail viruses - An e-mail virus travels as an attachment to e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book.

3. **Trojan horses** - A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically.

4. **Worms** - A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

- Data Storage.

On many of the computers photos, documents are downloaded to the computers from Websites and emails, which use's vast amounts of memory. The users would have copied these photos to CD's, floppy drives or USB flash drive sticks and taken them away but forgot to delete the originals on the computer. This can slow down the computer's memory.

- Computer Misuse.

People can cause a lot of damage to computers, by not knowing what they are doing, especially children. Many people come into the library having never used a computer before, and don't know how it works or what to do, and can change files around or delete files, not knowing if they are important or not, this can cause serious damage to the computers.

The reinstalling of the operating systems.

The reinstalling of the operating systems was a good idea, it removed any viruses that may have been on the systems, but this is a temporary solution to a much larger problem. Without the correct Internet Security in place, the slowing down of machines will occur again. The reinstalling of operating systems should be the last option because:

- The reinstalling of operating systems from scratch takes a long time, all applications need to be installed, and drivers for printers need to be found or downloaded.
- People would have saved information or photos on the Hard Drive and unless saved onto an external disk would have all been erased.
- People would have had their own user accounts on the network, settings for their computer, and their favorite websites would have been saved, and they would have gained access with their own passwords, all these things would have to be set up again to the frustration of many people.

2. Children accessed sites of pornography and thus other groups were exposed to this material as it was still on the system .

No web filter was installed after the operation system was reinstalled, only 2007 Internet security was installed which protects against viruses, phishing attacks, spyware and malware. Web filtering software ensures that inappropriate Web sites such as those featuring adult content, gambling, or offensive material are not viewed on the computers. With Internet Explorer it is possible to see what Websites the previous people had viewed because Internet Explorer stores information in files about each site it has visited, these files are called Cookies. This material can be viewed again because Internet Explorer saves its history, and you don't even have to be connected Internet, it can be viewed offline. After checking the system, I confirm this is a major problem which will be dealt with in due course.

Web privacy and Internet cookies.

A common way for organizations to learn about the habits of a web user is to use cookies. Internet cookies are small files that are added to the hard drive while browsing the Internet. Cookies can be used to monitor the number of times Web site has been visited, to store user names and passwords for a particular Websites, or to gather information about the users Web browsing habits. Although cookies can make browsing more convenient, they can also be thought as intrusive. It can be unsettling to know that someone else can monitor what is browsed on the Web.

One site cannot necessarily access another site's cookies, but if someone gains access to your computer, they can copy your cookies and possibly get hold of personal information. Keep this in mind when deciding whether or not to allow your browser to store information like user names and passwords. You should certainly not do this at a workstation used by other people, and keep in mind that a computer's physical security is as important as its network security.

3. There was a recent deletion of all library records. How could this have occurred.

There are many possible ways someone could delete files on a computer, could have been an accident, could have been on purpose or worse a hacker could have gained access to your computer. But this is very unlikely as it was a standalone computer not connected to the Internet. This happened because the one password "Admin" used as the username and password, is used to log into all computers in the library. This means that anyone at anytime could have deleted the records. This information was on a computer in the office behind the library, so more than likely it was an accident caused by someone in the office, who simply didn't know what they were doing.

I accept that data was deleted so in the next section I will look at the ways to secure data and prevent data loss, by users of the computers and outside hackers.

4. The use of chat rooms by children has led to a few overly friendly online 'children' wanting to meet people in person.

Personal safety on the Internet.
The fast-changing technology underpinning this growth in Internet use is very poorly understood by the vast majority of its users. Indeed, one reason for the prodigious success of the Internet is that users can "surf the web" without having to understand the technical means by which information is accessed or communicated. The many layers of technology that lie beneath the interface seen by the user, typically a software application known as a web browser, are effectively hidden. But just as the technology is for most users invisible, so are the risks.

These risks are manifold. They threaten personal security—that is to say, they may undermine the individual's ability to control the information that they have entered into or stored on connective devices such as PCs, mobile telephones, or databases operated by commercial organisations, government agencies and others. Victims typically suffer financial loss through fraud, though in cases of identity theft they may also suffer loss of reputation, or, in extreme cases, may be accused of crimes they did not commit.

Online risks may also impact upon personal safety—by which we mean they may lead to direct physical or psychological harm to the individual.

One high-profile threat is that posed to children by predatory paedophiles, who conceal their true identity whilst using the Internet to "groom" potential victims. Probably far more common is the online bullying of children by their peers, while even adults who injudiciously disclose personal information online have found that their personal physical safety has been compromised.

Children have always been curious about other cultures and have always tried to make friends with other children, at one time you used have to post letter to your pen pal and then wait with excitement for weeks for a reply, but with the explosion in the use of social networking sites such as Bebo, MySpace, YouTube and Facebook, you can send an email to anyone you want to be friends with, many of these websites have their own chat rooms where you instantly chat to any one you want, and anyone can contact them very easily. Here I will discuss the benefits and dangers of children using these social networking sites.

The benefits to using social networking sites .

Childern and young Adults like to can keep in contact with their friends by email and can make new friends very easily online by searching social networking sites, for people with similar interests. To create their own profile they can register with a particular social networking website, and can post a profile of themselves which can be read by others online. The next step is to invite their existing contacts to join their profile. They are usually invited from their existing e-mail and messenger contact lists. Many young people are using social networking sites everyday; it's just another part of their life. They can be surfing social networking sites while doing their homework, downloading music, or chatting on Instant Messenger.

They want to be with their friends in a space that is not inhabited by adults and because of the constraints imposed on them; they rarely get the opportunity to do this outside their virtual environment.

The dangers to using social networking sites .

Like most online activity there are risks to the users. In the case of social networking websites the primary risks involve the unintentional disclosure of personal information, bullying and in a small number of cases targeting of users by predators.

Disclosing Personal Information.

The way these sites work is based on users creating sites /profiles including their personal opinions and in most cases photographs on aspects of their lives. This enables people with the same interests to meet others. Users' profiles are also a way of attracting potential girlfriends or boyfriends. Many young people will send flirtatious comments to others having been attracted to photos on their site. The problem with posting personal information to the Internet is that as soon as it goes online, the user has lost control over who will see it and how it will be used.

Pictures can be easily be copied and displayed in a completely different context. Given that most photos now are digitally produced, they can be even be altered or distorted. Many social networking websites give the impression to users that they are in closed networks of friends. This encourages young people to disclose more personal information or to be more intimate with their communications than they would be if they thought it was a completely public forum. The fact that certain websites claim to connect students from the same school does not necessarily mean that they are safer.

The information provided by users when they are registering is often not validated. Any individual can create a user profile pretending to be anyone else. Moreover, anyone regardless of their real or pretend age can join any online community they choose irrespective of their age just as the can when joining a chatroom or bulletin board online.

Being Targeted by Predators.

Because there is no routine validation of users, personal information contained in profiles can be used by unscrupulous individuals as the basis for scams, malicious attacks, or in the worst cases by paedophiles to groom potential victims. These people often operate by collecting small pieces of information at a time while slowly building up a bigger picture of their target without arousing suspicion. They can use multiple different identities to avoid detection.

With regards to this pacific problem I can confirm this sounds like its Predators targeting children and trying them to meet up with them, I have solutions for this in the next section.

5. Information being received by e-mail that was never requested is confusing some older groups.

This is a major problem on the internet there are two types of email that you get almost daily. The first is Spam or "junk mail", this is unsolicited direct marketing, these emails try to get you interested in buying products. The second is Phishing and this is far more serious. Phishing refers to the scam of sending out mass email messages in an attempt to get someone to respond by providing personal information, thinking the e-mail message is from a legitimate source. The message might look like it's from a bank and request that the reader follow a hyperlink to a page that looks like the bank's Web site. If the user logs in he has just provided the scammer with his user name and password. After checking the system I can accept that this is a problem which must be dealt with.

6. The secure transfer of data from the Local Library to the County Library is sensitively discussed, how could this be protected.

The secure transfer of data is vital to most banks, businesses and library's, if this information got into the wrong hands many people would be put at risk. In the case of library information which consists of personal information on individuals, keeping it secure is of vital importance. Many people have taken up Internet Banking and Shopping in the Library and they're personal data needs to be kept safe A safe option to transfer data across the Internet would be to software which has been encrypted.

What is Encryption.

To protect confidentiality of the data stored on a computer disk a computer security technique called disk encryption is used, which is software that is used to implement the technique. Such software encrypts data stored on a computer's mass storage and transparently decrypts the information when an authorized user requests it: no special action by the user (except supplying a password or passphrase at the beginning of a session) is required. Some also provide plausible deniability with deniable encryption techniques. The volume-level encryption is particularly suited to portable devices such as laptop computers and thumb drives. If used properly, someone finding a lost device will have access only to inaccessible encrypted files. A strong passphrase is essential for full security.

INTERVENTION / RECOMMENDATIONS

For each of the main problems addressed in the Analysis, I will now provide a solution that will adequately solve these problems.

1. Computers became extremely slow and the operating systems were reinstalled.

I stated that the three major problems were Malware, Data Storage and Computer Misuse. I will look at how to prevent these problems from occurring.

- Malware.

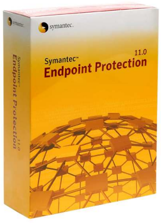
What needs to be installed is a new **Antivirus Software** that was released this year.

Viruses are one of the biggest problems related to internet security. They can come in many forms, and there are new ones all the time so it's important that you have an antivirus program installed AND that you keep it up to date on a regular basis.

What I recommend: Antivirus software that comes highly recommended is one that is used in all major businesses throughout the world.

Symantec™ Endpoint Protection

The next generation of antivirus technology from Symantec



About Symantec.
Symantec is a global leader in providing security; storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.
Symantec Endpoint Protection provides the following:

1. **Antivirus and Antispyware:** Antivirus and Antispyware scan for viruses and for other security risks, including spyware, adware, and other files that can put a computer or a network at risk.

2. Personal Firewall: The Symantec Endpoint Protection firewall provides a barrier between the computer and the Internet, preventing unauthorized users from accessing the computers and networks. It detects possible hacker attacks, protects personal information, and eliminates unwanted sources of network traffic.

3. Intrusion Prevention: The intrusion prevention system (IPS) is the Symantec Endpoint Protection client's second layer of defense after the firewall. The intrusion prevention system is a network-based system. If a known attack is detected, one or more intrusion prevention technologies can automatically block it.

4. Proactive Threat Scanning: Proactive threat scanning uses heuristics to detect unknown threats. Heuristic process scanning analyzes the behavior of an application or process to determine if it exhibits characteristics of threats, such as Trojan horses, worms, or key loggers. This type of protection is sometimes referred to as zero-day protection.

5. Device and Application Control: Device-level control is implemented using rule sets that block or allow access from devices, such as USB, infrared, FireWire, SCSI, serial ports, and parallel ports. Application-level control is implemented using rule sets that block or allow applications that try to access system resources.

6. Kernel-level rootkit protection: Symantec Endpoint Protections expands rootkit protection, to detect and repair kernel-level rootkits. Rootkits are programs that hide from a computer's operating system and can be used for malicious purposes.

7. Role-based administration: Allows different administrators to access different levels of the management system based on their roles and responsibilities.

8. Group Update Provider: Symantec Endpoint Protection clients can be configured to provide signature and content updates to clients in a group. When clients are configured this way, they are called Group Update Providers. Group Update Providers do not have to be in the group or groups that they update.

9. Location awareness: Symantec Endpoint Protection expands location awareness support to the group level. Each group can be divided into multiple locations, and, when a client is in that location, policies can be applied to that location.

10. **Policy Based settings:** Policies control most client settings, and can be applied down to the location level.

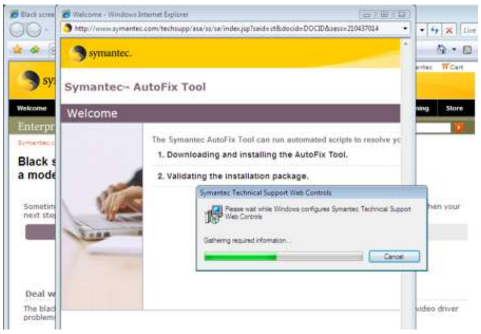
11. **Enhanced LiveUpdate:** LiveUpdate now supports the downloading and installation of a wide variety of content, including definitions, signatures, white lists to prevent false positives, engines, and product updates

The Advantages.

With this software you will have the most up to date security. Automatic Updates. This one product can solve several of your problems.

The Disadvantages.

Is expensive at 150 euro for a business package.
Only lasts one year till it has to be replaced.



Black scree
Welcome - Windows Internet Explorer
http://www.symantec.com/techsupp/asa/ss/sa/index.jsp?said=ct&docid=DOCID&sess=210437014
symantec.
Welcome
Enterpr
Store
Cart
Live

Symantec™ AutoFix Tool

Welcome

The Symantec AutoFix Tool can run automated scripts to resolve yo

1. Downloading and installing the AutoFix Tool.

2. Validating the installation package.

Symantec Technical Support Web Controls

Please wait while Windows configures Symantec Technical Support Web Controls

Gathering required information...

Cancel

Antivirus Checks.

With so much computer equipment be it hardware or software, anti-virus software dates very quickly, so one should get your anti-virus soft- ware checked at least twice a year if possible to ensure you have adequate protection and if not to get your anti-virus software upgraded accordingly.

Automatic updates.

In order for any antivirus software package to be effective, it’s imperative that the virus signatures be kept updated. Signatures, sometimes called definitions, are descriptors used by the software to identify virus programs. Signatures are specific to the antivirus software you use. Most modern antivirus programs automatically download and install new virus signatures if you are connected to the Internet.

Writers of malicious software are always finding new operating system vulnerabilities, and software vendors continually patch holes in response. Microsoft regularly releases updates to Windows to address problems and new security threats and to add new features. Although the new features can be a nice reward, the most important reason for you to update your copy of Windows is to keep pace with the ever-evolving security threats that you and your PC face.

- Data Storage.

All computers need to be checked to see if there are unnecessary files lying around on the hard drive which is taking up space. I would strongly recommend telling people not to leave personal files on the computers and it will be removed after a certain amount of time. Another good idea is to use Disk Cleanup and Disk Defrahmenter.

Disk Cleanup.

You can use the Disk Cleanup utility to remove unnecessary files, such as temporary Internet files, unused programs and Windows components, and deleted files. Disk Cleanup scans your drive for files that can be safely deleted, but still gives you the option to keep or delete these files. Disk Cleanup also gives you shortcuts to the Windows Components and Remove Programs windows so you can remove features and programs you don't use. You can also remove all restore points but the most recent one.

Disk Defragmenter .

Over time, your drive might become fragmented, meaning that individual files are broken up, with the parts saved in different physical spaces on the hard disk. Your computer's performance suffers when your disk becomes highly fragmented. This slowdown occurs because Windows has to access multiple locations on the disk to read or write all the various parts of your files. Defragmenting you disk consolidated files so that each one is saved in a contiguous physical space on the disk. This makes access faster and used storage space more efficiently.

2. Children accessed sites of pornography and thus other groups were exposed to this material as it was still on the system following the children.

To prevent children accessing such sites you need:

Internet filter software.

Internet filter software gives you the ability to control content displayed, block websites and set up passwords. Powerful services like email filtering, popup blocking and chat room monitoring are just some of the tools available with today's internet filter software, each designed to protect against and counteract the tactics of aggressive online porn companies.

What to Look For in Internet Filter Software,

Even though the perfect internet Filter does not exist in today's marketplace, there are a number of great solutions depending on your Library’s needs. There are many different brands of Filtering software e.g. Cyber Patrol, Net Nanny or Surfwatch, McAfee and Kaspersky, which all provide the same filtering options

Ease of Use.

The most important attribute an Internet filter program can offer is an easy-to-use design, making it possible for people with all levels of computer experience to easily install and use the filter to its fullest capacity.

Effective at filtering.

Top internet filter software offers a good balance between filtering objectionable material and not filtering too much content. Another important aspect is the ability to customize the filter's sensitivity for each family member.

Filtering algorithm.

The best filter programs use a combination of filtering techniques, including URL filtering, keyword filtering and dynamic filtering.

Activity reporting.

The most useful internet filter software offer reports on what each family member has been doing on the computer, which includes websites visited, chat room activities, IM conversations and so on.

Client-Server based.

Good filtering programs offer a flexible platform, which allows users to decide whether their optimal filtering solution is client (home computer) based, server (Proxy or ISP) based or a combination of both.

Port filtering and blocking.

Filtering programs should block or filter all major internet protocols, including web access, chat rooms, email, peer-to-peer networks, bulletin boards and pop-up windows.

Advantages: With internet filter software and proper supervision, parents can keep their families safe from the ever-present problems and help them enjoy the most educational and entertaining aspects of the internet.

Disadvantages: This product costs around 100 euro and again this software has to be updated each year.

3. There was a recent deletion of all library records. How could this have occurred.

As I mentioned earlier this was caused by the one password being used by all computers. They are always benefits to using one password, very simple to remember and you can gain access to all the computers, but very serious problems can occur when using this method. To prevent this problem from happening again I recommend three suggestions.

1. Changing the passwords.
Every working in the library should have their own password, for security reasons and no one would be able to gain access to their computers. If anyone loses or forgets their password the network administrator should be able to help.

2. Keeping the files on the server and only letting certain users gain access to it.
All important information should be kept on the server, so people can gain access to if from their own computers. The administrator can block people from getting this information or allow certain to gain access, and the administrator can allow people to only read the documents and not to change or delete it.

3. Backup.
Most organisations backup their data, on external hard drives, or on Tape which is still a popular method of storing data, every day, week or month it is usually backed up. So it any valuable information was deleted again you will always have a copy stored somewhere.

4. Firewall.
A Firewall can come in two forms Hardware and Software. It comes as a hardware component in the shape of a router, the software scans and checks web pages, making sure no viruses or worms can access your computer, while you are viewing websites.

Advantages: A properly-configured firewall will help shield your computer from outside hacker attacks.

Disadvantages: Firewalls can be difficult to configure correctly, especially for novices. Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly

4. The use of chat rooms by children has led to a few overly friendly online ‘children’ wanting to meet.

This problem is very hard to solve, because technology can only do so much, the best software in the world can’t tell if an email or that instance messaging is sent from an adult or a child. But you can supervise what content they have viewed and you can take steps to prevent anyone gaining information about your children. Here are some steps for you and your children to enjoying a safer time on the web.

Communication.

Explain to the kids what kind of dangers they need to watch out for on the internet. Set some rules that they need to follow, such as never sharing any personal information with anyone, tell you if something happens that makes them uncomfortable, and never meet someone in person who they've met online without your permission.

Parental Control Software.

Parental control software will limit access to certain types of websites or other content that is objectionable. This software is not 100% foolproof but it will filter a great deal of what you don't want your kids to see.

Key Logging Software.

The other option is software that keeps a log of everything your kid’s type. It can track chat sessions, websites visited, email sent and more. If you use this, it's best to let your kids know you're doing so. Explain to them that you're not spying on them but you want them to be careful of what they do online.

Communication.

Communication is the most important aspect of keeping kids safe online. Help them to understand why you're concerned and what kind of dangers are out there, and they'll be safer for it.

I have set out some guidelines for parents and teachers who should supervise and screen the contacts the children have on the web.

Never give out personal details.

Some children and young people have their own web sites or post material to web sites maintained by their school or a youth group they are involved with. Tell the children, if you choose to post something on the web, be sure never to include your address, telephone number, or a photograph of yourself. If you do want people to be able to contact you through the web, just give an email address, preferably a central email address used by the school or youth group's website.

Chat Rooms.

Chat rooms are widely regarded as probably the most dangerous area on the Internet as you have no reliable way of knowing whom you are chatting to or who is listening in, so never say anything in a chat room you would not say in public. You might meet someone in a chat room who appears to be sympathetic and understanding and offers wonderful advice and friendship. If the relationship remains strictly online, that could be fine as long you are careful not to give out any personal information and you also let your parents (or school or youth group if using one of their computers) know that such a relationship has developed.

Meeting Up.

The thought of getting together with someone you meet in a chat room and you like to 'chat' to is natural and can be exciting to look forward to, but remember people are not always who they seem to be. The basic rules for online safety apply to all areas of the Internet, but they are especially important in chat areas. Never give out personal information or arrange a face-to-face meeting with someone you meet in a chat room without first checking with parents, also be suspicious of anyone who tries to turn you against your parents, teachers, or friends or wants to meet you in secret.

5. Information being received by e-mail that was never requested is confusing some older groups.

Be particularly careful when opening email and/or attachments to email from unknown or new sources. Where possible run an anti-virus software package, because the email could contain a virus. If in any doubt do not open an email, simply delete it. If it is genuine and important the individual will usually follow up by another communication method if they do not receive a reply to the email.

People get email messages every day claming to be from major banks, credit card companies, PayPal, ebay, and so on, as explained in the pervious chapter this is known as Phishing or Spam. These messages often claim that your account will be disabled if you don’t log in soon, or that your account might have been compromised by a third party and you’d better log in to prevent someone from taking your money.
One rule of thumb is to simply never click a link in an e-mail message that asks you to log into a secure account or provide other personal information. Before you log into a secure site, check the address bar and be sure the address starts with the legitimate site name. There is nothing to stop a phishing site from imitating the look of a legitimate site in every detail, but if you check the Address bar, you should be safe.

The best defence against these emails is Phishing software which comes with Symantec Endpoint Protection and The Phishing Filter which comes with Internet Explorer 7. They can be set to automatically evaluate pages you visit, or you can manually test a site that you might suspect.

The Phishing Filter.

The Phishing filter can be set automatically to evaluate pages you visit, the Phishing filter evaluates sites in three ways.

- It checks the site against a list of known phishing sites. This is stored on your computer,
- It checks the site for a series of characteristics common to phishing sites.
- If you consent, it checks the sites against of frequently updated list of phishing sites maintained online by Microsoft.

To check a site manually, click Tools and choose Phishing Filter, Check This Site. If a site has not been checked before, the status bar will display an icon that allows you to check the site. This icon looks like a window with a black exclamation mark in a yellow circle. To turn on automatic checking, click Tools and choose Phishing Filter, Turn on Automatic Website Checking.

The Phishing Filter submenu also has options for changing filter settings and reporting a site you may think is fraudulent. You can disable the Phishing filter completely, in which case the icon will not appear when you visit new sites.

Advantages: With this software you can block spam and it comes with Symantec and Windows explorer 7 so no extra cost.

Disadvantages: Can block genuine emails from time to time, but they are only sent to your junk folder.

6. The secure transfer of data from the Local Library to the County Library is sensitively discussed, how could this be protected.

You can buy software to Encrypt and secure your company's data. This software protects confidential information and ensures regulatory compliance with a range of solutions that deliver policy-based security across mixed environments and operate transparently to users. A product I would recommend is Sophos.

Sophos.

Sophos protects confidential information and comply with regulatory mandates–safely and securely–with SafeGuard Enterprise solution. SafeGuard Enterprise is a modular information protection control solution that enforces policy-based security for PCs and mobile devices across mixed environments. It is fully transparent to end users and is easy to administer from a single central console. SafeGuard Enterprise provides multi-layered endpoint data security by combining encryption and data leakage prevention (DLP).

Its modular architecture provides comprehensive data security tailored to user’s organization's needs and growth requirements. SafeGuard Enterprise has the most flexible centralized policy and key management functionality available today:

Why Sophos.

Industry certified, award-winning technology already protecting millions of users. Superior key management for secure and easy data sharing and recovery. Reduces cost by integrating easily into your existing infrastructure. Centralized, integrated policies for full disk encryption, removable media encryption and port control. Modular architecture enables users to tailor the solution to their needs.

Key Features:

1. Delivers centralized data security control across mixed IT environments
2. Provides consistent implementation and enforcement of company-wide security policies.
3. Centralized state-of-the-art key management makes storage, exchange and recovery of keys simple and easy.
4. Provides comprehensive data protection on all kinds of devices: laptops, desktops, removable media, PDAs, CDs, email, etc.
5. Only product to offer encryption and data leakage prevention (DLP) under a single management console.
6. First and only solution that fully manages Windows Vista BitLocker Drive Encryption.
7. Integrates quickly and effectively with existing security infrastructures and automates administrative tasks.

- Advantages:

  With its modular, scalable and open architecture, SafeGuard Enterprise provides seamless integration of current and future SafeGuard modules, new security components and third-party products—guaranteeing continuous investment protection.

- Disadvantages:

  Can be expensive at 120 euro, needs to be installed on both computers.

CONCLUSION

In this conclusion I will briefly revisit the main topics of my report.

- The slowing down of the computers.
  What I recommended was Symantec Endpoint Protection to beat any Malware, cleaning up the hard drive with Disk Cleanup and Disk Defragmenter.

- Children accessed sites of pornography.
  I mentioned Internet filter software that should be gotten and several brand names that are available. What to look for when buying the software.

- The deleting of Records.
  Change the passwords, only letting certain people access to valuable information, backing up your information and Firewall protection so hackers can't get access information.

- The use of chat rooms.
  Here I outlined the dangers using chat rooms, and said children should be supervised at all times and gave guidelines for Parents and Teachers.

- People getting emails.
  The Phishing Filter and Phishing software would help solve these problems

- Securing data.
  Here I mentioned software that would secure the data, and be safe to send by email.

SUMMARY OF RECOMMENDATIONS

- Purchase up to date Internet Antivirus software for your Internet Security.
  I recommended using Symantec Endpoint Protection and outlined all the benefits.

- Purchasing Internet filter software to filter out any unwanted Sites.
  I recommended the benefits and brand names that can be purchased.

- Change Passwords, Save Information on the Server, Backups up files.

- Supervise the children while on the Internet,
  Closely supervise the children, warn them of the dangerous and never to give out personal details.

- Use The Phishing Software and Phishing Filter in Internet Explorer 7.
  This will help protect your computer from viruses being secretly downloaded to your system.

- Use Sophos Software to Encrypt data.
  When transferring files by email all data should be encrypt, so information will be safe.

BIBILOGRAPHY

Introduction - sections taken from from *www.mitnicksecurity.com/company.php*

Background - section taken from Project Brief

Analysis

- Sections taken from *CompTIA Strata, PC FUNDAMENTALS* by *CompTIA PRESS*
- Sections taken from *www.publications.parliament.uk.pdf*
- Sections taken from *safe social networking guidelines-PDF*
- Sections taken from *www.wikipedia.org*
- Sections taken from *Sams Teach Yourself Networking* by Uyless Black published by SAMS

Intervention / Recommendations

- Sections taken from *CompTIA Strata, PC FUNDAMENTALS* by *CompTIA PRESS*
- Sections taken from *Sams Teach Yourself Networking* by Uyless Black published by SAMS
- Sections taken from *www.Symantec.com*
- Sections taken from *Symantec Endpoint protection - PDF*
- Sections taken from *from* www.internetsecurityguide.org
- Sections taken from *www.Sophos.com*