



# Online Security

Protect your identity, your personal  
information and your family.

make it safe • make it simple • [makeITsecure.org](http://makeITsecure.org)

## Welcome Note from the Minister for Communications, Energy and Natural Resources

I am delighted to welcome you to our third national computer security awareness campaign: **makeITsecure** 2008.

A handwritten signature in black ink that reads "Eamon Ryan".

As this is the first time the campaign has been delivered on an all Ireland basis, I would also like to welcome and thank Rt. Hon. Peter Robinson MLA, for working with us to include Northern Ireland in this year's campaign.

I would also like to extend our thanks to our sponsors for their continued involvement in our national campaign and to extend a warm welcome to new partners 3 and O<sub>2</sub>.

The aim of the campaign is to ensure that using computers, broadband and the Internet is a positive experience by providing some basic information on the issues that may affect computer users.

Please visit [www.makeITsecure.org](http://www.makeITsecure.org) for more information.

## Welcome from Rt Hon. Peter Robinson M.P. MLA Minister for Department of Finance and Personnel

I am delighted that the Department of Finance and Personnel (DFP) has been able to support a project as unique and important as **makeITsecure**.

As valuable as modern technology, the Internet and web surfing may be, computer security awareness is a very real issue. It is important that the safety awareness message continues, and that is what this campaign aims to do.

As DFP continues with its digital inclusion policy and broadband usage levels increase in Northern Ireland, it is incumbent upon us to remind citizens not only of the benefits of broadband and the Internet but also make them aware of some difficulties they may face and provide some easy and effective steps to keep safe whilst online.

A handwritten signature in black ink that reads "Peter Robinson".

By learning from this campaign, we can all enjoy the undoubted benefits of information technology and the world wide web, and more importantly be able to do so safely.

# Make the most of your Internet experience by surfing wisely

The Internet is now an integral part of our business and home life.

As well as making shopping and banking easier, it provides an encyclopedia of information at our fingertips, which we can access and share. The web is also a large community where users meet, share and communicate every day.

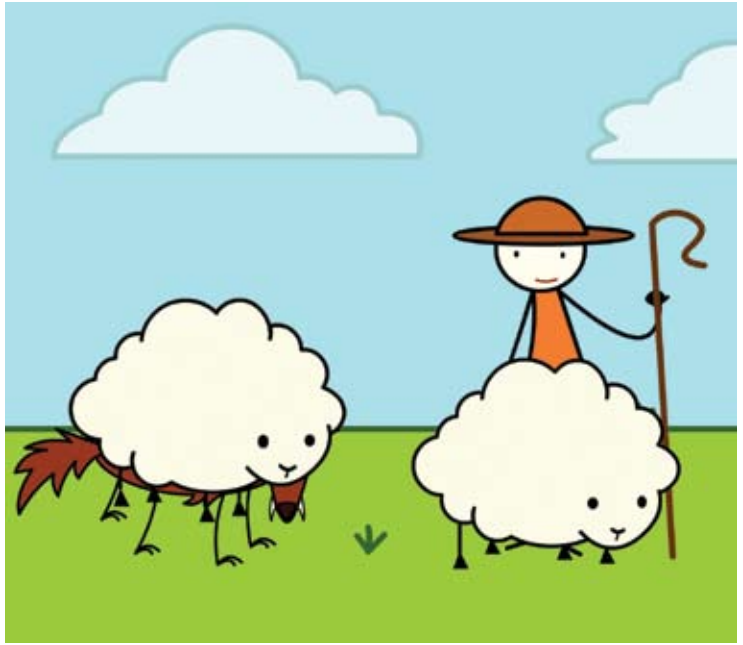
While surfing and transacting online is a convenient and rewarding experience, it is important to be aware of potential risks.

It is also important that your computer is protected and that you're careful about giving out personal details online.

This brochure and the **makeITsecure** website are designed to help individuals and families protect themselves while using the Internet.

It identifies some common risks of surfing and transacting on the Internet and offers solutions to these risks, so that everyone can enjoy a more positive and secure online experience.

**make it safe • make it simple • [makeITsecure.org](http://makeITsecure.org)**



# Phishing

## What is phishing?

**Phishers** are criminals who pretend to be legitimate organisations to trick you into giving them your personal details.

Phishing occurs when criminals (phishers) pretend to be legitimate organisations, like banks and credit card companies in order to trick you into giving them personal details such as bank account numbers or PIN numbers.

Phishers usually send you an email in which they may ask you to 'verify' or 're-submit' personal information by return.

They could ask you to complete an online form and may offer you something attractive like money or a holiday if you do so.

Be alert for anyone requesting your bank account details, credit card numbers, passwords, PIN numbers, Personal Public Service number (PPS) or National Insurance number.

Phishers can use this information to impersonate you and make unauthorised withdrawals from your bank account or use it to pay for online purchases. They can even sell on this valuable information to third parties.

## How will I know if I've been 'phished'?

Trust your instincts. If an email looks suspicious, delete it immediately or if it offers something that looks too good to be true, it probably is. If it appears to come from your bank or credit card company, inform their customer services department immediately.

## Here are some phrases that may be used in a phishing email:

'Verify your account'.

'Respond within 48 hours or your account will be closed'.

'Dear valued customer'.

'Click the link below to gain access to your account'.

## How can I avoid phishing fraud?

Trust your instincts. Remember, no reputable company will ever ask you to give out personal details by email.

Never give out personal details by email, fax or in response to a pop up advertisement or unexpected website address.

Always check your credit card and bank statements for any irregularities.

Use up-to-date anti-virus and anti-spyware software to keep unwanted or malicious software at bay. A phishing filter can help protect you from web fraud by warning or blocking you from reported phishing web sites.

**Pop up ads** are online advertisements that pop up in a new browser window.

## What to do if you think you've been phished?

If you suspect you've been phished, alert the relevant company that's being impersonated by using another form of communication such as a landline, mobile phone or another computer. Then contact your local Garda station or in Northern Ireland, contact the Police Service of Northern Ireland (PSNI) at 0845 600 8000.

Find out more at [www.makeITsecure.org/phishing](http://www.makeITsecure.org/phishing)

# Social Networking

## What is social networking?

Social networking websites help create and support communities of Internet users.

**Bebo** is a popular social networking site in Ireland with the majority of members belonging to the 13-24 year old age bracket.

You have to be 13 or over to open an account.

**Facebook** is a social networking site popular with the 25+ market though minimum age for sign up is 13 years.

**Nimble** is an Irish social networking site.

**Blog** is short for weblog. A blog can be a personal journal or diary, a political debate forum, a breaking-news outlet or a collection of links. At its simplest, a blog is a web site where you write and put information online on an ongoing basis.

Sites like Bebo, Facebook and Nimble attract thousands of Internet users from all age groups and allow members to communicate with friends and, if they choose, strangers online. Depending on the website in question, members share a variety of interests and hobbies and they can use the site to chat, message, email, upload and download photos and videos, blog, discuss and share information.

## How does it work?

When you create a profile on a social networking site, you usually upload some basic details about yourself, for example, your profile user name, where you're from and what music and interests you like. You can then decide whether you want to make your profile private or public. So, if you mark your profile 'private', nobody should be able to access any of your personal details unless you approve and add them to your friends list first.

## What are the risks?

Social networking sites by their nature, require a certain amount of personal information to be given. When deciding how much personal information to give out, users may not exercise the same amount of caution as they would when meeting someone in person. For example, don't give out your house address or telephone number and always mark your profile 'private' to ensure you always know who you are communicating with.

## How can I protect myself?

Be careful about how much personal information you put up online. Remember the Internet is a public resource. Only put up information you are comfortable with anyone seeing and prevent identity theft by limiting the amount of information you put online.

## How can I protect my child?

Social networking can be fun and educational provided your children are careful about what personal details they reveal online.

Tell them not to believe everything they read as sometimes people can lie about their identity.

Advise them never to meet anyone they've only chatted to online without a trusted adult being present.

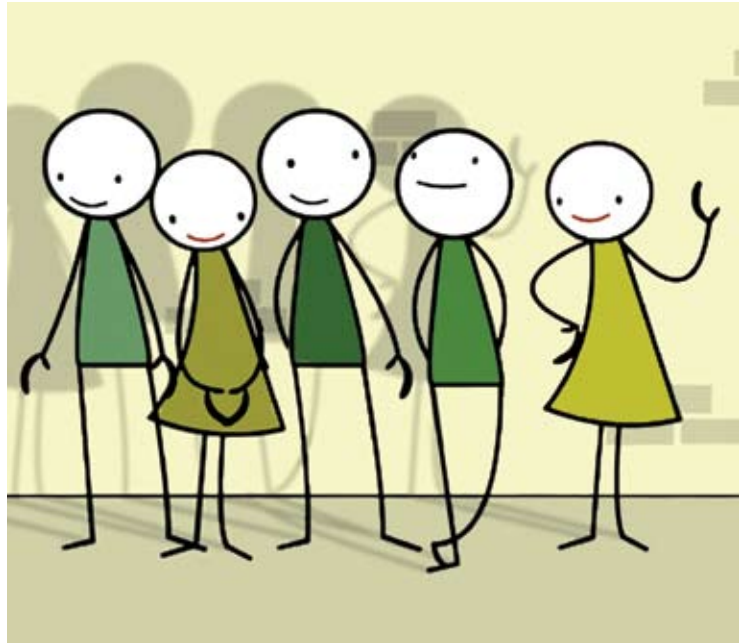
Warning them against meeting strangers may not be enough, as they may not consider the person they've been chatting to online a stranger.

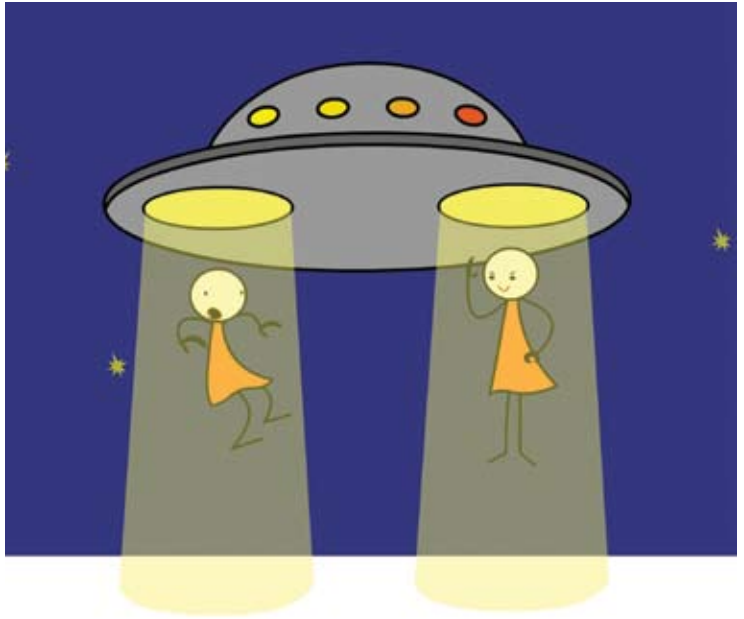
Get to grips with the technology they're using so you can talk about the Internet together. And remember, the Internet is now widely available on mobile phones, as well as in the home.

Know what sites your child has visited and if they are suitable or not.

Most Internet browsers now feature parental controls that you can use to limit your children's Internet access. It's advisable to familiarise yourself with these controls and to implement them accordingly.

**For more information, visit [www.makeITsecure.org/socialnetworking](http://www.makeITsecure.org/socialnetworking)**





# Identity Theft

## What is identity theft?

Identity theft is when a criminal impersonates you by stealing your personal information to withdraw money from your account or to pay for goods online. They may even make money from selling your details on to a third party.

## How do I recognise it?

Unfortunately, by the time you recognise it, you are likely to be a victim already. Some examples include:

- Refusal of credit or loan applications.
- Collection agencies contacting you for overdue debts you have never incurred.
- You may receive information regarding an apartment you've never rented, a job you've never had or a house you've never bought.

## What do I do if I am the victim of identity theft?

Immediately phone An Garda Síochána or the PSNI and report the identity theft.

Advise by phone and in writing the relevant bank or financial institution you have accounts or dealings with.

Notify in writing the relevant organisation or website where the identity theft occurred.

Cancel any cards or close any account that you know or believe has been tampered with.

## How can I avoid identity theft?

Be careful when giving out personal details over the Internet.

If you're making online purchases make sure your connection is secure. A closed padlock icon should appear on the status bar and the characters on the address bar should start with `https://` rather than `http://`

Check that companies display a clear privacy and security policy.

Use a strong password and don't share it with anyone. A random combination of numbers and letters and punctuation – at least 8 characters – is ideal.

Set up a special email address for shopping and newsgroups. If you need to change this address, it is less disrupting than changing the main one you use for correspondence.



`http://` and `https://` are found at the start of a website's address. When giving out credit card details over the Internet, a secure site will display `https://` at the beginning of its address.

**Find out more at [www.makeITsecure.org/identitytheft](http://www.makeITsecure.org/identitytheft)**

# Keeping your Internet Access Secure

While accessing the Internet is never completely secure, there are a few simple steps you can take to protect your PC or device and reduce any risk to your information or data.

## Always use up-to-date anti-virus and anti-spyware software

Computer viruses are small pieces of software that attach themselves to real programs such as word processors or email applications. As well as potentially damaging, copying or stealing your data, they can even replicate themselves and infect other users.

**Spyware** is software that secretly collects and transmits information about you through your Internet connection without your knowledge.

Spyware is a category of small applications that can be downloaded onto your system without your knowledge. It can collect your personal information and send these details back to its originator via the Internet.

Spyware and computer viruses are commonly referred to as malicious software or 'malware'.

**Anti-virus software** is software that you install onto your computer which scans all files and programs for viruses and subsequently removes them.

Anti-virus and anti-spyware software finds and removes malware from your system. Since viruses and spyware are continuously evolving, it is important that you keep your anti-virus and anti-spyware software constantly up-to-date. All anti-virus and anti-spyware applications will provide a way of updating themselves via the Internet.

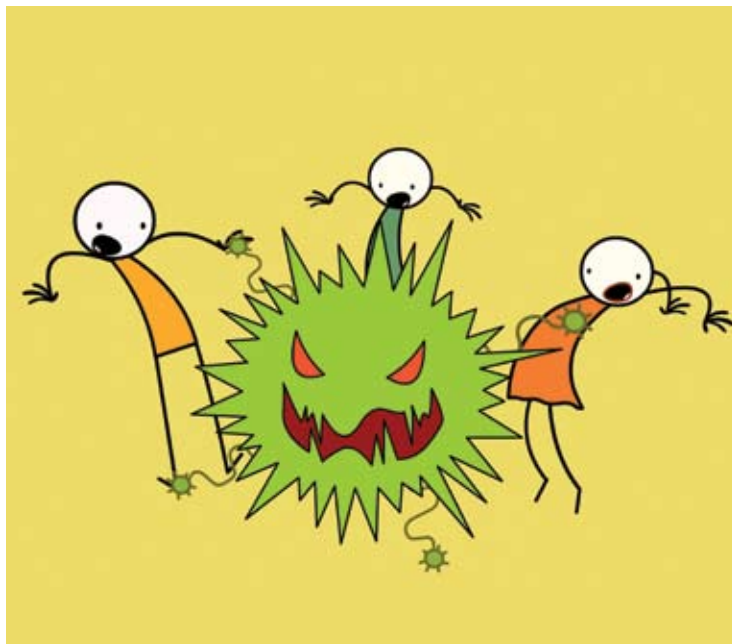
## Always apply trusted application security updates

**Operating Systems** are the software foundation on which computer programs run. Examples of operating systems are, Microsoft® Windows, Linux and Mac OS.

Many programs run on your computer or device including the operating system. This acts as a platform for applications such as word processors, games or Internet browsers.

Since malware is continuously evolving and creating new threats, the application writers are continuously creating security updates to stop the infection from happening.

Therefore, it is vital that you always apply legitimate security



updates offered by the companies who originated the software, to ensure that your system is up-to-date.

## Always use an Internet firewall

An Internet firewall acts like a virtual doorman. It continuously filters data that comes from the Internet onto your computer and only allows data that you have approved, to pass in and out of your system. Most modern operating systems or security software packages will contain a firewall. Always ensure your firewall is switched on whenever you are accessing the Internet.

**Firewalls** are devices or programs designed to prevent unauthorised access to your computer while it's connected to the Internet.

# Top Tips

**Do** use up-to-date anti-virus software, a firewall and anti-spyware.

**Don't** open email attachments if you are suspicious.

**Do** choose 'Yes' to install the latest official security software updates to protect your computer from viruses and phishers.

**Don't** share your password with anyone

**Do** make sure your Internet connection is secure when giving out personal details – look for the padlock icon.

**Do** make back-up copies of your files and store them in a safe place.

**Don't** give out personal banking and credit card details by email.

**Do** mark your profile private on social networking sites.

**Don't** allow your children to meet someone they have only met online without taking you or another adult they trust, along. Not everyone is who they say they are online – people often lie.

**Do** advise your children to be careful when meeting new friends online – if it 'feels wrong', tell them to talk to you or to another adult they trust.

**make it safe • make it simple • makeITsecure.org**



Department of Communications, Energy and Natural Resources  
Roinn Cumarsáide, Fuinnimh agus Acmhainní Nádúrtha



Department of  
**Finance and  
Personnel**

[www.dfpni.gov.uk](http://www.dfpni.gov.uk)

**Microsoft**



Disclaimer: The contents of these pages are provided as an information guide only. They are intended to enhance awareness regarding basic computer security issues. While every effort is made in preparing material for publication, no responsibility is accepted by, nor liability assumed by or on behalf of the Department of Communications, Energy and Natural Resources, Department of Finance and Personnel (NI), 3, Microsoft, Symantec, Irish Banking Federation, BT Ireland, Vodafone, O<sub>2</sub> Ireland, National Centre for Technology in Education, Internet Advisory Board (IAB), RTÉ, eircom, for any errors, omissions or misleading statements on these pages or any website featuring information similar to that contained in this booklet and any links from such a website. Although every effort is made to ensure the reliability of listed sites this cannot be taken as an endorsement of these sites.

