Autumn 2016

Are you as safe as you think?

HELPFUL TIPS

EPA Online Safety Team

--- Featured Advice ---

★Password Security *(Page 1)*
★ Computer Viruses *(Page 2)*
★ Social Networking Sites *(Page 3)*
★ Chatroom Dangers *(Page 4)*

Password Security

How secure is your password?

Did you know?
Most people's passwords are not safe and could easily be cracked in a relatively short space of time by an automated hacking tool.

Creating Strong Passwords

Start with a sentence that you can easily remember, maybe for a personal reason, for example "I drink tea in the morning"

Remove the spaces and use the first character of each word as well as combining upper and lower case letters; "**iDtItM**"

For extra security add numbers e.g. the date: "**iDtItM2409**"

It would be even better if you added symbols as well:

iDtItM#2409

Do's

- Use at least 8 characters
- Use a mixture of UPPERCASE and lowercase letters, numbers and symbols
- Use different passwords for different accounts
- Change sensitive passwords on a regular basis
- Cover the keypad/keyboard whenever you type your password

Don'ts

- Use a dictionary word as your password
- Tell somebody what the password is
- Write it down on a piece of paper
- Use the same password for multiple accounts
- Use standard number substitution like **P455W0RD**

More Information

ConnectSafely
Smart Socializing Starts Here™

http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords

GET SAFE ONLINE
Get Safe Online
Free expert advice

https://www.getsafeonline.org/protecting-your-computer/passwords

PLURALSIGHT

https://www.pluralsight.com/blog/life/password-tips

HOW SECURE IS MY PASSWORD?

https://howsecureismypassword.net

The Password Meter

http://www.passwordmeter.com

Test Your Pas$w0rd

http://www.testyourpassword.com

Computer Viruses

Definition:
A virus is a file written with the sole intention of doing harm, or for criminal activity. There are many types of virus. Viruses and spyware are also known as 'malware'

The Risks
Viruses and spyware can attack your computer via the following means:

- Opening infected email attachments such as .exe files.
- Opening infected files from web-based digital file delivery companies (for example Hightail - formerly called YouSendIt, and Dropbox).
- Visiting corrupt websites.
- Via the internet, undetected by the user (worms are an example of this).
- Macros in application documents (word processing, spreadsheets etc).
- USB connected devices (e.g. memory sticks, external hard drives, MP3 players).
- CDs/DVDs.

Viruses and spyware can cause very serious consequences including:

- Identity theft.
- Fraud.
- Deletion, theft and corruption of data.
- A slow or unusable computer.

Internet security (antivirus / antispyware) software
It is vital to keep your internet security software up to date in order to provide the most complete protection.

Thousands of new viruses are detected every day, to say nothing of the variants of new and existing ones. Each has a set of characteristics or ‘signatures’ that enable internet security software manufacturers to detect them and produce suitable updates.

Most internet security software automatically downloads these updates (sometimes referred to as ‘definitions’) on a regular basis, as long as you are online and have paid your annual subscription (for a paid-for product). This should ensure protection against even the latest virus threats.

Internet security software scans for viruses in a number of different ways:

- It scans incoming emails for attached viruses.
- It monitors files as they are opened or created to make sure they are not infected.
- It performs periodic scans of the files on your computer.

Internet security software will not protect you against:

- Spam.
- Any kind of fraud or criminal activity online not initiated by a virus.
- A hacker trying to break into your computer over the internet.

Choosing internet security software
For personal use there are a number of choices that you can take to decide which internet security software to buy.

Whichever you choose, make sure it is a reputable brand from a mainstream supplier, and get the best you can afford.

Here are a few of the best-known suppliers:

Norton Security Deluxe
https://uk.norton.com

Kaspersky Lab Protection
https://www.kaspersky.co.uk

McAfee Antivirus
http://uk.mcafeestore.com

Sophos Endpoint Protection
https://www.sophos.com/en-us/products/endpoint-antivirus.aspx

AVG AntiVirus
http://www.avg.com/us-en/free-antivirus-download

Avast Free Antivirus 2016©
https://www.avast.com/en-gb

Social Networking Sites

What is social networking?

Social networking is a global revolution, enabling over a billion people worldwide to stay in touch with their friends, share experiences and photographs and exchange personal content. In many ways it has replaced the telephone and email. For many users, it has become a way of life.

Various social networking sites are also valuable tools used by many companies and individuals to extend their contacts and deliver marketing messages.

The nature of social networking – having such a massive base of users who are unknown to you – means that using it carries a degree of risk including becoming a target for cyber-criminals.

The Risks

- Disclosure of private information by either yourself or friends / contacts.
- Bullying.
- Cyber-stalking.
- Access to age-inappropriate content.
- Online grooming and child abuse.
- Encountering comments that are violent, sexual, extremist or racist in nature, or offensive activities and hateful attitudes.
- People trying to persuade or harass you into changing your basic beliefs or ideologies, or adopt an extremist stance.
- Prosecution or recrimination from posting offensive or inappropriate comments.
- Phishing emails allegedly from social networking sites, but actually encouraging you to visit fraudulent or inappropriate websites.
- Friends', other people's and companies' posts encouraging you to link to fraudulent or inappropriate websites.
- People hacking into or hijacking your account or page.
- Viruses or spyware contained within message attachments or photographs.
- You or a family member posting that you're away or going away on holiday and therefore advertising that your home is empty, leaving the way open for burglars. If you do so and you make an insurance claim for a burglary while you are_away, your insurance company may well reject it for this reason.

You can avoid these risks and enjoy using social networking sites by following a few sensible guidelines:

- Be wary of publishing any identifying information about yourself – either in your profile or in your posts – such as phone numbers, pictures of your home, workplace or school, your address or birthday.
- Pick a user name that does not include any personal information. For example, "rob_romford" or "dagenham_dave" would be bad choices.
- Keep your profile closed and allow only your friends to view your profile.
- Use strong passwords.
- Set up a separate email account to register and receive mail from the site. That way if you want to close down your account / page, you can simply stop using that mail account.
- What goes online stays online. Do not say anything or publish pictures that might later cause you or someone else embarrassment.
- Never post comments that are abusive or may cause offence to either individuals or groups of society.
- Learn how to use the site properly. Use the privacy features to restrict strangers' access to your profile.
- Don't post your holiday dates - or family photos while you are away - as social networking sites are a favourite research tool for the modern burglar.
- Ensure you have effective and updated antivirus/antispyware software and firewall running before you go online.

More Information

For more advice on using social networking sites safely, visit the ThinkuKnow site.

https://www.thinkuknow.co.uk

Or visit the social networking sites' own online safety pages:

Facebook
Twitter
Bebo
Myspace
YouTube
Instagram

Chatroom Dangers

Most children now chat daily either online or via their mobile phone. They are connecting to a huge community of other children all over the world. Some are shy 'in real life' but socialise with confidence online, others find support from people of their own age on relationship issues, or problems at home such as divorce and family bereavement.

Children and the internet

The online world, just like the real world, can introduce problems, such as bullying or arguments. Going online is great fun, but there are also a few people who use the internet for offensive or illegal purposes. Children must be made aware of both the good things and the dangers.

To keep children safe, supervision must cover the family computer. Parents should chat with their children and agree which websites are suitable, and chatrooms or chat application they can visit or use.

It is important to convince and remind children that online friends are still strangers. The number of known cases where Paedophiles have approached children online is extremely low, but reminding children of the risks, will keep them alert.

TEENS MESSAGE BOARD

Topic – Love

Dealing with fake messages wastes time that could be spent helping those in real need. Please consider this when posting.

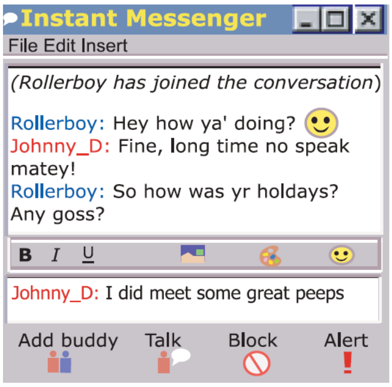
Internet chat – getting technical

The language of chat is strange to many parents too, chatters love to use abbreviations such as:

atb	all the best
bbfn	bye bye for now
cul8er	see you later
gr8	great!
idk	I don't know
imbl	it must be love
kit	keep in touch
paw	parents are watching
lol	laugh out loud
xlnt	excellent!

Instant messaging

The instant messaging is another chat facility used by many children. It is a safer facility than chatrooms as you can build up a 'buddy' list of trusted friends who you allow to chat with you, or who ask you if they can be put on your list of recommended friends. 'IM', as it is more commonly known, flashes an alert and opens a window when someone 'calls' you to chat.



(Rollerboy has joined the conversation)

Rollerboy: Hey how ya' doing?

Johnny_D: Fine, long time no speak matey!

Rollerboy: So how was yr holdays? Any goss?

Johnny_D: I did meet some great peeps

Parents should be aware that IM chats create conversation logs which can used as evidence if cyberbullying is encountered.

What parents and carers can do

Whether children are chatting via the internet or mobiles, they should learn how to chat safely. Families should be encouraged to spend time together discussing both the good things and the problems of chatrooms and IM tools. This will significantly reduce any risks. If children are aware of the dangers and agree to abide by some agreed rules for online activity, they'll know what to do to stay safe.

For extra security and peace of mind, parents can add filtering software that prevents children entering sites you would not wish them to see; however filters may need updating from time to time and also may block sites that are ok. The most effective tool of all is common sense.

Parents should encourage their children to let them know if they experience anything which might make them feel angry, upset or uncomfortable during an online conversation. Incidents can be reported to your service provider.

Top tips

Browse together - Play and explore online with your child so you know which websites they like to visit and can talk about them together.

Keep it public - It's a good idea to keep all devices that have access to the internet in a family space so you can be involved and talk about what your child is doing.

Keep it private - Impress on your children that they should not give out personal information without checking with you first.

More Information

https://www.thinkuknow.co.uk/Parentsold/SafeUse