What do I do if I am worried?

If you are worried about something you have seen online, something you have clicked on or been sent, or something that someone has said to you or asked you to do online, you should speak to an adult that you trust.

If you don't feel comfortable speaking to someone, you can seek help online.

On the back of this leaflet there are some useful websites and contacts that you can use to talk about, or report, anything that you are worried about.

You should always tell someone if you think you have been scammed or if you have been approached by a stranger asking for money or personal information.

Useful websites and contacts

Childline – 0800 1111

No matter what is on your mind, Childline will be there to support and guide you, and help you to make decisions that are right for you. If you would prefer not to call, you can visit their website at www.childline.org.uk.

Thinkuknow

If you want to report something that you are worried about, visit www.thinkuknow.co.uk – the website has lots of helpful advice about having fun safely, games and more.

Action Fraud – 0300 123 2040

Action Fraud has created an easy-to-use, 24-hour online reporting tool, which can be found at www.actionfraud.police.uk. This tool can be used to report any incidents of fraud or cybercrime.

The Mix – 0808 808 4994

The Mix is a free, confidential helpline for people under 25. It is open 11am-11pm every day and you can call or chat online at www.themix.org.uk.

March 2023

William Gilbert C of E Primary School

Cyber Crime – Protecting yourself online

Why is it important?

We all like to use the internet and talk to others online, but do you know the rules you need to follow to keep safe?

There are many risks from using the internet. Some of these include cyber bullying, grooming, breaching privacy and losing personal information, but there are many more.

Staying safe online isn't just important for you – when using sites, you need to think about what you're saying about, or to, other people.

Ask yourself:

- Do you know how to protect yourself and others online?
- Do you know what the risks are?
- Do you know what to look out for?
- Do you know who to report concerns to?

What is fraud?

Fraud is a word used to describe types of crime, like the ones listed below:

- Selling fake concert tickets online.
- Allowing criminals to send money through your bank account.
- Using your parents' bank details to pay for online shopping without them knowing.
- Illegally downloading or listening to music.
- Hacking someone's computer to find out their personal information.
- Using someone else's personal details instead of your own.

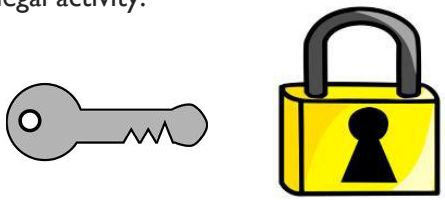
What are the consequences of fraud?

Fraud is illegal, so if a person commits or assists in fraudulent activity, they could face the following:

- Police investigations
- Paying money back that you have gained
- Having your online seller accounts shut down
- Having your details kept by banks, police and anti-fraud agencies, which can make it harder to take out loans or credit cards in the future
- A criminal record
- Difficulty applying for a phone contract or mortgage in the future
- Difficulty with getting a job

Protecting yourself from fraud

Protecting yourself from online fraud can be easy and the more aware of the risks you are, the less likely you are to be drawn into illegal activity.



Some of the ways you can protect yourself include the following:

- Never posting pictures of yourself wearing your school uniform on social media
- Making sure you only enter your bank details on genuine websites – look for the padlock in the left-hand corner of the search bar; you can ask friends or relatives for their opinion if you are unsure, or do an internet search
- Never buying things online or using online banking while you are on public Wi-Fi
- Setting your social media profiles so that only your friends can view your posts
- Renewing your anti-virus software as soon as it runs out (ask your parents about this if you are unsure)
- Asking before using someone else's personal information
- Password protecting your phone and computer – passwords should be least 10 characters long and use numbers, letters and special characters, and you should use different passwords for every account you have
- Never giving out your personal details or displaying them on your social media profiles

Money mules

A money mule is the name used to describe someone who transfers stolen money, usually through their own bank account for someone else. Young people are in danger of becoming money mules so it is important that you can recognise when others are using manipulation and persuasion, and how you should respond.

Criminals will target vulnerable people by befriending them first and making it seem like you have a lot in common and that they are there for you. They might then ask if you can look after money for them, using pressure techniques that make an offer hard to resist – these can progress to blackmail or other threatening behaviour.

A lot of the time, if something seems too good to be true then it is. Criminals will also send out fake emails; these can be identified where:

- The email is addressed to your email, not your name.
- You never applied for the job being offered, or entered the competition you have 'won'.
- Time pressure has been used to encourage you to respond quickly.
- It doesn't look official.
- There are spelling and grammar mistakes throughout.