BBC Worldwide

4. TROJANS, WORMS AND HOAXES

Trojans*: In its war against Troy, the Greeks built a large wooden horse and hid soldiers inside it. When the people of Troy saw the horse, they assumed that the Greeks had gone home and left them a trophy. They dragged the horse into the city. At night the Greek soldiers climbed out and slaughtered the Trojans. 'Beware of Greeks bearing gifts!'*

1. For a computer user, an innocent looking picture, music file or movie mpeg may not be all it seems. Explain, using the example of the wooden horse of Troy, what a 'Trojan' means to a computer user, and how it may carry not soldiers, but a damaging virus. How can you protect against 'Trojans'?

Always keep your software up to date. This goes doubly true for important programs like your operating system and browser. Hackers exploit known security holes in these types of programs that can help the Trojan do its work, and even if the vendor patches the holes, it won't do you any good unless you maintain the latest version of your software. To keep your Internet connection as secure as possible, always keep a firewall up. Both software and hardware firewalls are excellent at controlling malicious Internet traffic, and can often stop Trojans from downloading to your computer in the first place.

Worms: *Computer worms, unlike viruses, replicate themselves and then move through the internet, infecting other computers. They have their own self-contained program, unlike a virus which attaches itself to an existing program. The Sobig Worm was one such malicious program that infected millions of computers in August 2003. Arriving in emails with subject lines such as Re: Thank You!, Re: Details, and Re: Your Application, it carried its own email sending program. The attachment it contained ended with the suffix .pif*

2. What is the difference between a virus and a worm? Why did 'Sobig' choose those titles for the subject lines of the emails? How could you know by looking at attachment name that all was not well?

Computer worms, unlike viruses, replicate themselves and then move through the internet, infecting other computers. They have their own self-contained program, unlike a virus which attaches itself to an existing program. The **Sobig** chose those titles because it got people interested as to what was in the email, instead of just saying "WELLDONE!!!!!!! YOU HAVE WON AN IPHONE!!!!!". "Details;" makes it sound much more believable. You would know by seeing the suffix that what you were downloading was not intended for, it would've been a word file, .doc.

jdbgmgr.exe

Hoaxes: *Some viruses are, in fact, elaborate hoaxes. The so-called "Teddy Bear Virus" arrived by email and informed the recipient that their computer may be infected with a virus. It advised the user to check a location on their hard drive. If they found the file jdbgmgr.exe, and the icon of a teddy bear, they were advised to delete it immediately. The email also asked them to send the message to all of their friends.*

3. Does the above message sound genuine? What is it about the file name and picture that makes you think that it might be a genuine virus?

This message does not sound genuine as you will hardly ever get an email to say you have a virus and the teddy bear is not exactly business like so it is probably fake especially with a random file name.

4. This message was a hoax. Deleting the file could have had serious consequences for your computer. How would you know to ignore this advice, or indeed the advice from any hoax email? Use examples.

Make sure it is from a valid source, make sure the valid source is in your contact book so you know if it is a hoax or genuine.