

IT Survival



Item Code FS295209 September 2005 Edition no 1

0845 300 1818

I'm fine. Why should I worry?

The Scout Association's websites and all the Member users form a massive virtual organisation with a huge IT infrastructure – certainly bigger than any company in the UK. However, unlike most IT infrastructures there is no central form of administrative control or security management, and much of the onus is on each end user to ensure they practise 'safe surfing'. As individuals we may feel that being lax with our IT security is acceptable because we consider that nothing 'bad' is likely to happen to us and, even if it does, we will be the only ones affected. Unhappily, where the Internet is concerned, this is just not true. The Scout Association's websites are regularly visited by thousands of users; a virus attack can easily generate over 1000 times the normal amount of email, clogging up our email systems and making it impossible to communicate. Almost all of these virus-infected emails are transmitted, albeit unwittingly, from Members' PCs. With Internet technologies becoming more and more central to The Scout Association's communications, this is a real and growing problem.

It looks too difficult to me!

The purpose of this Fact Sheet is to explain the requirements for 'safe surfing'. It focuses on Windows PC technology, but the general

principles and practices are applicable to any system. Do not get paranoid about the risks inherent in going online; it is certainly not the purpose of this document to scare users away from the Internet. However, it is important to understand both why you need to be secure, and the implications if you do not take some simple precautions. This is not an exhaustive technical paper, but it does go into some detail to enable you to comprehend the reality of Internet use.

Online nasties. Be warned! Be aware!

Bots, Spyware, Diallers, Key Loggers, Viruses, Worms, Trojan Horses..

Yes, there's a whole regiment of nasties loose in the online world. There are technical differences between the types of programs, but what they have in common is that they do unexpected and unwanted things on your computer, and also spread themselves to others. A common collective term is 'malware'.

Malware can spread in either of three distinct ways, or as a combination:

1. Talking to other machines across a network, and hopping onto them to run, usually exploiting bugs in software

2. Transmission via email
3. Fooling the user into performing an activity (i.e. running a program or entering sensitive data into a website)

Social engineering

'Social engineering', in the IT context (also called 'phishing'), is a term used to describe the tricking of users into giving out sensitive or personal information. An example of this might be an email purporting to come from your bank, or perhaps an online auction site, asking you to go to a specific website and confirm your personal details. It is relatively easy for criminals or tricksters to duplicate the appearance of a genuine website, so, if you follow the suggested link and enter your details, you will almost certainly be putting yourself at risk to online identity fraud. Another example might be an official looking email purporting to be from a well-known software company and advising you to install a supplied patch; follow these instructions, and you will almost certainly be helping to spread a virus.

A reputable organisation will NEVER send you an email requesting personal details; a reputable IT company will NEVER send out software patches by email. If you have the slightest doubt concerning an email, contact the alleged sender either by telephone or via the enquiries email link on their website (and enter the address into the web browser yourself, do not just click on the email link).

There is no technology or anti-virus software that can directly protect you from social engineering – common sense is your best defence. Viewing something on a screen, on a website, or in an email does not make it official; treat anything

uninvited or unexpected with the utmost suspicion.

Hoax emails

A form of social engineering, these emails usually contain emotive content intended to make you react in a particular way. This could be as relatively innocuous as making you smile, or raising your curiosity. Other less innocent examples include promises of prizes for forwarding the emails, or security warnings that tell you to perform certain actions on your machine. Often, they invoke the names of well-known companies or organisations to lend credibility and realism. Again, be aware that just because you see it on screen does not make it real or proven. Any email urging you to forward it on to everyone you know, chain-letter style, is almost certainly a hoax; you have no control over the ultimate distribution – and it has your name permanently attached to it! Do not respond to hoax emails, they are almost as much of an Internet evil as any of the nastier forms of malware. If you do know the sender, then perhaps a polite, personal approach is an appropriate course of action.

Spam

Spam is the term used to describe unwanted and mostly bulk-sent email - usually claiming to offer dubious services. Because spam can be sent so cheaply, and innocent PCs are often hijacked as servers to do so, it is easy to distribute millions of emails on a daily basis. Unfortunately, spam is a fact of Internet life at present. There are products that can identify and delete spam with reasonable levels of effectiveness, but these same products may well trap valid emails (false positives), and in any case spammers are active in working out how

to get round these filters. There are, however, a few steps you can take to minimise spam.

Your email client should be set up so that any emails you receive which contain graphics are not allowed to show those graphics; showing them will guarantee that you receive more spam. This is because the email has a unique reference to your email address, and in displaying the graphic the email client will contact a remote website with this unique reference, thus confirming that your email address is live and is being read. For a similar reason never respond to the invitation to remove your address from further spam emailing. Even assuming the reply address is valid all you are doing is, again, confirming your live email address.

Complaints about spam to the apparent sender or company are usually pointless; the details shown will almost certainly be spoofed. You (and thousands of others!) will simply be contacting the wrong people.

Diallers

This particularly nasty type of malware will disconnect the connection to your Internet Service Provider (ISP), then reconfigure the dial up number to be a premium line, or an expensive telephone line abroad. Typically they can be found in the seedier regions of the Internet, and often use social engineering to install themselves. A web page may prompt you to click on 'Yes' in the 'next' box to gain access to the content of the site – the next step is a prompt asking you to agree terms and conditions, and to the installation of software. Or the software may be sent to you in an email; either way, operating system vulnerabilities can be exploited on installation. Many anti-virus (AV) programs will detect diallers,

and prevention is definitely better than cure; once a dialler is installed by design it is difficult to remove. You should consider requesting your telephone company to bar premium and international numbers if you do not normally use them. Telephone companies will not refund the cost of the calls from your number as they are valid, and often there is nothing illegal because the end user has agreed to the original terms and conditions.

Your PC's dial up modem should be disconnected to prevent its illegal use by diallers. If in fact you connect to the Internet by means of a broadband connection - there is no known way to subvert a broadband connection (yet).

Spyware, Bots and Zombies

Similar in design to diallers, these programs – once installed – allow a third party to use your computer for whatever purpose they see fit. Without your knowledge your computer will be turned into a so-called 'bot' or 'zombie'. It is most likely that hundreds of thousands of PCs across the Internet have bots installed, waiting for the bot writer to issue instructions. These may involve participating in a co-ordinated attack against online businesses in order to extort money from them (known as a Distributed Denial of Service (DDoS) attack), or to send bulk unsolicited email (spam); to log your keystrokes (with a view to stealing confidential passwords), or to record which websites you visit. Spyware software can be incredibly sophisticated, and you are unlikely to be aware of its existence.

There are certain indicators to watch for which may reveal the presence of an unwelcome guest. You should run your security software at once if, despite normal good housekeeping, the PC

suffers considerable degradation in performance, or suffers repeated crashes; if advertising pop-ups appear even when you are offline; or if your browser's appearance has changed. If the changes will not go away, then get help.

Protecting yourself – and others

So far, you may feel that everything is stacked against you when you venture online. Yes, it is serious and we cannot ignore the reality of these daily occurrences. Knowing the problem is half the battle, the other half is the use of some very good software packages (many of them free or low cost) to safeguard your PC. You must have them installed and working. (See Annex A).

Anti-Virus

It is essential that you have up-to-date anti-virus (AV) software running on your machine. This will not guarantee total security on its own, but is a good line of defence. These AV programs are reactive in that they all depend on knowing about and protecting against specific threats; most packages also offer 'heuristic' detection (guarding against what it thinks looks like a virus). Most AV suppliers issue upgrades to their virus data files on a weekly basis as a minimum, and even more frequently if a serious, widespread, virus attack takes place. You must remember to manually upgrade the program, but, fortunately, many packages will have an 'automatic update' function to do this for you.

If you receive an email and your virus scanner alerts you to the fact that it's carrying a virus as cargo, do not rush off and blame the sender. It is more than likely that the virus will have manipulated the 'From' header, thus the apparent sender of the virus is in fact quite different from the person who actually sent it. The ensuing

communication chain of 'you sent me a virus' - 'no I didn't' can actually cause more problems than the original virus.

Anti-Spyware

These programs, although similar to AV programs, actually detect spyware and related nasties rather than viruses. They are an important defence. Their use requires a little more thought and care than anti-virus software, because sometimes they will detect as 'spyware' something that you actually want to retain. For example, some software is available free on the condition you allow it to display adverts, and anti-spyware software may detect this advertising and offer to remove it - crippling the free software. However, the more sophisticated anti-spyware software has a database of known spyware which is likely to be damaging, and is thus able to offer advice as to what it has found and the nature of it, as well as providing a 'roll back' facility should things go wrong. Whilst AV programs are normally always working in the background, anti-spyware programs usually need to be run manually. You should do so regularly, at least once a week if you spend a considerable amount of time online, and update the program whenever so prompted.

Personal firewalls

By their nature, computers are fairly trusting, and will let any other computer talk to them. In the modern world, however, this is no longer desirable. A good personal firewall will stop unwanted communication to your machine, and in so doing will stop a lot of the malware in its tracks. Most personal firewalls also stop installed software from 'calling home' without your permission. Many packages will require training

after installation in order to understand what you want to allow to talk to the Internet. They will do this by prompting you for answers as to the use of your system, but once trained they will work unobtrusively. Personal firewalls can block a lot of malware from operating, even programs that anti-virus programs cannot yet detect; this makes them an online essential. You should note that personal firewalls complement, and do not replace, AV and other security software.

Patches and security fixes

Modern software contains millions and millions of lines of instruction code, created by many programmers. Numerous bugs (mistakes) are picked up during testing, but many more slip through and only come to light when thousands of end users start utilising the software in different ways. In the past these bugs might have just caused a program to crash; malware writers now deliberately exploit them to propagate their programs. The types of bugs that malware writers can use to gain access are termed vulnerabilities, and you should be aware of the need to combat them as they are identified.

If using a fairly recent Windows Operating System, you should subscribe to the Windows Automatic Update service (<http://windowsupdate.microsoft.com>). This will scan your system and determine which fixes and patches are required, download them to your PC, and alert you when they require to be installed. You should also be familiar with the application software running on your machine, and note how the vendor issues updates and information about them – especially any AV and personal firewall products. Many will have a mailing list to keep you up-to-date; you should subscribe to it.

Other platforms

Security problems are not just related to the Microsoft Windows environment. Windows gets more publicity because the sheer size of its installed user base makes it an attractive target. However, other operating system users perhaps need to be even more vigilant because problems are often not as widely known, or because more skill is needed to resolve them. Linux users, especially if not using an up-to-date distribution, need to be aware of problems that can be exploited, and the amount of open ports on their machines. Mac users should use the Mac OS Software update feature.

Backup

After securing your machine, there is one point you must consider – it is the one that most of us ignore or forget about until it is too late. This is the backing up of your data.

Reputedly there are two types of end user – one who makes sure to backup, and one who has not yet lost any data. Any data you have on a PC should be considered transient at best. It is highly possible it will be gone tomorrow. Consider as scenarios the total shutdown of your computer due to one injudicious click on the enclosure to an email, or due to a catastrophic hard disk failure. This is not alarmist, it can and does regularly happen. Would you even be able to re-install your basic operating system? You probably bought your computer with that software ready installed, and were given no original disks. Many manufacturers will offer to supply a recovery disk to cope with this; it seems expensive at the time... until the need arises for its use! A recovery disk will take you back to the original 'factory-installed' state, which will come as something of a shock if

you have been using your computer for quite a while.

So, your chosen method of backup, and its frequency, depends on how quickly you need to be up-and-running again, and the importance of the data i.e. how much can you afford to lose? The simplest and cheapest solution is to regularly copy your data to a recordable CD (CD-R), and perform a manual re-install of all application software should this prove necessary. Remember to backup things like Internet favourites and bookmarks, and also user names, passwords and dial up details for your Internet Service Provider (ISP). Consider also where to store the backup – if your PC suffered flood or fire damage, would the backup suffer equally?

Having the newest and best technology is of little use if a backup procedure is not in place. Perhaps if the PCs are in your Scout Hall, it could be done before a regular Group Executive Meeting?

Conclusion

The use of computers in Scouting is comparable to many of our activities. It is no more acceptable to run a computer system without proper protection, than it is to undertake an adventurous activity without the appropriate experience, kit, and preparation. A certain degree of diligence is required to use a computer responsibly nowadays - the alleged lack of available time or resources is not an excuse.

Summary

In brief then, the advice is:

1. Install a personal firewall
2. Install anti-virus software, and keep it up-to-date

3. Install and use anti-spyware software, and keep it up-to-date
4. Make sure your computers receive all the latest security updates
5. Backup all of your data to a schedule, and stick to it
6. Evaluate critically everything you receive from the Internet

These security housekeeping requirements may seem tiresome, but once set in place will become part of your computing routine. Further developments in Internet business use will, inevitably, attract yet more sophisticated criminal activity; as a responsible member of the Internet community you will want to avoid being made an innocent part of this. Adhering to these requirements will not guarantee you total avoidance, but you will as far as possible 'Be Prepared', and it will make the online experience as safe and smooth as possible – for you and others!

Annex A

Annex A to this paper lists a set of readily available software packages that have attracted favourable comment from many working in the field of IT Security. Whilst The Scout Association offers no specific endorsement of these packages, they are free for you to use to protect your PC and to enable 'safe surfing'.

A suggested security software suite

As the main paper indicates, it is not prudent to use the Internet without taking personal responsibility for your security. The positive approach is to use protective software specifically designed to counter the various threats with which you are faced. This regular and constant security 'housekeeping' may appear tiresome - nevertheless, you may well be surprised at what is found to be residing on your computer the first time you run some of these programs. So, where do you get this software? Is it expensive? Is it easy to use?

The easiest approach would be to advise Members themselves to find out what is needed, and to take appropriate steps. We can, however, be a little more helpful than that, without in anyway suggesting that The Scout Association endorses the use of any of these programs - it does not.

What we can say is that the following programs are widely available, they are free, they are easy for you to use, and they are regularly recommended in computing publications and the Press. For these reasons alone it is worthwhile using them to safeguard yourself - and by using them you will also help to stop the further spread

of 'zombie' or compromised PCs, which are spreading Spam and other Internet attacks.

Although some programs may appear to offer protection from the same threat, it has been found that some do in fact pick up malware etc. missed by others ... and of course it is safer to have more than one wall of defence.

Even with a dial up connection, none of these programs can be regarded as excessively large for a download.

The first two programs, firewall and anti-virus, should be installed and running all the time your computer is operating:

1. Kerio Personal Firewall. (Critically, this program will not only control data transfer in, but also out of your computer).
(www.kerio.com/kpf)
2. AVG Anti-Virus Free Edition.
(www.grisoft.com)

The following programs should be installed and run on a regular basis dependant upon the extent of your use of the Internet, and not less than once per week. Most will themselves advise you when they require updating; for those that don't you should manually try to update not less than once per month. It is suggested that the programs are run in the following order:

3. 3CWShredder - CoolWebSearch Trojan Remover.
(www.intermute.com/products/cwshredder.html)
4. Ad-Aware SE Personal Edition.
(www.lavasoft.de/)
5. Spybot - Search and Destroy.
(www.spybot.info/en/index.html)

6. Microsoft AntiSpyware.

(www.microsoft.com/athome/security/spyware/)

7. HiJackThis - General Browser Hijacker Detector and Remover.

(www.merijn.org/files/hijackthis.zip)

For your convenience, all of these programs (with the exception of HiJackThis) can also be downloaded from the computer magazine PC World's web site at www.pcworld.com/downloads/index.asp