THE DUSTON SCHOOL 4-19

Knowledge Organiser

Computing

Year 8 Term 1 E-Safety

Enquiry Question

What are the dangers of not knowing how to be safe online?

Big questions that will help you answer this enquiry question:

1. Do you know the dangers of social media?
2. Can you list the rules the school have for using the internet?
3. Do you understand the risks of posting inappropriate content on the internet?
4. What are some of the dangers with sharing personal information online?
5. If you felt/fell uncomfortable about anything you saw, or if anybody asked you for your personal details on the internet, do you know where to go for help?
6. Would you meet up with people you have met online?
7. Would you befriend people you don't know?
8. Why are privacy settings important?
9. If anybody sent you a hurtful message on the internet or on your mobile phone, do you know who to tell?
10. What is a phishing email?
11. What is a virus?
12. What is a Trojan?
13. What do you do with an email from an unknown person?

Keywords

Terminology you need to know!

Keywords:

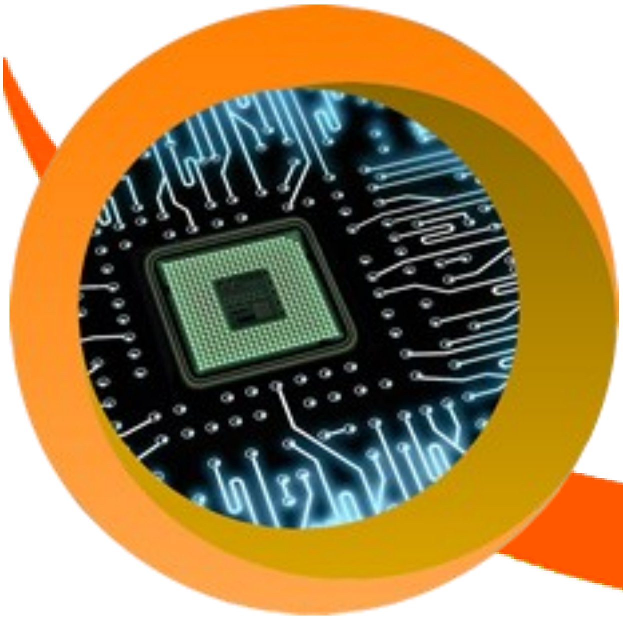
The Good:

Firewall A system that prevents unauthorised access to a computer over a network, such as the internet. Firewalls can be either hardware or software businesses tend to use the former; home users the latter.

Netiquette A term referring to good behaviour while connected to the Internet. Netiquette mainly refers to behaviour while using Internet facilities such as individual Web sites, emails, newsgroups, message boards, chat rooms or Web communities. Teach your pupils 'netiquette'!

Password A word or series of letters, numbers and punctuation that only you know, which you use to log on to computers, networks or online services.

Filtering Software or hardware product designed to prevent access to inappropriate websites on the internet. It does this by denying or allowing access based on lists of pre-classified addresses, or by examining the web data for keywords or unwanted content.



Anti Spam Computer program that puts into action anti-spam/spim/spit techniques.
Anti Virus Software Application designed to protect PCs from malicious computer code (virus)

Keywords

Terminology you need to know!

Keywords:

The Bad:

Cyberstalking Using information and communication technology, particularly the Internet, to harass an individual, group of individuals or organisation.

Grooming The actions undertaken by a paedophile to befriend and establish an emotional connection with a child in order to lower the child's inhibitions in preparation for sexual abuse and/or rape. Paedophiles may initiate online conversations with potential victims to extract information about location, interests and sexual experiences.

Hacking Slang term used to describe illegal access of computer systems by unauthorised users.

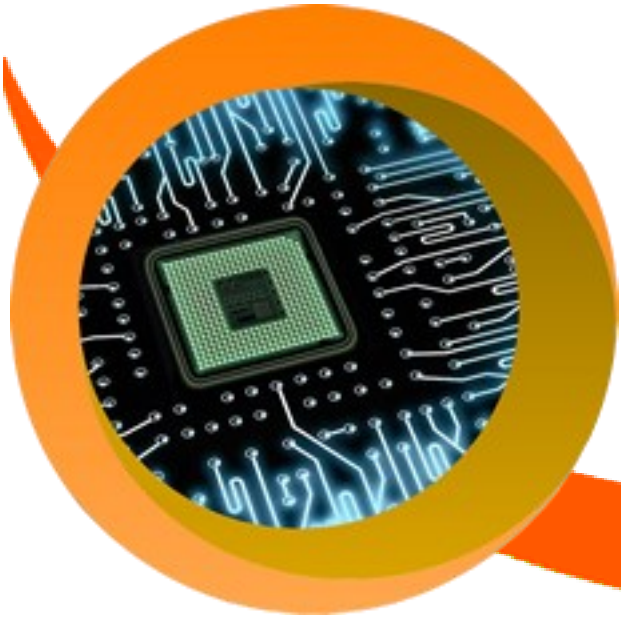
Identity Theft The practice of stealing personal details (e.g. name, birth date, credit card number) and using them illegally.

Malware Malicious software that is designed to infiltrate or damage a computer system without the owner's informed consent. It includes computer viruses, worms.

Phishing The criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Spyware usually installs itself on the computer and monitors activity in order to send private information to third parties.

Trojan A computer program that takes control of the computer it is installed upon without the knowledge of the owner and is designed to access or damage sensitive data.



- **Virus** A computer program which distributes copies of itself without permission or knowledge of the user. Viruses often hide themselves inside other programs.

Worm A special type of virus that is self-replicating and can spread across many computers and harm networks, consume bandwidth and shut computers down. And the 'it really depends on how you use it'!!

Knowledge

What are the dangers of not knowing how to be safe online?

Gaming

What's the big deal?
Do you enjoy playing games online? Chances are, if you don't, you know somebody who does. The gaming industry is huge! Did you know that around the world, more money is spent on games than on the film industry?

Multiplayer magic
With the internet, it is now possible to play with dozens, even hundreds of people at the same time through online games like World of Warcraft, Clash of Clans or gaming portals like Miniclip.

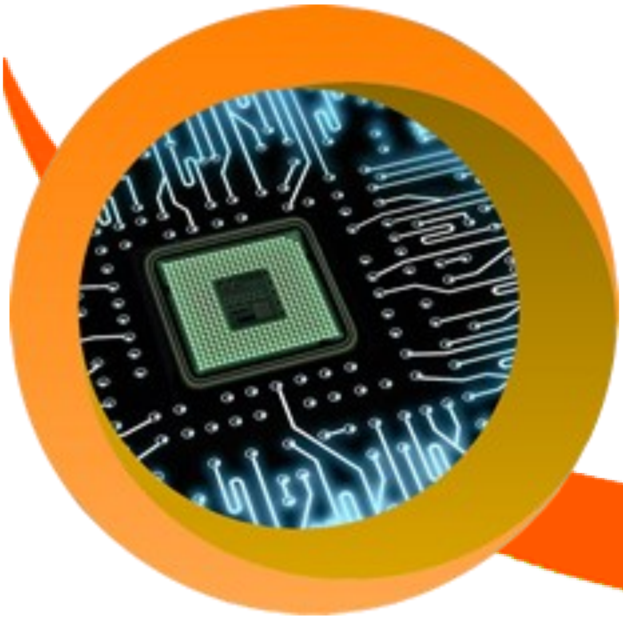
Being able to game with people all over the world makes online gaming even more exciting and with the ability to 'chat' in these games, it is easy to 'make friends' with the people you play with.

Just like in the real world though, you need to be careful when playing with strangers. Some people you meet online may not be very nice!

Are you worried about someone you've met in an online game?
Is someone being weird with you in a game? Talk to an adult you trust or get help from CEOP .

Report it!
CEOP helps young people who are being sexually abused or are worried that someone they've met is trying to abuse them.

If you've met someone online, or face to face, and they are putting you under pressure to have sex or making you feel uncomfortable you should report to CEOP.



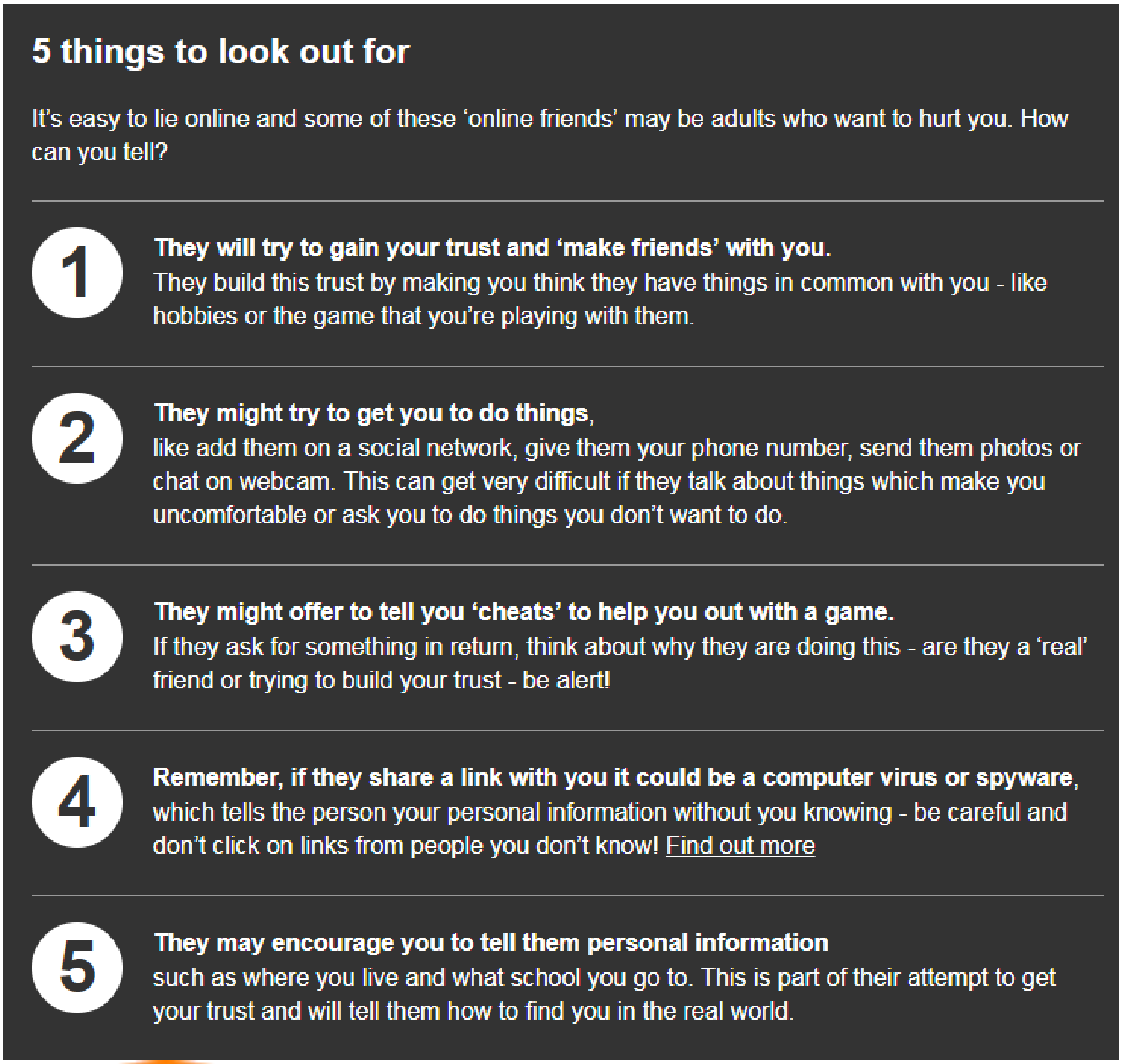
This might be someone:

- Making you have sex when you don't want to
- Chatting about sex online
- Asking you to meet up face to face if you've only met them online
- Asking you to do sexual things on webcam
- Asking for sexual pictures of you
- Making you feel worried, anxious or unsafe

If this is happening to you, or you're worried that it might be, you can report this to CEOP.

Knowledge

What are the dangers of not knowing how to be safe online?



5 things to look out for

It's easy to lie online and some of these 'online friends' may be adults who want to hurt you. How can you tell?

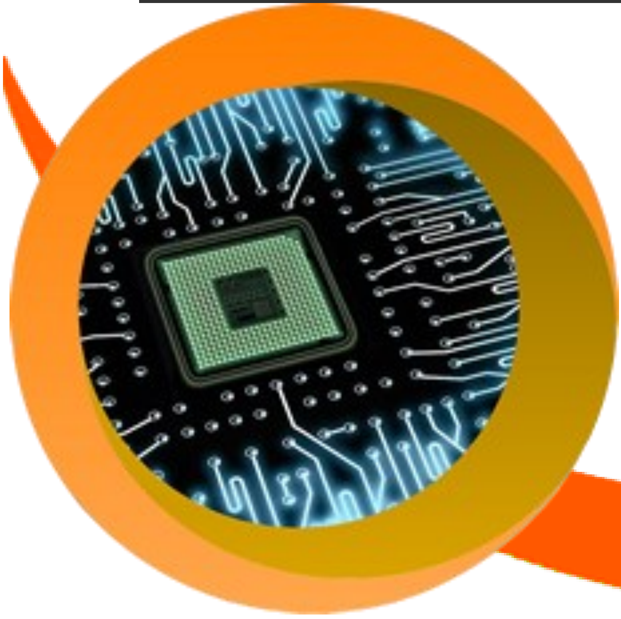
1 **They will try to gain your trust and 'make friends' with you.**
They build this trust by making you think they have things in common with you - like hobbies or the game that you're playing with them.

2 **They might try to get you to do things,**
like add them on a social network, give them your phone number, send them photos or chat on webcam. This can get very difficult if they talk about things which make you uncomfortable or ask you to do things you don't want to do.

3 **They might offer to tell you 'cheats' to help you out with a game.**
If they ask for something in return, think about why they are doing this - are they a 'real' friend or trying to build your trust - be alert!

4 **Remember, if they share a link with you it could be a computer virus or spyware,**
which tells the person your personal information without you knowing - be careful and don't click on links from people you don't know! Find out more

5 **They may encourage you to tell them personal information**
such as where you live and what school you go to. This is part of their attempt to get your trust and will tell them how to find you in the real world.



Knowledge

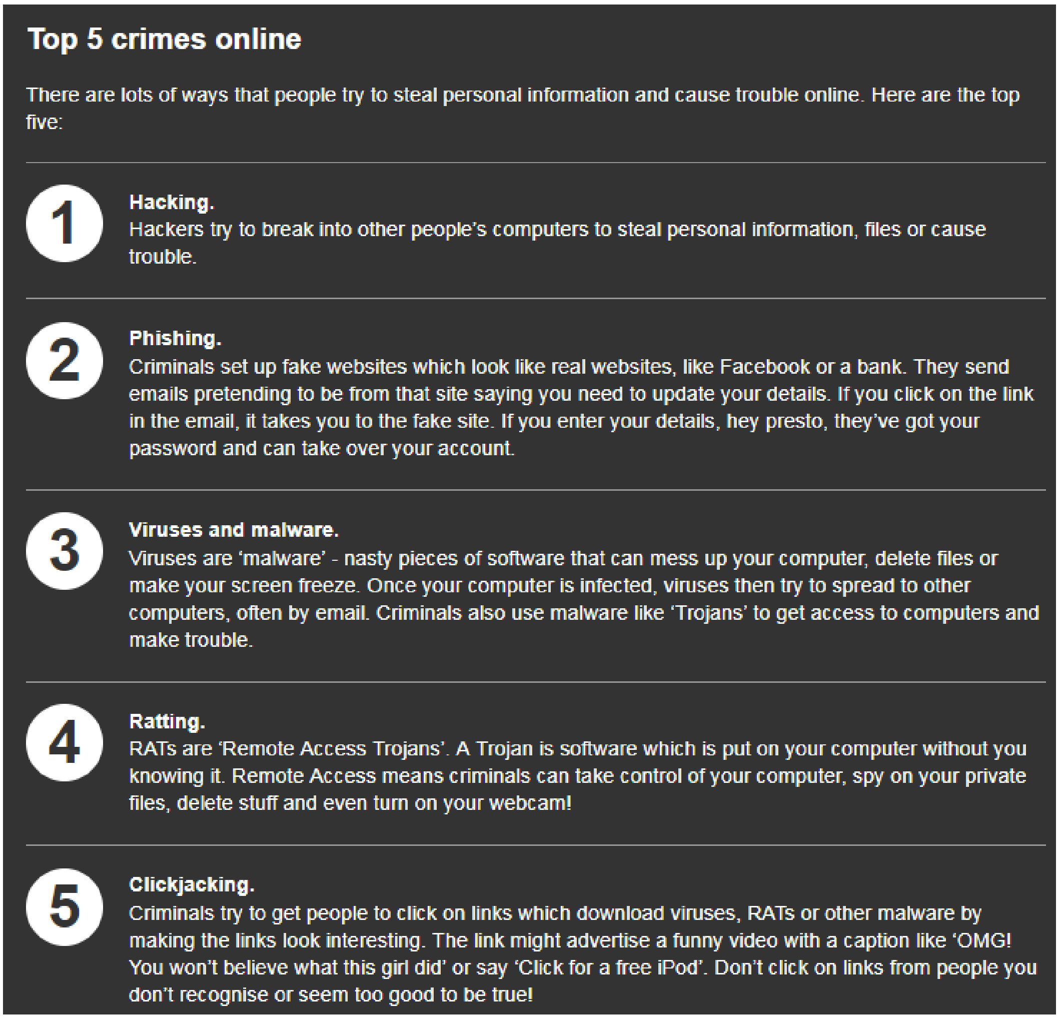
What are the dangers of not knowing how to be safe online?

Online Bullying

Lock up your loot

Just as you wouldn't leave your front door or windows open, you shouldn't leave your computer or phone unlocked.

Your computer, tablet and phone hold loads of information about you. Your name, address, birthday, a list of your friends, hobbies, text messages, private photos and videos. What else might be on there? All of this is personal information which you need to keep secure. It's valuable to you and to criminals. Make sure you keep it locked up!



Top 5 crimes online

There are lots of ways that people try to steal personal information and cause trouble online. Here are the top five:

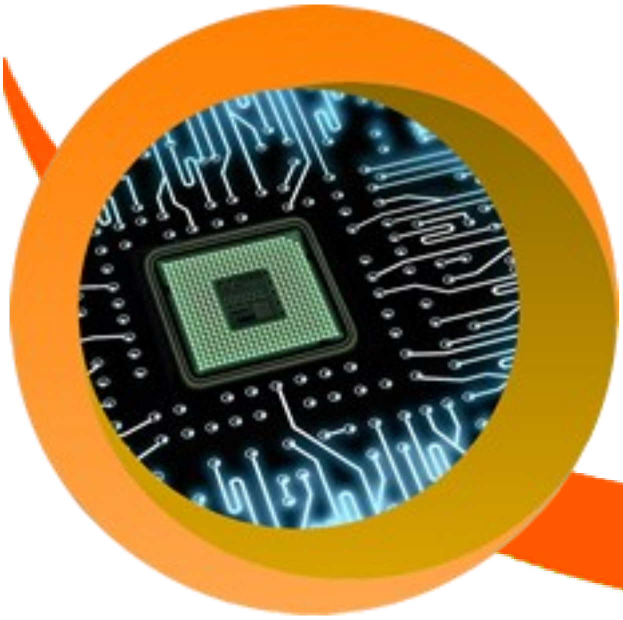
1 **Hacking.**
Hackers try to break into other people's computers to steal personal information, files or cause trouble.

2 **Phishing.**
Criminals set up fake websites which look like real websites, like Facebook or a bank. They send emails pretending to be from that site saying you need to update your details. If you click on the link in the email, it takes you to the fake site. If you enter your details, hey presto, they've got your password and can take over your account.

3 **Viruses and malware.**
Viruses are 'malware' - nasty pieces of software that can mess up your computer, delete files or make your screen freeze. Once your computer is infected, viruses then try to spread to other computers, often by email. Criminals also use malware like 'Trojans' to get access to computers and make trouble.

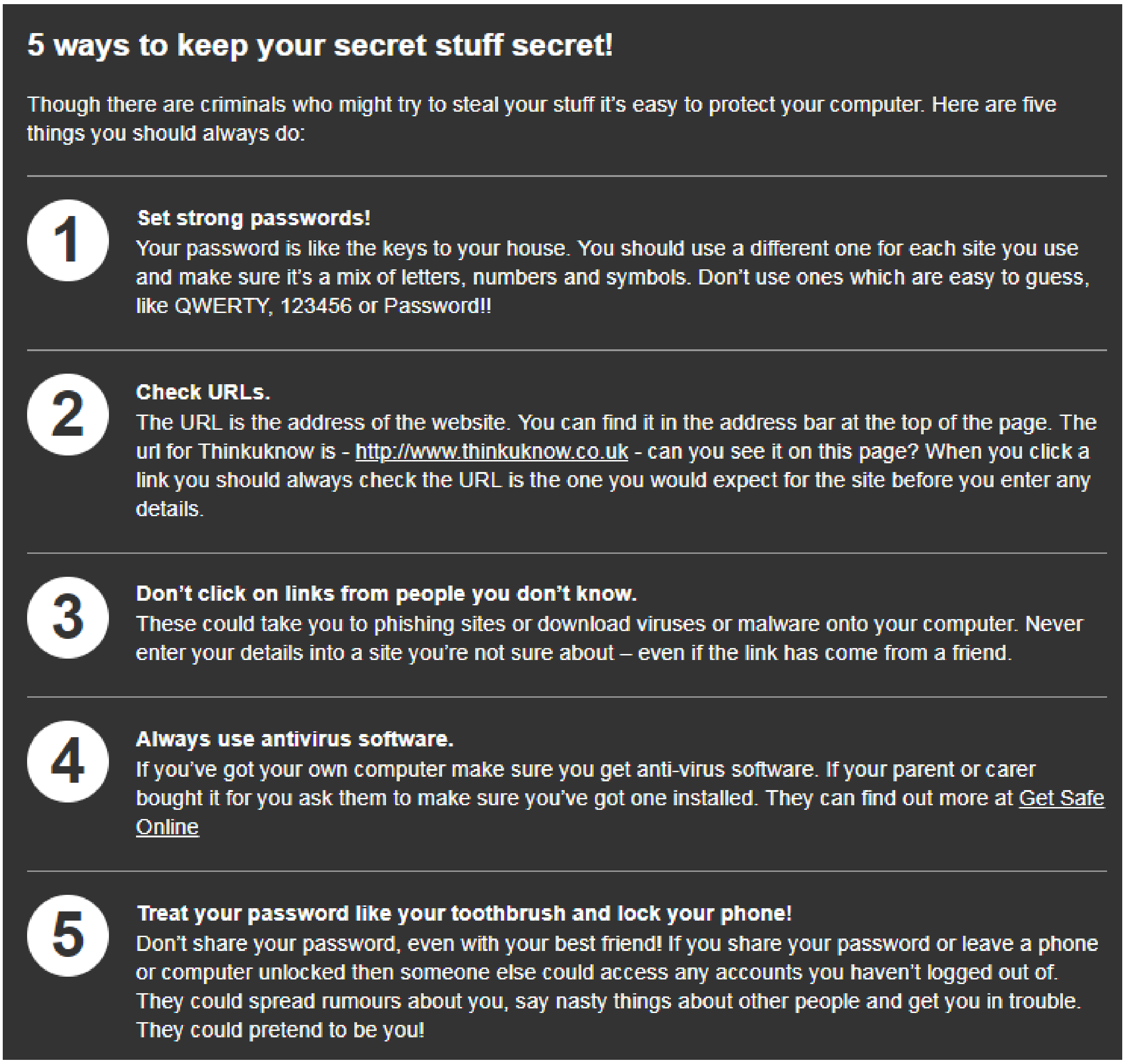
4 **Ratting.**
RATs are 'Remote Access Trojans'. A Trojan is software which is put on your computer without you knowing it. Remote Access means criminals can take control of your computer, spy on your private files, delete stuff and even turn on your webcam!

5 **Clickjacking.**
Criminals try to get people to click on links which download viruses, RATs or other malware by making the links look interesting. The link might advertise a funny video with a caption like 'OMG! You won't believe what this girl did' or say 'Click for a free iPod'. Don't click on links from people you don't recognise or seem too good to be true!



Knowledge

Digital Footprint and online safety.



5 ways to keep your secret stuff secret!

Though there are criminals who might try to steal your stuff it's easy to protect your computer. Here are five things you should always do:

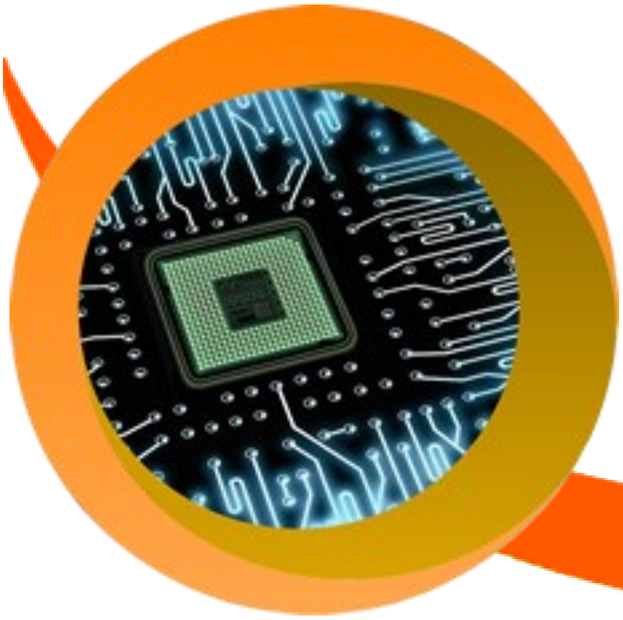
1 **Set strong passwords!**
Your password is like the keys to your house. You should use a different one for each site you use and make sure it's a mix of letters, numbers and symbols. Don't use ones which are easy to guess, like QWERTY, 123456 or Password!!

2 **Check URLs.**
The URL is the address of the website. You can find it in the address bar at the top of the page. The url for Thinkuknow is - http://www.thinkuknow.co.uk - can you see it on this page? When you click a link you should always check the URL is the one you would expect for the site before you enter any details.

3 **Don't click on links from people you don't know.**
These could take you to phishing sites or download viruses or malware onto your computer. Never enter your details into a site you're not sure about – even if the link has come from a friend.

4 **Always use antivirus software.**
If you've got your own computer make sure you get anti-virus software. If your parent or carer bought it for you ask them to make sure you've got one installed. They can find out more at Get Safe Online

5 **Treat your password like your toothbrush and lock your phone!**
Don't share your password, even with your best friend! If you share your password or leave a phone or computer unlocked then someone else could access any accounts you haven't logged out of. They could spread rumours about you, say nasty things about other people and get you in trouble. They could pretend to be you!



Homework

What are the dangers of not knowing how to be safe online?

Homework for week 1 and 2

Question! Imagine all your status updates that you ever put on social media, suddenly became public via a search engine like Google.

How would you feel?

Write a short account of your feelings and the impact it will have on your social life.

Your written piece must be at least 1/2 a page to 1 whole page of A4.

Homework for week 3 and 4

Answer the following questions. Write your answers on an A4 page.

1. What is a computer virus?

2. In some ways a computer virus is similar to viruses that give you coughs and colds. Why might that be?

3. Do computer viruses damage the actual computer equipment?

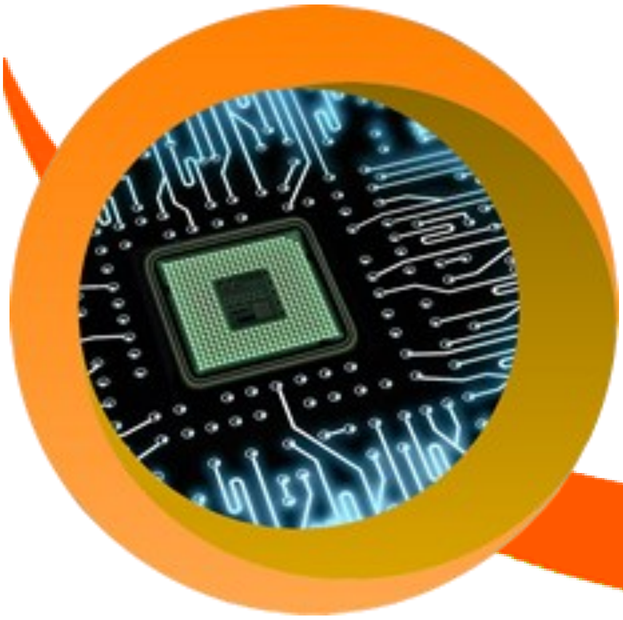
4. What harm can computer viruses cause?

5. How is it possible to introduce a computer virus to your computer?

6. If you receive an email with links, what questions should you ask yourself before opening it?

7. How could you know if your computer had a virus?

8. If you do get a virus on your computer, what steps can you take to remove it?



Homework

What are the dangers of not knowing how to be safe online?

Homework for week 5 and 6

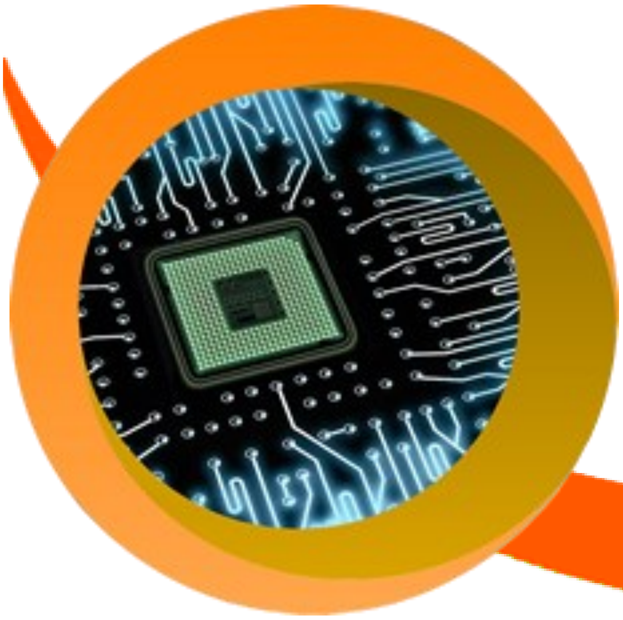
News Bulletin: Passwords

There have been a lot of news stories recently about the issue of **password security**

News 24, the 24 hour news channel, have decided to run a five minute human interest story about this issue in their lunchtime bulletin.

You are to work in groups of 4-5 to research, write and present the news bulletin.

Role	Purpose
Newsreader	To introduce the story and ask questions
Businessman	To explain how difficult it has been to get their staff to choose secure, yet memorable passwords
Teenager	To discuss what happened when an ex-friend used their password to access their school and online accounts
Expert	To explain why password security is so important and how to choose memorable passwords
Researcher (if working in groups of 4 this role can be left out)	Ensures facts are correct. Finds images to show on the screen whilst the interviews are taking place



Be prepared to act out your news bulletin to the rest of the class.