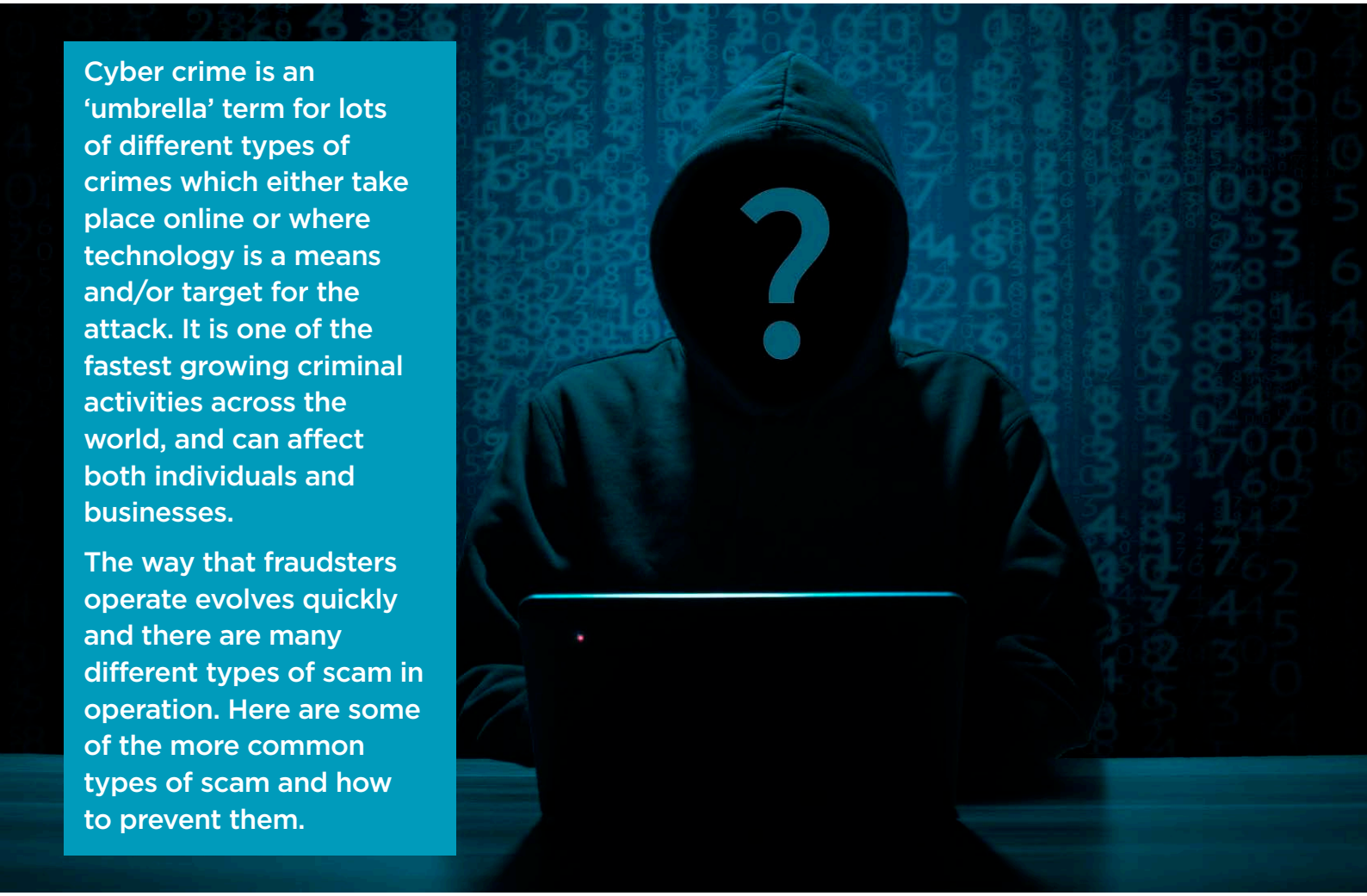
Police Mutual
We look after our own

Let's Talk 19

JULY 2021

Cyber Crime



Cyber crime is an 'umbrella' term for lots of different types of crimes which either take place online or where technology is a means and/or target for the attack. It is one of the fastest growing criminal activities across the world, and can affect both individuals and businesses.

The way that fraudsters operate evolves quickly and there are many different types of scam in operation. Here are some of the more common types of scam and how to prevent them.

Identity Fraud - is increasingly prevalent and can occur via phone, online, mail and in person and involves the fraudster trying to get hold of someone's personal information such as bank account numbers, dates of birth, address details etc. This information is then used to either access the victim's bank accounts or else obtain credit.

The consequences of being targeted in this way go much wider than the actual fraud activity itself and it can take a lot of time to deal with what has happened in terms of updating passwords, dealing with banks etc.

In order to reduce this type of fraud you need to regularly check your bank statement for any suspicious transfers, shred any mail that include any personal details and never disclose any PINs to anyone you don't trust. You can also sign up to the Mail Preference Service and the Telephone Preference Service to prevent marketing letters and calls.

Online fraud - has evolved quickly and takes many forms. It can be an email purporting to be from a bank or another trusted provider asking the user to input their password or account details. These emails look authentic but are operated by scammers who use the details to take money from the targeted person's bank account.

You may have received emails from someone you do not know offering to put money in your account if banking details are sent. Even if such emails do not explicitly ask for banking details they may contain attachments which, if clicked on, will infect the computer with a virus that can make personal data available to fraudsters. Another widespread fraud is for someone to receive an email supposedly from someone they know saying they need money urgently.

Other instances of online fraud may relate to bogus websites offering services/products. The purchaser hands over their bank details for services/products that don't arrive and the fraudster now has their bank details.

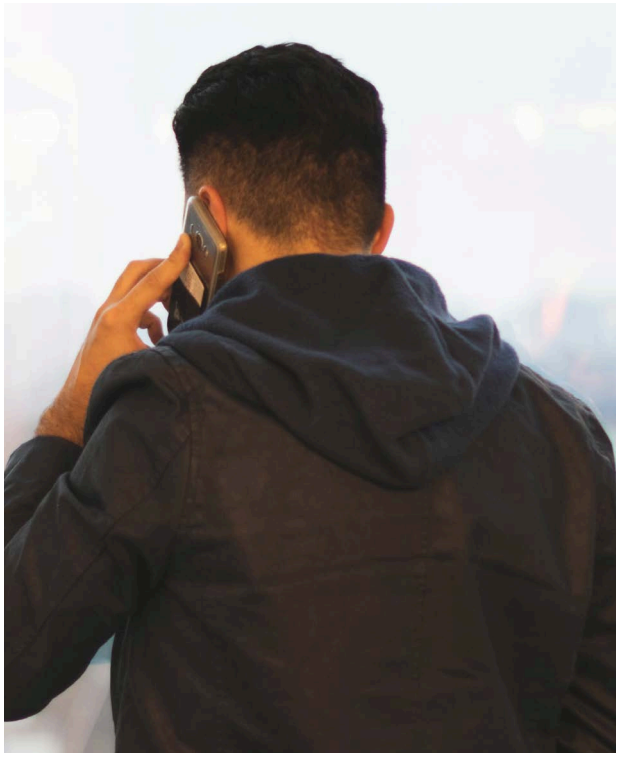
In order to reduce this type fraud, if you shop online or use online banking, then ensure you have anti-virus software installed on your computer. Delete any suspicious or unsolicited emails or texts you receive, don't reply to them and ensure you check your bank statements regularly to see if there have been any suspicious transfers.

Investment Scams – you may be contacted by someone offering an investment apparently generating high returns and often located overseas. The seller is likely to try and pressure someone into making a quick decision.

Beware of unsolicited contact from firms whether it be via letter, text, phone call or people coming to your door offering services such as free pension reviews. Regulated financial advisers or services such as Citizens Advice would not contact someone directly.

If you are offered an exciting new investment opportunity. It could be based overseas, have "guaranteed" returns or else promise unusually high returns. It's important to bear in mind that if something sounds too good to be true then it usually is.

No financial adviser would pressure their client into making an investment decision. If you feel you are being pressured either put the phone down/ leave the meeting/ ask the person to leave. Many people do not want to appear rude but if they are being put under pressure they should terminate the conversation.



All incidents should be reported to Action Fraud (see details at the end of this guide).

Mass marketing fraud - We have all received mail from agencies telling us we have won a prize in a draw that we don't remember entering. All you need to do to claim said prize is to send in some money and the prize will be released.

Another popular scam is to offer services or items which must be paid for upfront. However, these prizes, services or items never materialise, or else when delivered they are not of the promised quality.

These letters can look very authentic and many people decide to send in the money but their prize never arrives. These scams are particularly harrowing in terms of the effects the scammers can have on their victims. There are many instances of victims being effectively brainwashed into believing what the scammers tell them.

Property scams - This is a growing threat affecting the many buy-to-let landlords in the UK. These scams, known as property hijacking, involve scammers putting themselves forward as tenants so they can commit identity theft and try and sell the property from under the owner's nose.

The scammers will use fake IDs to act as tenants before changing their names by deed poll to match that of the owner. The scammer then uses fake documentation to put the property up for sale with a request for cash buyers. These potential buyers will then be pressurised into making a quick sale as this leaves less time for the scam to be discovered.

The owner is likely to find out what has happened when the buyer's solicitor attempts to register the change of ownership with the Land Registry. This is then the beginning of a long and complex process while the real owner attempts to unwind what has been done and get their property back.

Landlords can register for a free alert service provided by the Land Registry which lets them know of any activity linked to one of their properties. This would include any attempt to change ownership details. Up to ten different properties can be monitored on one account. All you need is a valid email address and the full address/es of the properties owned.

Go to **https://propertyalert. landregistry.gov.uk** to set up an account.

Courier fraud - Again, this type of fraud is growing rapidly. The victim is called by someone purporting to be from their bank or even a police officer to say they have noticed fraudulent activity on a bank account and need their assistance in finding the culprit.

The victim will then be asked to either disclose their PIN over the phone and the fraudster will then send a courier around to pick up the bank card to be used as evidence. Once in possession of the bank card then the fraudster can start to take money from the account.

Another popular bogus story is that the victim's bank card is about to expire and to save them the trouble of handing it in at their local branch the bank will send a courier to the person's house to collect it.

The courier despatched to pick up the items may have no idea they are involved in fraudulent activity. Don't hand you card over.

Instances should be reported to Action Fraud but if they are feeling in any way intimidated or frightened then they should not hesitate to call the police.

Advance loan fee fraud - This scam involves being asked for an upfront fee in order to get accepted for a loan. The fee can be between £25 and £450 and you may be asked to pay it by bank transfer, Western Union or even iTunes vouchers. No matter how much you pay, the loan never materialises.

Warning signs to look for include being contacted by text or email out of the blue, or being put under pressure to pay the fee quickly.

You can protect yourself by checking that the firm that asks for an upfront payment is authorised by the FCA. Simply type the firm's name into the FCA's Register.

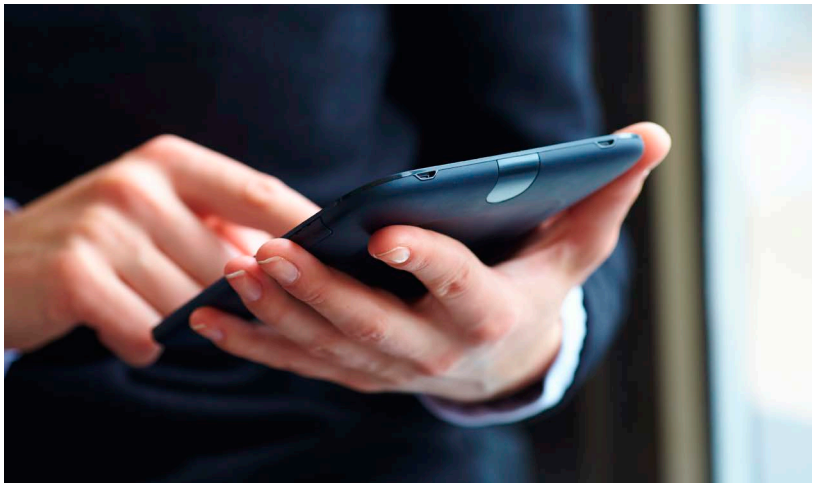
Good cause scams - Criminals have also been targeting people with a number of scam emails asking for donations to good causes. For example, one convincing-looking email pretends to be from the government, and asks for money for the NHS. Others appear to come from an organisation that claims donations will go towards the production of hand sanitiser or protective equipment for the NHS.

Don't download attachments or click on links in emails unless you're sure who sent them. Even if the email is from an organisation you know, if the email itself is unexpected or asks you to click on a link, it could be a scam. That's especially true if it asks for personal or financial information. Your bank will never ask you for personal information in an email.

You can reduce the risk of being scammed by only donating to legitimate charities. You can search for a registered charity in England and Wales on the Gov.uk website charity register. If you're in Scotland, check the Scottish Charity Regulator's website. In Northern Ireland, it's the Charity Commission for Northern Ireland.

Number spoofing scams - Number spoofing is where a scammer sends a text message that looks like it's come from a genuine organisation, such as the government, HM Revenue and Customs or your bank. These scams are very hard to spot especially as the messages will sometimes appear in a chain of otherwise genuine text messages.

Don't click on any link in a text that appears to come from a legitimate source. HMRC doesn't issue tax rebates by text, and banks don't ask for personal information this way.



Clone firm scams - This is where scammers pretend to be from an FCA-authorised firm to try and convince you they are genuine. A firm needs to be authorised by the Financial Conduct Authority to sell, promote or advise on the sale of shares or investments (including pensions) in the UK.

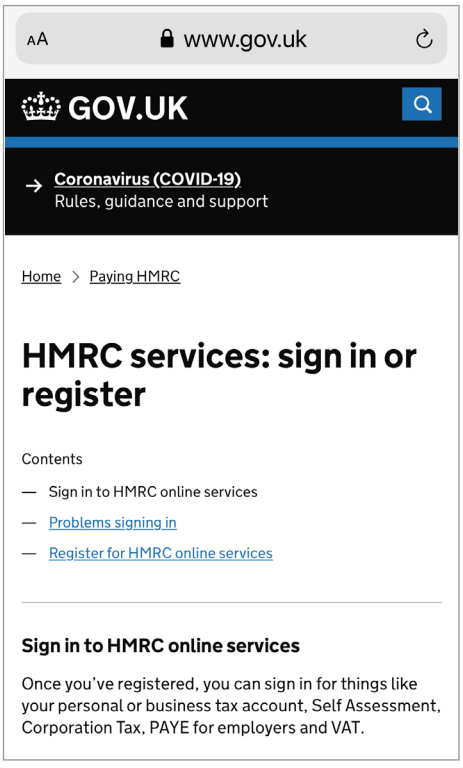
These fraudsters set up websites that use names similar to those of legitimate firms, and typically cold-call you to promote worthless or non-existent shares, property or investment opportunities.

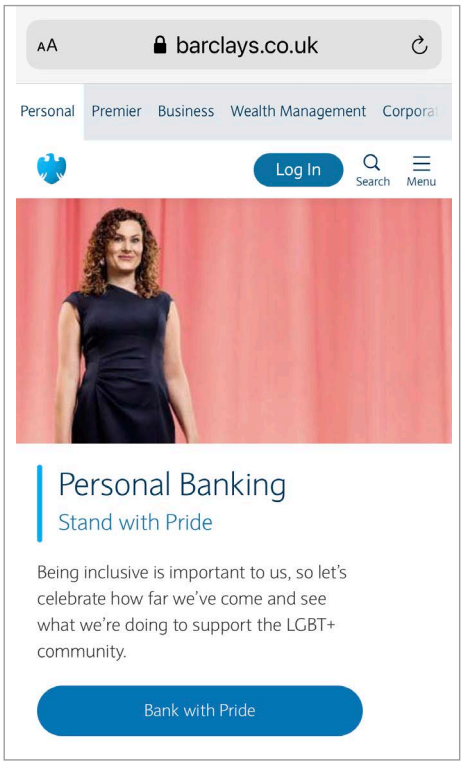
Protect yourself by checking the FCA register to see if the firm is authorised. Always access the FCA's Register directly from register.fca.org.uk rather than from any links sent to you by the firm itself.

The FCA also recommends using the switchboard number given on the FCA Register to call the firm back rather than the one the firm gives you. If the firm claims the number on the register is out of date, contact the FCA's Consumer Helpline on **0800 111 6768.**

Lookalike websites - There's been a sharp increase in the number of people visiting the websites of debt advice charities since the government introduced coronavirus measures, and scammers are taking advantage of this. They are advertising websites that offer debt advice.

These sites have very similar names to the genuine services and charities. They're not illegal, but you could end up paying for debt advice that you could get for free. And you may end up sharing your personal details with a company you don't know anything about.





If you're visiting a website to get debt advice, always check the website address to make sure you're not clicking on a 'lookalike' site by mistake.

Looking after your children online

Our children have grown up using the internet from a young age, they probably use it every day to play games, watch videos, learn and do research, and connect with friends.

It's important to help them to use the online world in a way that's safe and positive for their mental health and to start to have conversation about being online from a young age and continue to do so as part of your regular conversations.

Show your child how to use the internet in a positive way, to research things, to do homework, to talk to family, and to find out about the world. Talk to them about your own experiences online. You should also talk about your own less positive experiences online. This may be concerning how you feel about showing the 'perfect' life for others to see on social media. Talking openly like this should help them understand that 'perfect' lives and photos that others share on social media don't always show reality. Encourage them to talk to you if they have similar experiences.

Ask your child to share with you their favourite Apps, games or websites. This will help you understand how they work so that you can assess if you have any concerns. A quick online search may also help.

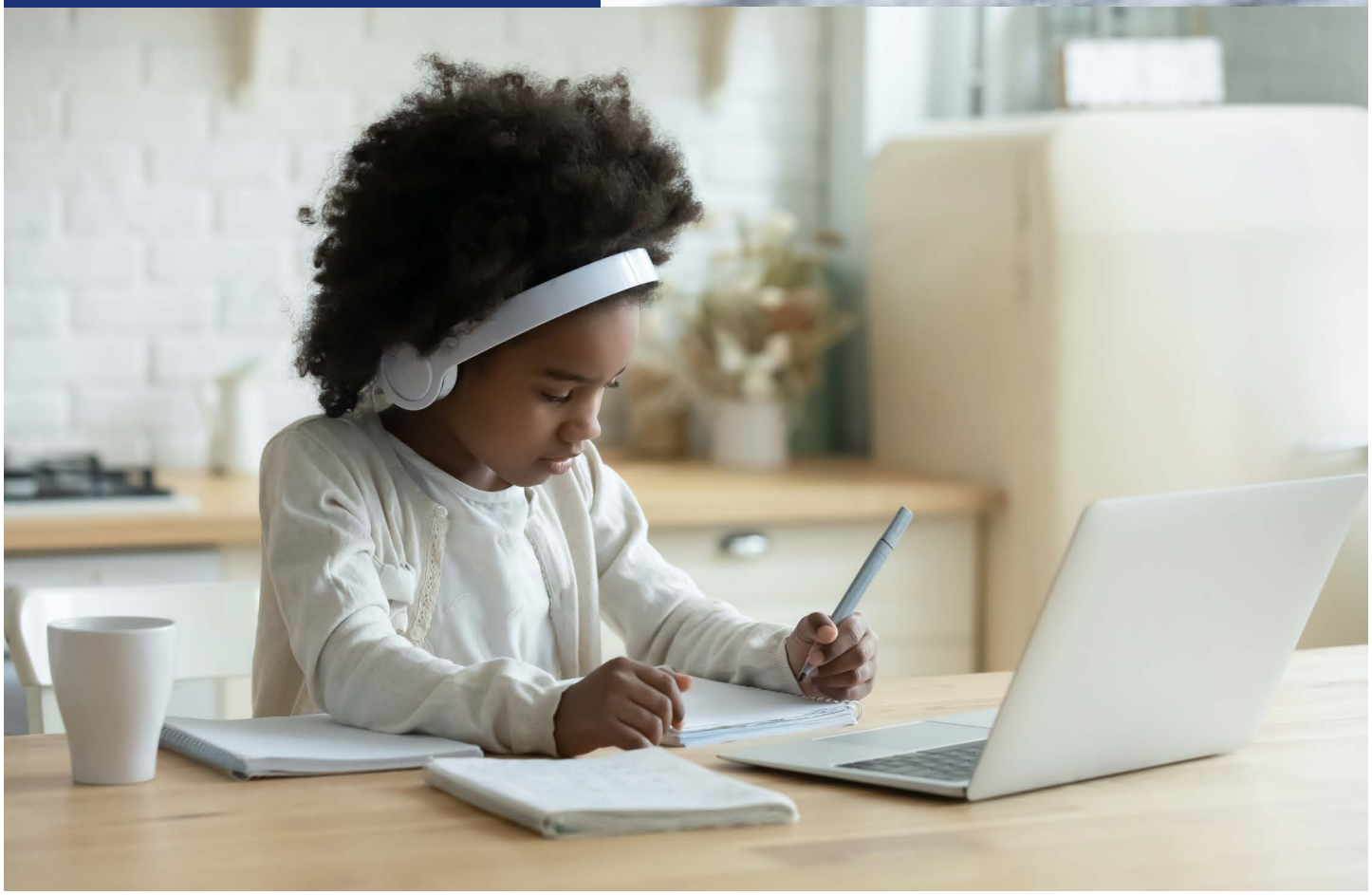
You are your child's role model, so, if you check your phone constantly at mealtimes, or play violent games in front of your children, then it's likely your child might do the same.

Set boundaries for your children, but be realistic as they need to be age appropriate. Whatever their age, it's a good idea to sit down together with your child to talk about it and agree some rules about how much time they spend online. For example, using a device just before bed.

If you think anything your child is accessing is not appropriate for their age, talk to them and explain why you think this. Where possible, make it a joint decision with your child, so they understand the reasons and are more likely to stick to it.

Many children play games online, so it's worth checking the ratings on the games your child is playing. There may be peer pressure for your child to play/buy a game that looks like it's extremely violent or too old for them. It's worth checking PGI ratings, which have more detailed information than ratings for films.

You can set up parental controls to stop your child from accessing harmful content online. However, be mindful that your child may know how to get round these and that's why it's more important to make sure your child is able to make good decisions for themselves.



It is a good idea to reassure your child that they can always talk to you. You may want to regular check with them if they've seen anything online that they are not comfortable with. Explaining that you won't overreact, that you'd much rather that they told you about it. If they are upset or worried about something they've seen, talk to them about how they feel, and how they can avoid seeing the things again in the future. If necessary, help them to report or block content they find disturbing.

Help your child to understand what is meant by personal information, so they can develop an awareness of why it's significant and why they should be cautious about sharing this type of information or pictures of themselves online.

Although most social media platforms are officially 13+, most children sign up to at least one when they're much younger. It's better that you encourage them to be open with you about this, rather than them keeping it a secret from you. Be aware that if they accept your friend request or follow you on social media, it's possible they may have another account that they're not sharing with you.

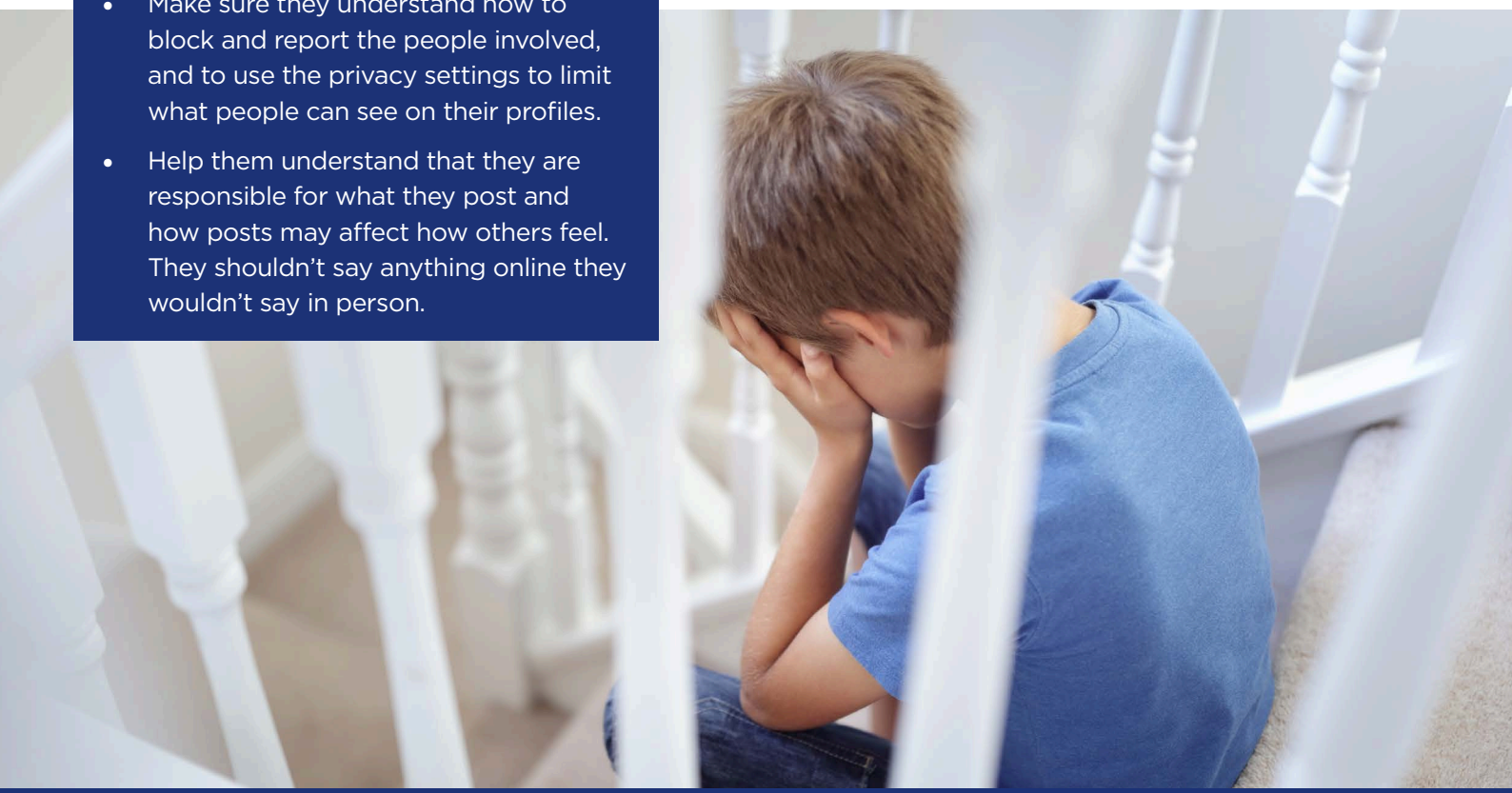
Bullying is awful, whether it happens face to face or online. If your child is receiving nasty messages, or people are posting unwanted things about them, or they feel harassed. To help them:

- Encourage them to talk to you, it will really help them to talk things though with you and discuss what actions to take.
- Make sure they understand how to block and report the people involved, and to use the privacy settings to limit what people can see on their profiles.
- Help them understand that they are responsible for what they post and how posts may affect how others feel. They shouldn't say anything online they wouldn't say in person.

Some things for you to explain to your child:

What you put online stays online. Even things you delete can be saved or screenshotted, including Snapchats meant for just one friend.

- Forums and group chats can be a great way to connect, but don't feel pressured to share more than you feel comfortable with. Remember, online strangers are still strangers.
- It's easy to over-share on social media, especially if you forget who can see your profile.
- Help your child to change their privacy settings on each platform they are using, to make their account can only people be seen by those you know and trust.
- Make sure your child understands how to report or block things that aren't appropriate or someone that makes you feel uncomfortable. Also to talk to someone they trust about it if this happens.
- Help your child to understand that they shouldn't feel the need to be available all the time on social media. It's okay to take a break, and you don't need to take part in every conversation.



Act on warning signs, if you think something is wrong. It's important to act if you are concerned:

- Talk to your child openly
- Listen to what they have to say
- Don't rush to judge
- Make sure they know that you'll always be there for them

WHO TO REPORT IT TO AND WHERE TO GET SUPPORT

Scams should be reported to:
Action Fraud **www.actionfraud.police.uk Tel: 0300 123 2040**

The Trading Standards department at your local authority can provide support in terms of supplying call blockers or removing mail. They can also tell you or your loved one has been included on any so called "suckers lists".

You can sign up for the Telephone Preference Service here:
http://www.tpsonline.org.uk/tps/index.html

The Mail Preference Service can be used to reduce the amount of mail received:
https://www.mpsonline.org.uk

Citizens Advice Consumer Service offer advice about scams:
www.adviceguide.org.uk Tel: 03444 111 445

Police Mutual Services

Worrying about money can be extremely stressful and may lead to mental health conditions. Police Mutual are here to help. We want to break down the stigma surrounding debt and get people talking about money.

We've teamed up with **PayPlan***, one of the UK's leading free debt advice providers, who offer free and confidential advice to anyone in serious financial difficulties.

They're able to advise you on a range of debt solutions suited to your individual circumstances, helping to protect you and your family with a sustainable way to manage your debt.

Get free and confidential help to combat your debt, call **PayPlan*** on **0800 197 8433**.

For more information about the products and services available from Police Mutual:

Call us 01543 441630
Visit policemutual.co.uk

We're open from
9am - 5pm Mon - Fri

*PayPlan is a trading name of Totemic Limited. Totemic Limited is a limited company registered in England, Company Number: 2789854. Registered Office: Kempton House, Dysart Road, PO Box 9562, Grantham, NG31 0EA. Totemic Limited is authorised and regulated by the Financial Conduct Authority. Financial Conduct Authority Number: 681263.

Police Mutual is a trading style of The Royal London Mutual Insurance Society Limited. The Royal London Mutual Insurance Society Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. The firm is on the Financial Services Register, registration number 117672. Registered in England and Wales number 99064. Registered office: 55 Gracechurch Street, London, EC3V 0RL. For your security all calls are recorded and may be monitored.

Police Mutual
We look after our own

PMLTM19 07/21