

# PROBLEMS WITH EMAIL

## SPAM

Spam is unsolicited commercial messaging by email. Think of spam as the electronic version of the mail that drops through your letterbox from estate agents, pizza companies, taxi firms etc – in other words it is unwanted mail trying to sell you things you don't want. Spam advertises similar products or it could be a hoax trying to mislead you. Mail that comes via your letterbox is controlled by government legislation but email is not. However, this may change in the future and the law may be toughened regarding spam.

Spam is so common and growing so fast because it is very profitable. Paper-based mail costs money to print and deliver and most people put junk mail straight into the bin. In cyberspace, spam is very cheap. The cost of sending a million messages is not much more than the cost of sending one email. Therefore a small response rate can provide large profits. It is hard to get accurate figures but we know that spam can be very profitable indeed.

There are companies that can block spam block spam before it reaches your inbox, and there is software that you can stop spam completely. However, you must keep your spam filter up-to-date with downloads from the supplier. You must also train the software to recognise messages which are spam and which are not spam other wise it will block the wrong messages or let some spam through. Also, you must remember that spammers are quick learners and they keep changing the way they try to get spam messages past blocking software.

Some spammers are very clever and to get a spam message past a spam filter they use very clever tricks. For example, a word like 'Viagra' in the subject line will usually be filtered out as spam. Spammers therefore change the way it appears to confuse the anti-spam software and insert spaces such as 'V i a g r a' or even colons such as 'V:i:a:g:r:a'. You can see the word but the spam filter cannot unless your anti-spam filter has been trained to look out for such tricks.

To try to stop the amount of spam you receive you should:

- Set rules to filter unwanted messages as they arrive.
- Ask your ISP to provide a spam filter. If they cannot, change to one that does.
- Be careful about giving out your e-mail address.

- Never publish your e-mail address on a web page. If necessary, set up a different email address which you don't mind giving out
- Use a different e-mail address on websites, chat rooms, forums or newsgroups. You can get a free webmail address from services such as Yahoo or Hotmail.
- Do not use the 'unsubscribe' link or button on unrequested emails. This lets the sender know that this is a legitimate address and they will keep sending spam to this address.
- Many spammers use computer-generated guesses to spam email addresses and they don't know for sure if the address is real or not. By clicking on the unsubscribe link, you are telling the spammer that your address is real. This address will then be sold to other people who wish to spam you. The only time you should click on an 'unsubscribe' link is if the email is from a reputable company known to you.

## **E-MAIL SCAMS**

A scam tries to make you send money to the sender of the message. The message will use many different methods or encourage you to read it.

Some scams involve 'offering money for no work' - e.g. a subject line saying 'You have won the lottery'. See **HANDOUT 5**

The most well-known money scam is the Nigerian scam which originated in Nigeria and is called the '419'. The 419 makes you an offer which is not true to try to get you to part with your money. See **HANDOUTS 6 and 7**

This scam tries to get the victim to provide details of his or her bank account. The criminals then use the information to get into the account and transfer money from it.

Scams rely on people wanting to 'get rich quick'. These scams imply they wish to transfer large sums of money into your bank account which is why they ask for your bank account details. They often use images to fool the anti-spam filters and many people fall for these scams each day.

## **E-MAIL HOAXES**

Hoaxes are messages that seem to warn you about dangers to get you to take action. They may ask you to delete something useful on your hard drive. Sometimes hoaxes tell the user to delete an important file that the computer

needs. For example, an email may say that a file called jdbgmgr.exe is a virus and it will tell you how to delete it. However, jdbgmgr.exe is not a virus. This hoax is called the 'Teddy Bear' virus hoax and is very common. Many people have deleted 'jdbgmgr.exe' which is an important Windows file. This hoax has had lots of success because the file 'jdbgmgr.exe' has a little teddy bear icon which looks out of place for a Windows file. See **HANDOUT 8**

Other common hoaxes warn about viruses that 'no antivirus company can detect' which is not true. Hoaxes try to make people pass on incorrect information to others. It may seem hard to believe how gullible people can be to fall for these hoaxes. However, they are often very convincing and play on people's fears.

To protect yourself from hoaxes you should follow the rules below:

1. Do not automatically accept a message that comes from a person who claims to be an IT expert.
2. Be wary of messages that ask you to forward the email to all your friends.
3. Microsoft does not send out unsolicited warnings.
4. Be wary of emails claiming that no antivirus software can detect them. This is almost certainly untrue.
5. If you are really unsure about a message, check with an adult or a teacher.

## **PHISHING**

Phishing (pronounced 'fishing') is a scam that usually comes in e-mail and tries to get passwords, credit card details or other information. The e-mail has a link or button that the user clicks. They are then taken to a website which looks like a bank website but which is actually a fake site. The victim is asked to type in their account details, password and user ID and they are captured by the site and used to take money from the account. Many people fall for phishing scams. See **HANDOUT 9**. Remember, banks do not ask for your bank account details or passwords by phone or the Internet.

## HANDOUT 8

SORRY - but as you're on my address list this virus has probably forwarded itself on to you.

It is easily removed if you don't open the file (jdbgmgr.exe) It has a teddy bear icon and is not detectable by norton or mcafee.

First go to Start then the find or search option. In the files or folders option type jdbgmgr.exe. Search C drive and tick the 'include subfolders' and any other drives you may have. Click 'find now' - the virus has a grey teddy icon. DO NOT OPEN IT. Go to edit (on the menu bar) and 'select all'. Now go to file (on the menu bar) and DELETE. This will send it to the recycle bin so then go and delete or empty it there as well.

If you find the virus (as I did!) you must contact everyone in your address book and send them these instructions. ASAP.



Here is the teddy bear icon for jdbgmgr.exe