



SCIP LEARNING

Internet skills in your community

PC Self-Defence

A workshop about Malware (Malicious Software) - Keeping your computer clear of viruses and other online threats.

Marcus Pennell, SCIP, 2008

This work is licenced under the Creative Commons Attribution-Non-Commercial-Share Alike 3.0 Unported License. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>

Internet skills in your community//Protect and maintain your computer

Marcus Pennell, SCIP, 2008

This work is licenced under the Creative Commons Attribution-Non-Commercial-Share Alike 3.0 Unported License. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>

Workshop Overview

This is a workshop lasting 4.5 hours.

It is designed for people who are comfortable using a PC for everyday tasks. No specialist knowledge is needed or expected. It is a 'hands on' session where students are guided through downloading and installing some security software from the Internet.

Learning outcomes from this session include:

- Jargon busting. You will understand what the most common terms are - such as the difference between a worm and a Trojan.
- The ability to spot a malware attack at an early stage. The sooner you spot it the better your chance of getting rid of it.
- Understanding how to install and run anti-malware programs like **Spybot - Search & Destroy** and **Adaware**.
- Understanding the importance of Windows updates, how to set them up automatically, and how to do them manually.
- Understanding how to avoid much of the problem by the use of some software and the avoidance of others.

Contents

- 1 Definitions of Malware
- 2 Why is someone doing this to my computer?
- 3 Update! Update! Update!
- 4 Install Spybot & Adaware
- 5 Have antivirus software and keep it up to date
- 6 Use Google tool bar or Firefox to stop pop ups
- 7 Keep a clean PC, remove temp files and defrag
- 8 Backup!
- 9 What not to do
- 10 Really useful websites for more information
- 11 What next?
- 12 Sudden Slowdown Checklist

Internet skills in your community//Protect and maintain your computer

1 Definitions of Malware

The term 'Virus' has taken on a double meaning. To most people it means just about anything nasty happening on a computer due to an attack from outside, but that term should really be Malware - Malicious Software. A true virus has certain characteristics which distinguish it from other threats.

Trojan

- Arrives as a tempting internet download like a sidebar, game, or screensaver.
- Can also arrive as a 'Drive-By' from visiting compromised websites.
- Does what it says it will, but then does a lot more that it doesn't tell you about like installing malware without your knowledge.
- Carries a secret payload that can include several dozen of the following:

Virus

- Arrives by Trojan, on a floppy or memory stick, or as an email attachment.
- Generally unsophisticated and not much seen these days.
- Attacks your computer, corrupting system files.
- Damage to computer can be a prank like inverting the screen or catastrophic like wiping the hard disk.
- Cannot get off the computer except if it sent as an email or carried on disk etc.

Worm

- Arrives by Trojan or email attachment, or through direct 'probing' of the network or your internet connection.
- Does not try to damage computer and tries to stay unobtrusive and hidden. However, some worms are badly written and can cause unpredictable computer behaviour and serious damage. Others can corrupt your PC if you try to take them off the wrong way.
- Replicates by sending copies of itself to everyone in your address book, or other PCs on your network.
- E-mail worms can fake their addresses by pretending to be from anybody and to anybody in any captured address book, so e-mails carrying the worm appeared to bounce around between colleagues and friends.
- May block access to Windows Update and anti-virus websites.
- Used to carry out mass email scams and 'denial of service' attacks.
- Slows down your pc and uses internet bandwidth.

Backdoor (Remote Access) Trojan.

- Arrives by Trojan or email attachment.
- Monitors internet traffic and 'listens' for instructions from its controller.
- Downloads new worms, diallers etc on demand.
- Turns the PC into a 'Zombie' - part of a Botnet.

Marcus Pennell, SCIP, 2008

This work is licenced under the Creative Commons Attribution-Non-Commercial-Share Alike 3.0 Unported License. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>

Internet skills in your community//Protect and maintain your computer

Dialler

- Arrives by Trojan or email attachment.
- Only a threat if you use an ordinary dial up modem.
- Calls premium rate lines automatically. Redials immediately you disconnect so the only way to stop it is to pull the plug out of the phone socket.
- May connect you straight to porn sites at premium rate.
- Other types of diallers can hijack your internet dial up connection so that when you think you are calling your unmetered Orange account you are really calling their premium rate 0986 number. You still get through to the internet and go straight to your home page. You don't notice anything is wrong until the phone bill arrives.

Keylogger

- Arrives by Trojan or email attachment.
- Records keystrokes. A sophisticated logger can recognise a bank's internet address or a sequence of numbers that could be an account number and start taking rapid screenshot pictures of your desktop and mail them off, with the keyboard input, to its master.

Browser Hijacks

- Arrives by Trojan or email attachment or by visiting malicious websites.
- Redirects your home page to porn sites or marketing portals such as WhenUSearch. Won't let you change this.
- Installs extra browser buttons.
- May refuse you access to real search engines.
- Not designed to harm your computer - most claim to 'enhance your web experience' - but when you get two or three all competing to do the enhancing it can lock your browser solid.

Distributed Denial of Service (DoS or DDoS)

- A form of commercial and political sabotage. Also called 'Bombing'.
- Masses of compromised zombie computers around the world mount a timed attack on a web site, sending hundreds of 'hits' a second from tens of thousands of computers, and bringing the site to a halt.
- Other DoS attacks may involve the active participation of a group of hackers, rather than compromised computers. The timed attack on Scientology websites in January 08 was one such attack and used a program called SciDBomb which had been distributed on the Internet a few days earlier.

Spam Server

- A Worm which contains its own email generator.
- Sends tens of thousands of spam emails out of compromised computers a day with adverts for Viagra etc.
- Uses supplied address list or an algorithm for guessing Hotmail or Yahoo addresses.

Popups (Adware)

Marcus Pennell, SCIP, 2008

This work is licenced under the Creative Commons Attribution-Non-Commercial-Share Alike 3.0 Unported License. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>

Internet skills in your community//Protect and maintain your computer

- Arrives by Trojan or visiting websites.
- Annoying little windows which obstruct the page.
- Clicking the 'Close' button will lead you on to other horrors.
- May arrive too fast to close, filling the whole screen.

Spyware

- Spyware can include a sophisticated keylogger with screen-grabbing ability plus the ability to intercept and re-route email and other communications like Instant Messaging sent to that computer.
- It is sometimes used to spy on partners, as it can be sent as a Trojan attachment in an intimate message. These may slip past your email anti-virus defence as DIY 'Love Cheat' spyware kits have been sold as legitimate software, although the practise has now been made illegal in most countries.
- Spyware can also switch on a computer's microphone or camera, allowing the spy to listen to what is happening nearby and see through its camera.

Phishing

- Arrives by email claiming to be from your bank or eBay or PayPal saying your account details need verifying. Clicking on the link in the email takes you to a bogus but genuine looking website which tries to get your credit card or bank details.

Pharming

- It's out there, somewhere.
- When you type www.google.com that instruction goes to the nearest 'phonebook' - called a DNS Server - on the internet, usually it's your Internet Service Provider. A DNS Server has a list of all the internet names in the world and can translate them into a string of 12 numbers in the format 123.123.123.123. These 12 numbers are the real addresses of the web sites on the internet.
- A Pharming attack involves inserting a false page into one of the servers, by hacking into it, so that requests for www.interbank.com don't go to 214.125.121.102 but to 112.134.103.127 (the attacker's lookalike webpage).
- There are 13 Master DNS Servers in the world. That's 13 computer systems which confer and agree on the layout of the internet in any nanosecond. Someone managed to simultaneously hack into 10 of them recently.
- There is nothing you can do about this.

Marcus Pennell, SCIP, 2008

This work is licenced under the Creative Commons Attribution-Non-Commercial-Share Alike 3.0 Unported License. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>

2 Why is someone doing this to my computer?

It's the question everyone asks when they realise something has infected their computer. Who would do this, and what do they get out of it?

The first virus appeared in 1986 after two programmers wrote a routine that changed the volume label of any 3.5inch floppy disk put into the infected computer. They weren't being malicious - they just wanted to show that it could be done.

They were followed by much nastier people who used this idea to cause havoc. A disk inserted into the infected computer could infect the next computer it was put into, and now the infection could cause the computer to wipe its disk at a given time and date - the Chernobyl Virus reformatted the hard disk on April 26 for instance.

But after a while, the fun went out of it, even for the most hardcore of vandals. It had all been done; there was nothing left to prove; nobody left to impress.

But there was money to be made. Not by destroying peoples' computers, but by secretly taking them over and using them without the owners' permission. The age of the Worm had arrived. Worms could turn a computer into an email monster capable of sending out tens of thousands of email a day containing adverts for Viagra, credit and mortgage offers, and dubious pills claiming to make various body parts bigger.

Worms could also be used to mount commercial attacks on your business rivals using a so-called Distributed Denial of Service Attack - hundreds or thousands of computers simultaneously send hundreds of requests a second to a particular web site, bringing it to its knees for hours or even days.

Then came all the other problems - keyloggers trying to steal your identity and diallers trying to connect you to £1.50 a minute porn lines. Every month or so someone comes up with a new way of trying to fleece the unwary using the Internet

It used to be enough to have a virus killer on your PC. Nowadays you need a lot more than that to keep yourself free of problems.

Microsoft make it relatively easy for the malware writers to do their evil business by regularly putting out security enhancements for Windows. The bad guys get hold of these updates and 'reverse engineer' them to find out what security flaw they were written to fix, then they write their programs to exploit those vulnerabilities on the assumption that not everyone is going to install the updates.

The result is that most computers are immune to these infections because they get updated regularly, but a significant number are left completely vulnerable and get infected. Once a hacker has got their program running on a vulnerable computer they are able to control it remotely and get it to do almost anything.

The majority of compromised computers are home PCs which are connected to the Internet by broadband. Business PCs usually get updated regularly and have extra defences such as firewalls to protect them.

3 Update! Update! Update!

If your computer is connected to the Internet and if Windows is not updated regularly it will become infected. That is a certainty. Having anti-virus software will not prevent this.

Do this simple test: restart the computer and look at the Windows XP splash screen as it loads. Can you see a date in the copyright line? If so your computer is badly out of date. If it says: 'Copyright 1985-2001 Microsoft Corporation' it means the a major upgrade called Service Pack 2 (SP2) has not been installed and your computer is very much at risk. Service Pack 3 is now available.

By default, Windows pre-SP2 does not update itself automatically. You can install SP3 and all the other security updates manually by going to the Windows Update website - there's a link in the Start Menu. You will have to go through the 'Windows Genuine Advantage Validation' routine to ensure your copy of Windows is authentic before you can proceed. (However, you will find an installable copy of SP3 on the Tools disk accompanying this course. There is a copy of SP3 for Office 2003 and SP1 for Office 2007 on the Tools disk as well.)

Once you visit the Windows Update website and pass the validation you can sign up for Microsoft Update. This will automatically update Windows and any other Microsoft programs you have installed.

Don't forget to set the update schedule. **Start -> Settings -> Control Panel -> Automatic Updates** and set it to a sensible time when the computer is on, or use the option to automatically download updates and tell you when they need installing.

4 Install Spybot & Adaware

What it is:

Both Spybot and Adaware are small free programmes that check your machine for malware.

Spybot - Search & Destroy can detect and remove a wide range of malware including trojans and spyware. It can also 'innoculate' your PC against threats. It can be set to run scans automatically. Get it from <http://www.safer-networking.org/en/spybotsd/index.html>

Ad-Aware is designed to provide protection from known Data-mining, aggressive advertising, and other pests such as popups. Get it from

<http://www.lavasoftusa.com/software/adaware/>

How to do it:

use www.download.com to get this free software. This is a safe site for downloading any software you need. Type Spybot (or Adaware) in the 'search'. You can then download them and install following the on screen step by step instructions.

A free alternative to Spybot is SuperAntiSpyware available from www.superantispyware.com.

NOTE: always backup your data before installing anything new, these sites are safe but it is a good policy, see section 8.

5 Have antivirus software and keep it up to date

What it is:

Antivirus software is able to detect known viruses on your computer and most can also eliminate them. Some can stop viruses getting to your machine. Anti-virus programs will stop most worms but not Trojans.

There are many well known AntiVirus software packages available such as Norton and McAfee. Some are free and some you need to pay for. The most well known ones can be more vulnerable to virus writers as they target weaknesses in the antivirus software so it is worth looking at reviews. SCIP use AVG which comes free for home use and at 50 percent discount for charity use.

Why you need it:

Viruses have been a fact of life to those with a computer connected to the Internet for many years. They come in many forms and range from cheeky to damaging. You do not want one running on your PC!

How to do it:

AVG is free for home use, you can download it from:

<http://free.grisoft.com/freeweb.php/doc/2/>

Clamwin is an open source viruskiller which can be used at home or in the office for free.

Download it from: <http://sourceforge.net/projects/clamwin>

WARNING: if you already have antivirus software on your computer you should not install another one. If you choose different software please uninstall the old one. If you end up with two anti-virus programs on your pc they will each treat the other as hostile and they will fight.

.

6 Use Google toolbar or Firefox to stop pop ups

What it is:

Pop up stoppers can be added to your Internet Explorer and block browser windows that you haven't specifically asked for.

There are lots available but a simple one to use and install and that is reliable is offered by Google.

Why you need it:

When using a browser to access the Internet you may notice that lots of small windows containing anything from promotional material to obscene photos 'pop up'. These are distracting and confusing and often offensive.

How to do it:

Go to the Google website, the direct address for the toolbar is: <http://toolbar.google.com/> and follow the installation instructions.

Once in place you will see an additional 'tool bar' on your browser. You can see how many pop ups have been stopped! If you run Spybot and Adaware regularly you should have less and less over time.

NOTE: Some sites actually use pop ups as part of their design, such as Exchange and Mart. If you click on a trusted link and nothing happens, your pop up blocker is stopping it. To override this you hold down your keyboard control key while clicking on the link and you will be able to view it as normal.

Alternatively, you can stop using Internet Explorer completely and use Mozilla Firefox instead. Firefox attracts fewer malicious attacks than Internet Explorer and its development team are better at fixing known problems than the Microsoft team.

Firefox has a built-in popup blocker. It can be downloaded from <http://www.mozilla.com/firefox/>

7 Keep a clean PC, remove temp files and defrag

Windows includes a number of tools as part of the operating system that allow you to keep things tidy. A tidy computer is a happy computer.

Disk Cleanup: this removes temp files that have been left from using the Internet and cutting and pasting etc.

Disk Defragmenter: this reorganises the way your hard drive stores files so that they are quicker to find.

Why you need to:

Over time your PC collects lots of unwanted files or parts of files, these slow the PC down and are of no use. It is like a service for your car but much easier and cheaper to do! A hard disk that has become fragmented is very slow to access and can cause the computer to crash or refuse to boot.

How to:

Windows provides tools for maintenance, we will look at Disk Cleanup and Defragmentation.

[GoTo: Start > Programs > Accessories > System Tools > Disk Defragmenter]

[GoTo: Start > Programs > Accessories > System Tools > Disk Cleanup]

You can then follow the instructions, both systems run themselves.

NOTE: you need to allow some time for both so let them run overnight or lunchtime. You do not need to watch it.

There are various free alternatives to these inbuilt Windows tools, and generally they do a better job. CCleaner is an excellent program for removing temporary files and other litter from your PC. It can be downloaded from www.ccleaner.com.

For defragmenting you could use Ultimate Defrag which is available from www.disktrix.com.

8 Backup!

Once you get used to a way of keeping reliable copies of your work, you will find it simple to do and then if anything does happen you will not have lost everything.

If you are lucky to work in a network environment with a network administrator you may find that backup is sorted out for you, so it is always worth asking and being clear about your role in this.

What it is:

Keeping a copy of important files separately from your computer so that if your computer dies or the files become infected you have a copy that you can use.

Backup needs to be appropriate for the way you work. For example, you can use a floppy disk (but these are unreliable) and copy across files at the end of the day or burn a CD (with rewritable CDs you can use one many times to keep the expense down) or you can have a backup system that your technical team has sorted out for you.

Why you need to:

If you lose a week's work on a funding bid that you are writing you will be very, very pleased if you have a recent copy and don't need to start again from scratch.

How to:

Firstly, talk to your technical team about your options.

Ideally you want a system that allows you to take the backup data off-site for storage, in case your office is burgled or has a fire.

If it is just your PC and you have a CD/DVD writer use a write-once or rewritable CD or DVD. You can store up to 700 MB on a CD and 4.7 GB on a DVD.

If you do not have a CD writer then consider buying a USB key (also called a memory stick). These come in different data storage sizes - currently up to 16 MB - but are not expensive and work like a reliable floppy disk. Make sure you 'stop' them before removing them from the PC otherwise you could lose data.

If you do not have a USB port in your computer (it is very rare now not to) you will need to use a floppy disk.

If you have several PCs in a network you can use the spare hard drive space on each one to back up the data from another. This method is easy and can be made automatic, but it is flawed because data isn't taken off-site.

Marcus Pennell, SCIP, 2008

This work is licenced under the Creative Commons Attribution-Non-Commercial-Share Alike 3.0 Unported License. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>

Internet skills in your community//Protect and maintain your computer

REMEMBER: whatever system you use, label it well and check that you can restore your files regularly (once a month is fine unless there is an ongoing problem).

Marcus Pennell, SCIP, 2008

This work is licenced under the Creative Commons Attribution-Non-Commercial-Share Alike 3.0 Unported License. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>

9 What not to do

1) Do not download free software that you are offered.

Games, Kazza, LimeWire and other software can contain malware. Make it a company policy that workers and users must not install software without consent. This should include screensavers, as these are one of the most common sources of infection.

2) Educate staff about the risks. Make sure everyone knows not to open email attachments unless they are expected. If necessary phone the sender to confirm that they really did send you the attachment.

3) Don't panic! If your antivirus software finds a virus it can usually clean it as well. If you are getting alerts you can be confident that you are doing all you can to have a safe machine.

10 Really useful websites for more information

For practical background reading:

<http://www.lasa.org.uk/knowledgebase/index.shtml>

articles include:

Safe and sound - keeping your computers and data secure

Sensible precautions to help keep your computers and data safe.

How Secure is the Internet?

A guide to the main Internet security threats and how to avoid them.

Dealing with Computer Viruses

Practical advice on keeping your PCs clean and safe from viruses.

Virus Alert

The basics of virus protection - based on Lasa's own experience of infection!

Updating your Antivirus software

Links to update pages of popular Antivirus Software vendors

Virus Hoax Alert - Recognising hoax viruses.

For information about viruses (a database of all and alerts about new ones):

<http://securityresponse.symantec.com/>

For a book to have at hand:

Marcus Pennell, SCIP, 2008

This work is licenced under the Creative Commons Attribution-Non-Commercial-Share Alike 3.0 Unported License. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>

Internet skills in your community//Protect and maintain your computer

Viruses and Spam: what you need to know

www.sophos.com

Marcus Pennell, SCIP, 2008

This work is licenced under the Creative Commons Attribution-Non-Commercial-Share Alike 3.0 Unported License. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-sa/3.0/>

11 What to do next:

Everyday:

Schedule your antivirus software to update.

This needs to be at a time the computer is connected to the Internet but that you are not using it. This can be lunchtime, at the end of the day, whichever suits you best.

Backup important files to CD or floppy or use your current backup system.

Weekly:

Run Spybot and Adaware.

Weekly backup routine.

When reminded/weekly:

Run Windows update

Check for virus alerts.

Monthly:

Test your backup.

3 monthly:

Office update.

In the future:

Keep up to date with Microsoft news, check Lasa Knowledge base.

You may wish to buy a PC magazine every now and then

All the above!