

# **The internet:**

**Keeping it a source for good not bad**



---

Diocese of Southwell & Nottingham

---

## Contents:

How much do you know about the internet? . . . . .	2
The statistics . . . . .	3
Tips to keep your family safe . . . . .	4
Important software . . . . .	6
Useful websites . . . . .	7
Glossary . . . . .	8

**“Finally, brothers and sisters, whatever is true, whatever is noble, whatever is right, whatever is pure, whatever is lovely, whatever is admirable—if anything is excellent or praiseworthy – think about such things.”**

Philippians 4:8

## **How much do you know about the Internet?**

The internet had its beginnings as a cold war project to create a communications system that was immune to nuclear attack back in 1969. It was really in the mid-90s that the internet that we know today was born and started to grow. Between 2000 and 2004 the number of people using the internet grew by 125% to over 800 million. It is very difficult to calculate how many web pages there are in the world, but the most popular search engine, Google, currently searches over 8 billion of them. The internet is now no longer merely an informational tool, it is used for shopping, banking, communicating, for phoning and video conferencing and is now a central part of many people's lives. What we know is- it is here to stay, whether we like it or not. The internet, due to it being uncensored and open to the whole world can be a dangerous place. Most of the internet is fine, but there are many places that Christians and non-Christians alike should avoid. Pornography, violence and obscene material is unfortunately far too common on the internet, and the problem is not going away. Parents, children and everyone should be aware of the potential dangers and get wise. The following statistics are taken from the website [www.internetfilterreview.com](http://www.internetfilterreview.com) and show the extent of pornography of the internet.

# The Statistics

## Pornography Industry Revenue Statistics

Size of the industry	\$57.0 billion world-wide
Adult videos	\$20 billion
Escort services	\$11 billion
Magazines	\$7.5 billion
Sex clubs	\$5 billion
Phone sex	\$4.5 billion
Cable/Pay per view	\$2.5 billion
Internet	\$2.5 billion
CD-Rom	\$1.5 billion
Novelties	\$1.0 billion
Other	\$1.5 billion

## Internet Pornography Statistics

Pornographic websites	4.2 million (12% of total websites)
Pornographic pages	372 million
Daily pornographic search engine requests	68 million (25% of total search engine requests)
Daily pornographic emails	2.5 billion (8% of total emails)
Average daily pornographic emails/user	4.5 per Internet user
Monthly Pornographic downloads (Peer-to-peer)	1.5 billion (35% of all downloads)
Daily Gnutella "child pornography" requests	116,000
Websites offering illegal child pornography	100,000
Sexual solicitations of youth made in chat rooms	89%
Youths who received sexual solicitation	20%
Worldwide visitors to pornographic web sites	72 million annually

## Children Internet Pornography Statistics

Average age of first Internet exposure to pornography	11 years old
Largest consumer of Internet pornography	12 - 17 age group
15-17 year olds having multiple hard-core exposures	80%
8-16 year olds having viewed porn online	90% (most while doing homework)
7-17 year olds who would freely give out home address	29%
7-17 year olds who would freely give out email address	14%
Children's' character names linked to thousands of porn links	26 (Incl. Pokeman and Action Man)

## Adult Internet Pornography Statistics

Men admitting to accessing pornography at work	20%
US adults who regularly visit Internet pornography websites	40 million
Promise Keeper men who viewed pornography in last week	53%
Christians who said pornography is a major problem in the home	47%
Adults admitting to Internet sexual addiction	10%
Breakdown of male/female visitors to pornography sites	72% male - 28% female

## **Women and Pornography**

70% of women keep their cyber activities secret

17% of all women struggle with pornography addiction

Women, far more than men, are likely to act out their behaviours in real life, such as having multiple partners, casual sex, or affairs

Women favour chat rooms 2 times more than men

1 of 3 visitors to all adult web sites are women

9.4 million women access adult web sites each month

Women admitting to accessing pornography at work 13%

## **Tips to keep your family safe**

People have different reactions to statistics such as these. Some people are not surprised, but most are shocked. Some people say that they would never be tempted by such filth. Don't get complacent! The Bible warns us not to consider ourselves above temptation. 1 Corinthians 10:12 says, "So if you think you are standing firm, be careful that you don't fall!" and Proverbs 16:18 reminds us that "Pride goes before destruction, a haughty spirit before a fall". Scripture also encourages us to take practical steps to "guard our heart" (Proverbs 4:23) and to look at only those things are "pure and lovely" (Philippians 4:8). It is important to put some safeguards in place for yourself and your family so that your computer is safer.

- **Place your computer in an open room with the monitor facing out.** This allows you to see and control what is occurring on the internet. A computer in a bedroom is extremely inadvisable. Remember all internet activity is stored in history and temporary internet files, and although this can be wiped, it is obvious when this is done.
- **Install anti-virus software.** Keep your virus definitions up-to-date (check daily) and do a full system scan once a week.
- **Install a firewall programme.** This keeps potential hackers out of your computer. You'll be surprised how often you will get hacked if you don't have one installed!
- **Install an Anti-Spyware Programme.** Keep your anti-spyware definitions up-to-date (check daily) and do a full system scan once a week.
- **Filtering software** may be appropriate to block unsuitable material. Keep filtering definitions up-to-date. It could be appropriate to install accountability software which will send the web sites you look at to an accountability partner.
- **Windows Update.** If you use windows, make sure that you check your version of windows is up-to-date with security patches that Microsoft release on the windows update website. In particular if you have Windows XP- make sure you get the SP2 update.
- **Internet Browser Issues.** It might be advisable to use an alternative browser to Microsoft Internet Explorer which apparently has a few security glitches. The new browser, Fire-Fox from Mozilla is free is fast becoming a close runner to Internet Explorer. Find it on [www.getfirefox.com](http://www.getfirefox.com)

- **Avoid Peer-to-Peer programmes** if possible which allow the transfer of illegal material.

If you have to use them, use with extreme care.

- **NEVER give out personal details** (address, phone numbers, photos of self). It may be inadvisable to give out email address, especially over chat rooms.

- **Use chat rooms with care.** Always remember the person you or your child is chatting with may not be all they say they are. Only use safe and monitored chat rooms. Monitor chatting on chat programmes such as MSN, Yahoo Messenger and AOL messenger and keep chatting times not too long.

- **Access at school.** Find out if the school your child attends has a policy on accessing pornography.

- **Talk about it.** Take time to talk to your child about sex, sexual relationships and pornography.

- **Internet Pornography Addiction.** Do you or someone you know have a problem with

internet pornography? The Care site has some very good advice on it - [www.care.org.uk/anon/advice/](http://www.care.org.uk/anon/advice/)

- Encourage your children to act NetSmart on the Internet - see [www.kidsmart.org.uk](http://www.kidsmart.org.uk)

- **New Technology.** Christians were rather slow to react to the internet. We must not make the same mistake with mobile technology especially the new 3G phones. Keep up-to-date with what is happening.

**Good and Bad.** Remember although the Internet is capable of much evil and has some worrying material on it- it is also capable of much good as long as we all act responsibly.

## Important Software:

The following are examples of the software you should have installed on your computer to stop it being vulnerable. They are here just as a guide:

### ANTI-SPYWARE SOFTWARE

- Spysweeper – Webroot Software – [www.webroot.com/products/spysweeper/](http://www.webroot.com/products/spysweeper/)
  - Spybot Search & Destroy - [www.safer-networking.org](http://www.safer-networking.org)
  - Ad-aware - [www.lavasoft.com/software/adaware/](http://www.lavasoft.com/software/adaware/)
- Mircrosoft Windows Antispyware (formally Giant Antispyware) – [www.giantcompany.com](http://www.giantcompany.com)

### ANTI-VIRUS SOFTWARE

- Norton Anti-Virus - [www.symantec.com/region/reg\\_eu/product/nis\\_index.html](http://www.symantec.com/region/reg_eu/product/nis_index.html) - McAfee - [www.mcafee.com/uk/](http://www.mcafee.com/uk/)

### FIREWALLS

- Norton Internet Security - [www.symantec.com/region/reg\\_eu/product/nis\\_index.html](http://www.symantec.com/region/reg_eu/product/nis_index.html) (Includes a Firewall and Antivirus)
- Zone Alarm - [www.zonealarm.com/](http://www.zonealarm.com/)

### FILTERING SOFTWARE/SOLUTIONS

There is no easy solution for filtering out inappropriate material. There a 3 ways that may be appropriate:

Filtering/Blocking software solution. There are so many solutions out there. Visit [www.filterreview.com](http://www.filterreview.com) or [www.internetfilterreview.com](http://www.internetfilterreview.com) for the latest. Popular ones are Content Protect, CyberSitter and NetNanny

Filtered Internet Service Provider Solution – a more failsafe option which filters internet content before it actually reaches your computer. This gives you less control, but the advantage it that it is less easy to override. Zen Internet uses a system called N2H2 which filters sites in three different severities. - [http://home.zen.co.uk/products/body\\_products.asp?ProdId=14899](http://home.zen.co.uk/products/body_products.asp?ProdId=14899)

Accountability Software. This does not filter or block any of the internet. It can be used in

conjunction with the above two solutions. You chose an accountability partner who is sent a list of your sites (or with some systems inappropriate sites only) that you have visited either weekly, fortnightly or monthly. The thought is that if you knew someone was going to see the sites you were about to view, would you view them? The two main ones are Covenant Eyes at [www.cvnt.net](http://www.cvnt.net) (go through [www.care.org.uk/anon](http://www.care.org.uk/anon) for a special offer) or X3watch from xxxchurch which is free.

## Useful Websites:

<a href="http://www.filterreview.com">www.filterreview.com</a>	Reviews and information on filtering software, with reviews by the public. A Christian-run website.
<a href="http://www.internetfilterreview.com/">www.internetfilterreview.com/</a>	Reviews and information on internet filtering software and information and statistics on the pornography industry.
<a href="http://www.anti-spywarereview.toptenreviews.com/software">www.anti-spywarereview.toptenreviews.com/software</a>	Reviews and information on antispyware
<a href="http://www.childnet-int.org/safer">www.childnet-int.org/safer</a>	A top award winning site making the internet a safer place for children.
<a href="http://www.care.org.uk/anon/">www.care.org.uk/anon/</a>	Care's website on internet misuse. Extremely helpful site- highly recommended.
<a href="http://www.exxit.org">www.exxit.org</a>	An American website with daily bible studies for those who are addicted to internet pornography.
<a href="http://www.xxxchurch.com/">www.xxxchurch.com/</a>	An American Christian site for discussing pornography on the internet.
<a href="http://www.kidsmart.org.uk">www.kidsmart.org.uk</a>	Is your Kid, Kid smart?
<a href="http://www.chatdanger.com">www.chatdanger.com</a>	Discussing the dangers of chatting online.
<a href="http://www.parentcentre.gov.uk/">www.parentcentre.gov.uk/</a>	The Department of Education and Skills online recourse for parents where you will find information on the latest internet safety issues.
<a href="http://www.thinkuknow.co.uk">www.thinkuknow.co.uk</a>	A website created by the Home Office designed to keep your child safe on the internet.
<a href="http://www.faxyourmp.co.uk">www.faxyourmp.co.uk</a>	If you feel your MP should be getting more involved in internet safety- this website lets you fax your MP for free.

# Glossary:

Information taken from [www.internetfilterreview.com](http://www.internetfilterreview.com) and [www.webopedia.com](http://www.webopedia.com)

- Adware** Adware is considered a legitimate alternative offered to consumers who do not wish to pay for software. Programs, games or utilities can be designed and distributed as freeware. Sometimes freeware blocks features and functions of the software until you pay to register it. Today we have a growing number of software developers who offer their goods as "sponsored" freeware until you pay to register. Generally most or all features of the freeware are enabled but you will be viewing sponsored advertisements while the software is being used. The advertisements usually run in a small section of the software interface or as a pop-up ad box on your desktop. When you stop running the software, the ads should disappear. This allows consumers to try the software before they buy and you always have the option of disabling the ads by purchasing a registration key. In many cases, adware is a legitimate revenue source for companies who offer their software free to users. A perfect example of this would be the popular e-mail program, Eudora. You can choose to purchase Eudora or run the software in sponsored mode. In sponsored mode Eudora will display an ad window in the program and up to three sponsored toolbar links. Eudora adware is not malicious; it reportedly doesn't track your habits or provide information about you to a third party. This type of adware is simply serving up random paid ads within the program. When you quit the program the ads will stop running on your system.
- Advertising** Advertising has become a huge business for websites. Most 'free' sites use advertising as their many revenue. Most legitimate and responsible businesses will not sell advertising space to pornographers. But unfortunately, that hasn't stopped a large number of pornindustry leaders, who have created fake system error messages, message alert boxes, or false forms that dupe you into thinking you have to click on the OK button or enter certain information, when in reality, you are clicking on the link to open the pornographer's front door.
- ASL** Chat room speak for "What is your Age, Sex and Location?"
- Attachment** A file attached to an email message. Before opening it check who it is from and what kind of file it is. Also make sure your virus detector has scanned the incoming mail and that it is not a threat. If the file is an 'EXE' file be careful as this is an executable file and could do harm to your computer. Image files (such as .JPG, .GIF and .BMP) are generally safe but could be of offensive content.

**Broadband** A faster connection to the internet than the dial-up method. It can be obtained through cable or through the telephone line (sometimes called ADSL) Usually the speeds are from 10X the speed of a conventional modem- 500, 1000 or 2000Mbps (Megabits per second) Usually the speed at which you can upload material (ie send from your computer) is at a lower rate (usually 256Mbps) Usually broadband is an always on connection, meaning that your computer is geminately connected to the internet. This makes it all the more important to have a good firewall software and anti-virus and antispysware programmes installed. Some providers put a 'cap' on how much you can use their connection.

**Browser** This is a piece of software which lets you browse in the internet. Popular browsers include, Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera and for the Mac platform, Safari.

**Cookies** A message given to a Web browser by a Web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly prepare customized Web pages for them. When you enter a Web site using cookies, you may be asked to fill out a form providing such information as your name and interests. This information is packaged into a cookie and sent to your Web browser which stores it for later use. The next time you go to the same Web site, your browser will send the cookie to the Web server. The server can use this information to present you with custom Web pages. So, for example, instead of seeing just a generic welcome page you might see a welcome page with your name on it. Cookies do not act maliciously on computer systems. They are merely text files that can be deleted at any time - they are not plug ins nor are they programs. Cookies cannot be used to spread viruses and they cannot access your hard drive. This does not mean that cookies are not relevant to a user's privacy and anonymity on the Internet. Cookies cannot read your hard drive to find out information about you; however, any personal information that you give to a Web site, including credit card information, will most likely be stored in a cookie unless you have turned off the cookie feature in your browser. In only this way are cookies a threat to privacy. The cookie will only contain information that you freely provide to a Web site.

**Cyber-Squatting** Many pornographers legally purchase domain names for legitimate topics in a switch-up referred to as "cyber squatting." As an example, someone expecting to find information about the President of the United States might type in a web address that they think might be to do with the White house, and be very confused (or outraged) at finding explicit porn on the site. There are many examples of this on the internet. The best way is to double check the domain name first, or check it out on a search engine.

**Dialers**

A more recent trick that unscrupulous porn dealers are experimenting with involves using downloads to covertly install expensive diallers on an unsuspecting user's PC that will automatically dial for-pay (and frequently long distance) porn sites, charging exorbitant fees every time they do so. Obviously if you don't use a dial-up modem in your computer connected to your phone line then you will not be at risk- this does not apply to broadband users. Always check the number you are dialling in your internet settings, and to make sure you can always block premium rate numbers by phoning up BT or your phone operator (for a fee).

**Dial-up**

A way of connecting to the internet using a modem and a phone line. Usually the computer connects to an ISP by dialing a number. This can be a free number while you pay the ISP a subscription or you pay as you go by paying for the internet usage by using a low-call 0845 number. It is a good idea to check that the number is still the same, and in particular that it is not a premium rate (09...) number or an international number (one that has 00 before it)

**Doorway Scams**

Very similar to porn-napping and cyber-squatting is a technique known as a "doorway scam", which makes use of one of the most common tools on the Internet-the search engine. Experienced pornographers have figured out that by carefully constructing their websites, and designing them around non-pornographic themes, they gain new opportunities to deceive unsuspecting surfers. Web page content is created to place the website high on a search engine's results, and after clicking on it, the user is redirected to a porn site. Another version of the doorway scam is to create a porn site around a common, non-pornographic theme. So rather than redirect the Internet user to another unrelated-but pornographic-site, this technique actually creates pornographic web pages related to their title.

**Email**

Email is a way of life for many people and a great way of communication. Depending on which email service you use, you may have already been flooded with unwanted and unsolicited pornography. Hotmail and AOL email accounts have been favourite targets for porn peddlers' aggressive marketing strategies. You can actually become entangled in an inappropriate or adult website before you even know that the email you received has anything to do with pornography. And don't make the mistake of thinking that simply following the unsubscribe instructions will end your email problems. By responding, you are telling the pornographer not only that your email account is valid, but also that you read his unsolicited message. Most likely he will continue to use and sell your address. Some emails contain high-tech multimedia video attachments that begin playing the instant you click on them, whether inadvertently or not. New email technology even allows a video to be sent as part of the email rather than an attachment, with the result being that the video begins playing on

your screen before you even realize what happened. Emails are infamous for transmitting worms or viruses. As an example, the worm known as "Homepage" can modify your browser's user default home page, so that every time you click on your browser, you are automatically sent to a porn website. (see also email spoofing, Spam and phishing)

- File extension** In Windows and other operating systems, each filename has an extension which determines what kind of file it is. The 3 letter extension is followed by a dot. For example a JPEG image has the extension 'JPG', a Word document has the extension 'DOC' and a pdf file has the extension '.PDF' If the file extension is 'EXE' this is an executable file and caution should be used before opening it unless you know that it is safe.
- FTP** File Transfer Protocol.
- History** The list of websites viewed over a period of time. Most browsers have a history folder which will hold the web addresses viewed over a period of time. The history can be wiped clean, but it is a good idea to keep in place so that accountability is in place.
- ICQ** An easy-to-use online instant messaging program developed by Mirabilis LTD. Pronounced as separate letters, so that it sounds like "ISeek-You," ICQ is similar to America OnLine's popular Buddy List and Instant Messenger programs. It is used as a conferencing tool by individuals on the Net to chat, e-mail, perform file transfers, play computer games, and more. Once you have downloaded and installed ICQ onto your PC, you can create a list of friends, family, business associates, etc. (who also have ICQ on their PC's). ICQ uses this list to find your friends for you, and notifies you once they have signed onto the Net. You can then send messages, chat in real time, play games, etc. Also see Instant Messaging
- Instant Messaging (IM)** A type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication. Typically, the instant messaging system alerts you whenever somebody on your private list is online. You can then initiate a chat session with that particular individual. Examples of such programmes are MSN Messenger, AOL Messenger and Yahoo! Messenger.
- IRC** Short for Internet Relay Chat, a chat system developed by Jarkko Oikarinen in Finland in the late 1980s. IRC has become very popular as more people get connected to the Internet because it enables people connected anywhere on the Internet to join in live discussions. Unlike older chat systems, IRC is not limited to just two participants. To join an IRC discussion, you need an IRC

client and Internet access. The IRC client is a program that runs on your computer and sends and receives messages to and from an IRC server. The IRC server, in turn, is responsible for making sure that all messages are broadcast to everyone participating in a discussion. There can be many discussions going on at once; each one is assigned a unique channel. Like all chat systems this can be open to abuse and the transfer of inappropriate files can be transmitted over IRC.

- ISP** Internet Service Provider. The company that enables you to connect to the internet through their system. Most companies have different services and different fees. Some offer a dial-up service which enables you to connect to the service via your normal phone line or ADSL (Broadband) or SDSL which are always-on connections.
- Looping** A trick pornographic pages use to put your internet browser in a never-ending loop with new porn pages appearing one after each other. If you close a window down, another appears, and so on...
- Misspelt Domains** A trick that when you misspell a domain name, you are taken to a pornographic site. The pornographer has bought-up similar domain names to popular sites and calculated popular misspellings to lure you to their sites. (also see cyber-squatting, doorway scams and porn-napping)
- MMS** Multi-media Messaging Service. The next generation of SMS which enables the sending of messages between mobile phones or to email. These messages can contain text, images, audio clips or even videos.
- Modem** A component in the computer or externally that lets your computer connect to the world wide web through telephone lines.
- Mousetrapping** Depending on the browser you use, some sites will alter the use of the Back button or the Close function, preventing you from exiting the pornographic website. This practice is sometimes known as "mousetrapping," because it renders your mouse useless. Regardless of what you do, you have lost control of your browser, similar to being caught in a mousetrap. Make sure you have the latest version of your internet browser, and if possible use a more secure one such as Mozilla Firefox.
- Newsgroups** Newsgroups, communities, forums and clubs are discussion groups on the internet. They do not allow users to communicate live, but to post messages on the site on a particular site. The majority of these sites are fine, but they are open to abuse by users posting inappropriate images and words. Filtering software and/or browsing them together may help in this situation.
- P2P** Person to Person. Chatting privately to someone in a chat room (See Whispering)

## **Peer to Peer**

When accessing the Internet, you access websites through an application known as a browser. Common browser applications are Internet Explorer, Netscape, and Mozilla. Peer-to-Peer networking, known as P2P, is similar in concept to a browser. It is an application that runs on your PC and allows sharing of files. Napster used to be one of the most popular peer-to-peer application programs, sharing MP3 music files, until it was shut down by the U.S. Justice Department. Today, favorites like Limewire, Gnutella, Morpheus, Bearshare, and Kazaa share center stage. P2P programmes include- Kazaa, LimeWire, Gnucleus, Gnutella, JungleMonkey, Morpheus, Bodtella, iMesh, FileNavigator, MojoNation, MyNapster, BearShare, DirectConnect, eDonkey2000, Konspire, Gnutella, Mactella, Freenet, Newtella, Filetopia, Aimster, WinMX, Hotline and Flycode. The concept of peerto-peer networking is to allow computers to communicate directly with each other, rather than through a central server like a website. Once you have a peer-to-peer application installed, you can allow anyone in the world to copy files from your home PC. This can be a single file, an entire directory, or your entire hard-drive. If care is not exercised, your entire hard-drive, including any confidential documents, may be wide-open to anyone in the world. Peer to Peer should really be avoided at all costs for many reasons. According to recent statistics more than 35% of downloaded material is pornographic. There is a high risk of downloading viruses and most P2P programmes have spyware as part of the installation process.

## **Phishing**

This is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay's site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.

- Porn-Napping** A trick pornographers play by registering a domain name that a company has forgotten to renew and then forwarding it to a porn site. Due to a clerical error, the accounting firm of Ernst and Young let the registration lapse on their children's money management site, moneyopolis.org. Quickly purchased by a pornographer, all visitors to the site ended up at a porn site, until Ernst and Young repurchased moneyopolis.
- Profile** Some chat rooms, dating services, forums and other websites let users create their own personal profile which others can see. This can include age, location, sex, photo(s) and likes/dislikes. Public profiles have the capability of being exploited and so should be avoided if possible. If one is needed then never include personal details such as address, email address, phone number, mobile phone and avoid posting your photo on it.
- SMS** Short Messaging Service. Sending short text messages by mobile phones. SMS messages can now be sent by landline phones and from the internet. If sent from the internet they are usually anonymous.
- SPAM** Electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited e-mail. However, if a long lost brother finds your e-mail address and sends you a message, this could hardly be called spam, even though it's unsolicited. Real spam is generally e-mail advertising for some product sent to a mailing list or newsgroup. In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail. However, some online services have instituted policies to prevent spammers from spamming their subscribers
- Spyware** (See adware first) Unfortunately, some freeware applications which contain adware do track your surfing habits in order to serve ads related to you. When the adware becomes intrusive like this, then we move it in the spyware category and it then becomes something you should avoid for privacy and security reasons. Due to its invasive nature, spyware has really given adware a bad name as many people do not know the differences between the two, or use the terms interchangeably. Spyware is considered a malicious program and is similar to a Trojan Horse in that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware type program or application. Once installed, the spyware

monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers. Because spyware exists as independent executable programs, they have the capability to monitor your keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, while consistently relaying this information back to the spyware author who will either use it for advertising and marketing purposes or sell the information to another party. Licensing agreements that accompany software downloads sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements are not always be read completely by users because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers.

**Startup file**

It is possible to have your computer altered with the consequences

**Alteration**

not showing up immediately. In one technique, pornographers place a program into your startup directory that sends you to a porn site or displays a pornographic image whenever you boot up. Always install a antivirus and anti-spyware software.

**Temporary (or Internet Cache)**

When browsing the internet your browser normally stores the web pages and images on your computer so that it does not have to keep downloading the material again from the web server. This speeds up your browsing. It is good to regularly wipe your files which can be done on the internet options as having too many of these files can slow the computer down. If the computer has been used to view pornography or other offensive material be aware that these might be stored in the temporary internet files.

**Trojan Horses**

With literally millions of free downloads readily available for the taking, you can get everything from screen savers, background images, and fancy desktop icons to serious gaming applications and highly advanced software programs. But be warned-that very appealing new screen saver may actually be a Trojan horse, that when clicked upon, kicks off a program that opens up into a world of pornography, and also possibly wreaking havoc in your system. Trojan horses and other malicious invaders can be placed on your machine even when downloading something as simple as a pretty calendar or a children's puzzle.

**URL**

Stands for Uniform Resource Locator. This is the address for the webpage which is then translated into a series of numbers called an IP address. URL's are used as they are easier to remember than IP numbers.

<b>Viruses</b>	A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. Since 1987, when a virus infected ARPANET, a large network used by the US Defence Department and many universities, many antivirus programs have become available. These programs periodically check your computer system for the best-known types of viruses. Some people distinguish between general viruses and worms. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.
<b>WAP</b>	Wireless Application Protocol. A technology used my mobile phone devices to browse the internet sites written in a compatible format
<b>Webcams</b>	Webcams are special cameras that are set up to record and broadcast full-motion video and sound over the Internet. Originally, this technology was used to implement inexpensive teleconferencing capabilities for businesses. Now it is one of the favorite technologies used on pornographic websites-real-time viewing of sexual activities. This concept, popularized by the movie, The Truman Show, allows for 24-hour uncensored and uncut online viewing. Webcams can be installed in a private place which can allow the visitor to participate in a voyeuristic journey into an individual's most intimate experiences. If you have a web cam make sure it is unplugged from your PC when not being used.
<b>Whispering</b>	A way of sending a private message to an individual in a chat room. This is like having a conversation with a stranger. Be careful! It is better to stay in the public area of the chat room unless it is someone you actually know.
<b>Worm</b>	A program that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down. Also see Virus.

Printed by the Diocese of Southwell & Nottingham  
Dunham House, 8 Westgate, Southwell, NG25 0JL Tel. 01636 817220  
email: [mail@southwell.anglican.org](mailto:mail@southwell.anglican.org)

**website: [www.southwell.anglican.org](http://www.southwell.anglican.org)**