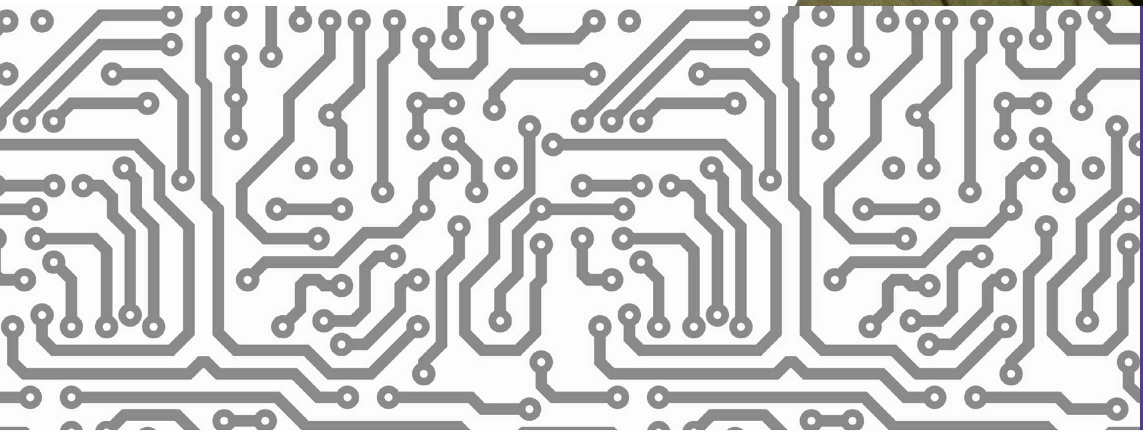


Basics

Use this document with the glossary

Beginner's guide to

Internet basics

2.3 Protecting your computer

How can I protect my computer?

This activity will show you how to protect your computer from malicious software and how to stay ahead of people who might want your private data.

What will I learn?

- What the risks are to your computer
- How to block viruses and spyware
- How to keep your computer up to date

www.connectingcumbria.org.uk

CONNECTING CUMBRIA

BT

How do I do it?

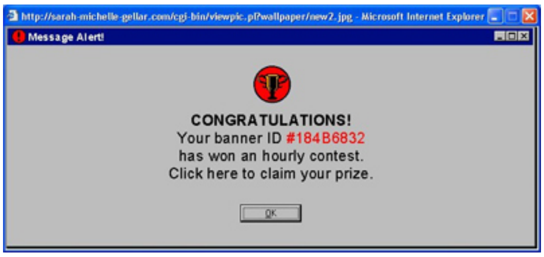
Be safe! If you're using this hand-out on a shared or public computer, remember to:

- **Log on using a 'strong password': one that includes upper and lower case letters, numbers, and isn't something that someone else could guess.**
- **Never share or write down your password.**
- **Log out when you're finished.**

The web links referred to throughout this document can be found in the Useful Links section at the end.

What are the risks to my computer?

1. When you're using the Internet, your computer downloads data. Normally this is safe, but some sites can trick you into downloading programs that can capture your personal information and send this to criminals. Names for these include viruses, trojans, malware and spyware. They work in different ways, but they all put you at risk:



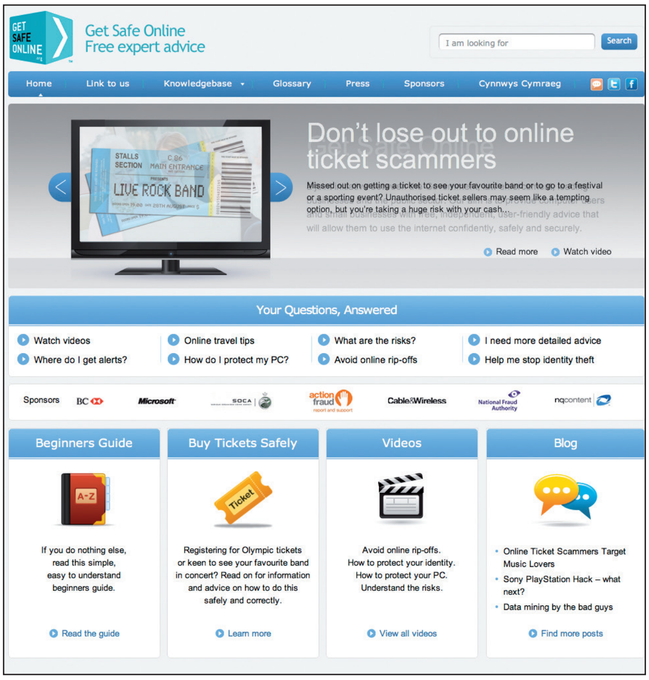
http://sarah-michelle-gellar.com/cgi-bin/viewpic.pl?wallpaper/new2.jpg - Microsoft Internet Explorer

Message Alert!

CONGRATULATIONS!
Your banner ID #184B6832
has won an hourly contest.
Click here to claim your prize.

Example of Malware

- Go to the Get Safe Online web link in 'Useful Links'. Scroll down and click on the link for advice videos and then click to watch 'Protect your PC'. You may have to press escape after you have watched the video.
- Scroll to the top of the page and hover your mouse over Protecting Your Computer and Protecting Yourself. Various options will appear – explore these to find out more about the myths about protecting your computer, the threats you face, and how people become victims.



Don't lose out to online ticket scammers

Missed out on getting a ticket to see your favourite band or to go to a festival or a sporting event? Unauthorised ticket sellers may seem like a tempting option, but you're taking a huge risk with your cash...

If you do nothing else, read this simple, easy to understand beginners guide.

Registering for Olympic tickets or keen to see your favourite band in concert? Read on for information and advice on how to do this safely and correctly.

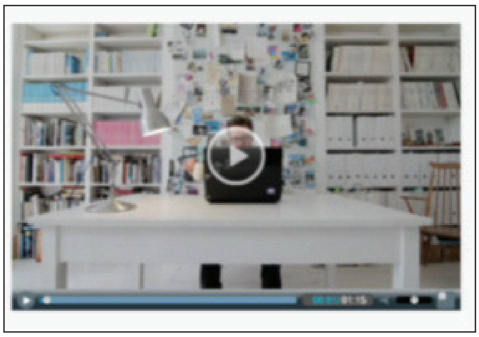
Avoid online rip-offs. How to protect your identity. How to protect your PC. Understand the risks.

- Online Ticket Scammers Target Music Lovers
- Sony PlayStation Hack – what next?
- Data mining by the bad guys

Get Safe Online website

How do I block viruses, spyware and other threats?

2. You can protect your computer by using the right software and the right behaviour. One of the best ways to be safe is to think before you click.
   - Visit the Get Safe Online site. Scroll down and click on 'Videos' and watch the 'Protect your PC' video.



Protect your PC video

3. Anti-virus software constantly scans your computer for problem software that might put you at risk of identity theft or fraud. There are many types available, some of which are paid for, and some of which are free.
   - Visit the Microsoft Security Essentials web page in 'Useful links'.
   - The support link will show the types of actions that can be taken in the event of a problem.
   - This page will identify which version of Microsoft Windows you have and show you the appropriate information.
   - For Windows 8, Security Essentials is called Windows Defender.
   - More information can be found in the Product Info section.

4. The latest versions of web browsers come with built-in security filters that can detect many fake websites. But don't just rely on your software. Think before you click:
   - Avoid dodgy websites that offer a deal that's too good to be true.
   - Don't click on links in a website or email that you're not completely sure about.
   - Don't give out personal information unless you're sure that the site is genuine and safe.

5. There's lots more you can learn about protecting your PC – and yourself – when online. The Get Safe Online site you mentioned earlier has a lot of useful information.
   - Go back to this site and hover the mouse over Protecting Your Computer again.
   - Read the information in the web links on:
     - Firewalls
     - Viruses and Spyware
     - Windows updates
   - Think about what you need to do to make your PC safe at home.

How can I keep up to date?

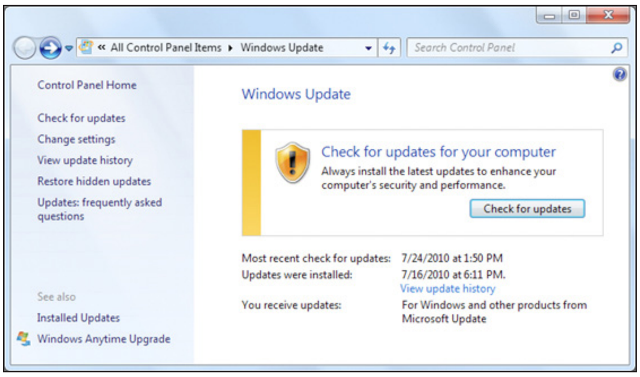
6. Your computer's software needs to be up to date in order to keep you safe. Regular updates fix any known security problems and update the anti-virus software's database of known threats. You need to keep your operating system (eg Windows), anti-virus software and web browser software all up to date:
   - Remember that to update, the computer's security software needs to download new data from the Internet. This won't

be possible if you just use the web for a few minutes a day and then turn off your computer.

- At least once a week, leave it on for a couple of hours so automatic updates can complete.

7. Most computers are set so that they update Windows automatically:

    - Click the Start button to open the Windows Start Menu (bottom left of the screen) or to access the search tool (magnifying glass).
    - In the search box at the bottom, enter ‘windows update’ into your search box and click on ‘Windows Update’ in the search results.
    - If automatic updates are not on, click the button to turn on automatic updates. The computer will immediately start checking for updates.
    - You can set how often your computer checks for updates. Click on ‘Change settings’ in the left-hand menu of the Windows Updates panel. There is a drop-down menu for each option. It’s best to leave these as they are, and to leave your computer turned on. But if you don’t leave your computer on all the time, change these settings to when you will, for example by leaving it on overnight once a week. It’s important that you then remember to do this every week.
    - This also makes sure that Microsoft Security Essentials or Windows Defender is kept up to date.
    - Another way is to visit the Windows Update website and follow the instructions.



Check for updates for your computer

Always install the latest updates to enhance your computer's security and performance.

Most recent check for updates: 7/24/2010 at 1:50 PM

Updates were installed: 7/16/2010 at 6:11 PM.

You receive updates: For Windows and other products from Microsoft Update

Example of Windows Update

8. Internet Explorer is updated as part of Windows Update and other browsers should also update automatically.

Quiz yourself

- Why can some websites put your privacy or computer at risk?
- What information can criminals find by installing software on your computer?
- What software can help protect your safety?
- What might tell you that a web link or site is not safe to use?

Try your new skills

Practice what you have just learnt:

- Check your firewall is on: you can check in the same way that you checked Windows Update.
- Check that you have anti-virus software installed and that it is up to date.
- Use a search engine to find out more about anti-virus software that you can buy.

Write down any notes that will help you:

My learning checklist

□ I can explain to someone why going online can put my personal information and my computer at risk.

□ I can browse the Internet safely and avoid dodgy websites.

□ I know what software I need for my web browsing to be safe.

□ I know how to install and update this software so I stay safe.

Top tips

- Your computer's security settings (accessed using the Control Panel) are pre-set to keep you safe. It's not a good idea to change any security settings.
- Beware of emails that are forwarded by friends or family. You might trust them, but you don't know who sent the link to them.
- Don't download software unless it's from a site that you trust. This applies to free and paid-for programs.

Where next?

Protect yourself from phishing:

- Phishing is the name for using fake websites to capture personal data. Usually, an email will try to lure you to the site, which is commonly for a bank or other financial provider.
- Get Safe Online has a video about phishing and more information in its Knowledgebase.
- Remember that a reputable site will never send an email asking you to provide your username, password or other personal information.

Check the spam filtering in your email programme:

- Spam is unwanted email that can also expose you to fraud or infect your computer. Up-to-date email programs, either on your computer or web-based, all include filters to block spam.
- Complete hand-out 4.1 Understanding email if you're not sure about email.
- Don't ignore spam in your inbox. Mark it as 'spam' or 'junk' to remove it, and don't open it.
- If spam is getting through, use your program's help facility to increase the filtering. If you do this, you may need to check your spam folder from time to time in case emails that you want to receive are getting blocked. You can 'unmark' these so the program won't filter them in future.

Write down any notes that will help you:

Useful Links

You may want to use these links in your session:

Get Safe Online:
http://www.getsafeonline.org

Microsoft Security Essentials:
http://www.microsoft.com/security_essentials/default.aspx?mkt=en-gb

Windows Update:
http://windowsupdate.microsoft.com

Internet Matters
(for additional useful information on keeping you and your computer safe)
http://www.internetmatters.org

In association with

Department
for Culture
Media & Sport

SUPERFAST
BRITAIN

Cumbria
County Council

EUROPEAN UNION
Investing in Your Future

European Regional
Development Fund 2007-13