POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Stewartry Secondary Schools

Police Newsletter

March 2021

Stewartry Secondary Schools Youth Engagement Officer

Hello

I hope you are all managing to keep safe in these challenging times. It has been an unusual year and the opportunities that would normally have allowed me to engage with pupils, and parents, have been limited due to the various restrictions that have been implemented as a result of the Covid-19 Pandemic.

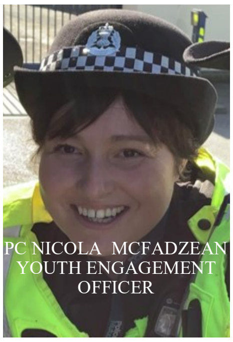
In the meantime, I thought a newsletter would be a good opportunity to reach out to pupils, parents and Carers in order to touch base and keep you updated of current crime trends, as well as issuing relevant advice in relation to such matters.

For my first Newsletter I thought it would be a good starting point to cover some Internet Safety matters. I am conscious that due to the current lockdown restrictions and home schooling routines we have found ourselves in, the internet is a great way for adults and children to connect with friends, family and can be vital as a means to assist with home working, home schooling , meetings, shopping, banking and other everyday business.

An increasing amount of children and young people, now more than ever, are using social media, gaming and live streaming apps to chat and share content with others. But connecting and sharing with people online can come with risks too. Privacy settings can help you and your child to manage how much and what kind of information is shared, whilst enjoying their favourite sites, games and apps.

During recent months we have also received a concerning amount of reports regarding frauds and scams mainly over the internet where people are being coned out of large amounts of money. We are also shopping far more online and more of us are using on line banking apps, but unfortunately more fraudsters are cashing in on this and are always coming up with new ways to get hold of our money.

Please have a read of some of the information I have attached below.
I wish you all well and I look forward to being back in the school environment in the coming weeks.


PC NICOLA MCFADZEAN
YOUTH ENGAGEMENT
OFFICER

Cool2Talk is a new way for young people to ask questions of the Police in Dumfries and Galloway.

It is a safe space where young people can ask questions anonymously about any subject they want. They questions will be answered by professionals with experience is a wide range of topics including, drugs, alcohol, bullying, healthy relationships and sexual health.

Questions can be asked anonymously and will be answered within 24 hours

How should I use privacy settings?

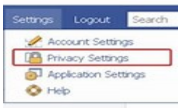
Follow these tips to help your child explore the internet safely. If you have an older child who creates their own accounts, consider these tips when talking to them about how they can use privacy settings.

1. Check the audience

2. Switch off location sharing

3. Check the tagging settings #

4. Review all privacy settings regularly



Advice For Online Home Schooling

As a parent or carer you play a key role in helping your child to stay safe online.

You don't need to be an expert on the internet to help keep your child stay safe online. There is advice and resources are available online to support you as you support your child to use the internet safely, responsibly and positively.

The links below, which are very informative and easy to follow, will open up the opportunity for you to start the discussion about online safety.
Thinkuknow is the online safety education programme from the National Crime Agency (NCA) and their website has home activity packs from the ages of 4yrs to 14+yrs to take support from.

https://www.thinkuknow.co.uk/parents/Support-tools/home-activity-worksheets/

CEOP, NSPCC and Internet Matters, at the links below, have created a number of fantastic free to use advice hubs to help you learn more to support you and your child or young person with Online issues. (control + click to follow link)

https://www.ceop.police.uk/safety-centre/

https://www.nspcc.org.uk/keeping-children-safe/online-safety/

https://www.internetmatters.org/advice/

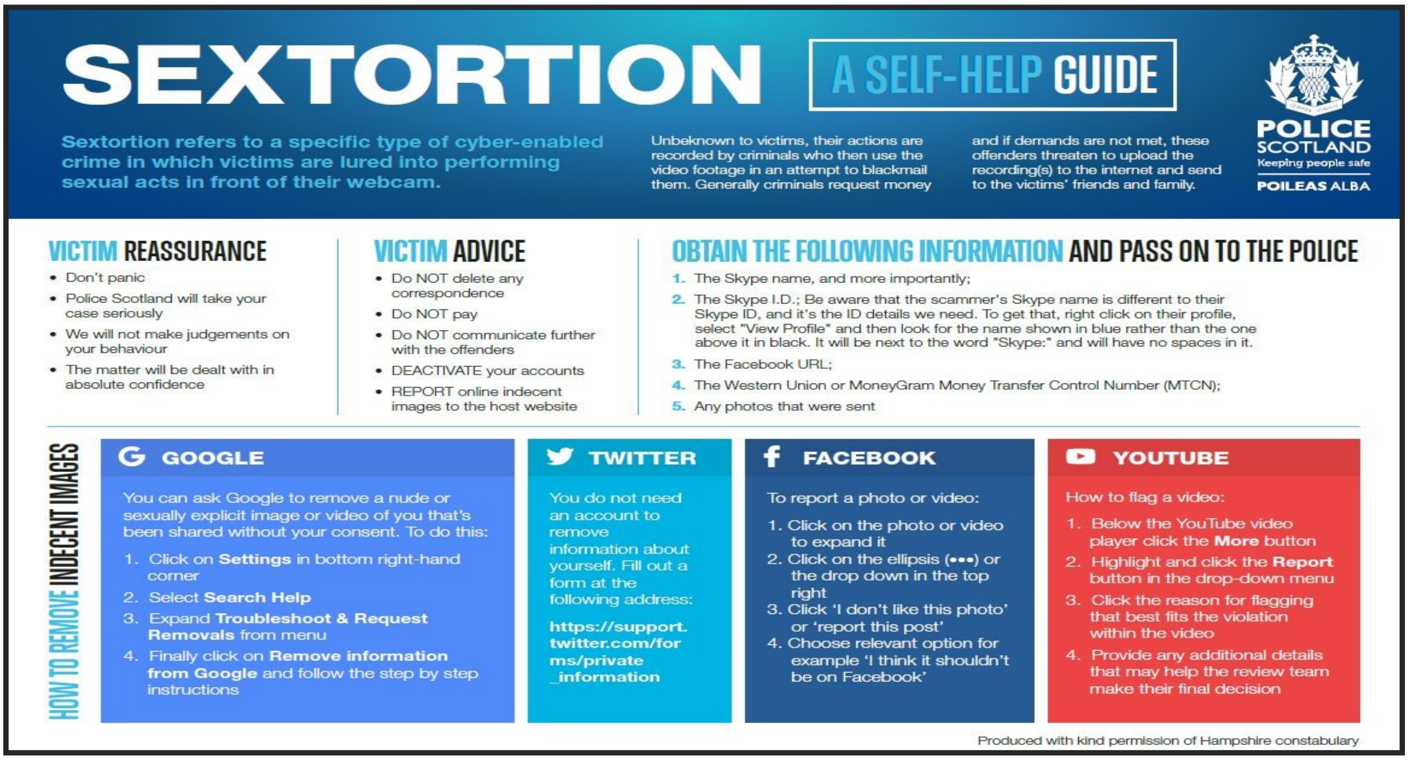
Please take time to enhance your knowledge in terms of the support that is available.

internet matters.org

NSPCC Cruelty to children must stop. FULL STO

CEOP

THINK U KNOW .co.uk



SEXTORTION

A SELF-HELP GUIDE

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Sextortion refers to a specific type of cyber-enabled crime in which victims are lured into performing sexual acts in front of their webcam.

Unbeknown to victims, their actions are recorded by criminals who then use the video footage in an attempt to blackmail them. Generally criminals request money and if demands are not met, these offenders threaten to upload the recording(s) to the internet and send to the victims' friends and family.

VICTIM REASSURANCE

- Don't panic
- Police Scotland will take your case seriously
- We will not make judgements on your behaviour
- The matter will be dealt with in absolute confidence

VICTIM ADVICE

- Do NOT delete any correspondence
- Do NOT pay
- Do NOT communicate further with the offenders
- DEACTIVATE your accounts
- REPORT online indecent images to the host website

OBTAIN THE FOLLOWING INFORMATION AND PASS ON TO THE POLICE

1. The Skype name, and more importantly;
2. The Skype I.D.; Be aware that the scammer's Skype name is different to their Skype ID, and it's the ID details we need. To get that, right click on their profile, select "View Profile" and then look for the name shown in blue rather than the one above it in black. It will be next to the word "Skype:" and will have no spaces in it.
3. The Facebook URL;
4. The Western Union or MoneyGram Money Transfer Control Number (MTCN);
5. Any photos that were sent

HOW TO REMOVE INDECENT IMAGES

GOOGLE

You can ask Google to remove a nude or sexually explicit image or video of you that's been shared without your consent. To do this:

1. Click on **Settings** in bottom right-hand corner
2. Select **Search Help**
3. Expand **Troubleshoot & Request Removals** from menu
4. Finally click on **Remove information from Google** and follow the step by step instructions

TWITTER

You do not need an account to remove information about yourself. Fill out a form at the following address:

https://support.twitter.com/forms/private_information

FACEBOOK

To report a photo or video:

1. Click on the photo or video to expand it
2. Click on the ellipsis (•••) or the drop down in the top right
3. Click 'I don't like this photo' or 'report this post'
4. Choose relevant option for example 'I think it shouldn't be on Facebook'

YOUTUBE

How to flag a video:

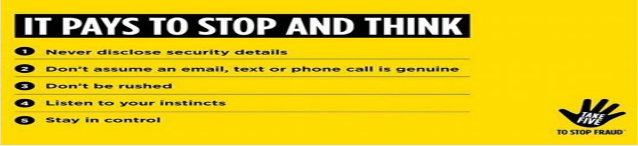
1. Below the YouTube video player click the **More** button
2. Highlight and click the **Report** button in the drop-down menu
3. Click the reason for flagging that best fits the violation within the video
4. Provide any additional details that may help the review team make their final decision

Produced with kind permission of Hampshire constabulary

AMAZON SCAM

A new and dangerous scam is circulating in various forms, which could prove dangerous if people come into contact with it.
Persons in our local communities have reported receiving a number of emails which urge them to take action on their Amazon account.
The email even contains an official looking watermark complete with the Amazon logo as well as the official address of the organisation's headquarters.
Both emails are illegitimate correspondence and by clicking the link and inputting personal information, this is likely to be intercepted by fraudsters who are looking for personal and sensitive information.
The consequences, therefore, could be disastrous with people standing to potentially lose a significant amount of money.

For more advice: visit https://takefive-stopfraud.org.uk. This is a national campaign offering straight forward, impartial advice that helps prevent e mail, phone based and online fraud—particularly where criminals impersonate trusted organisations.



IT PAYS TO STOP AND THINK

1. Never disclose security details
2. Don't assume an email, text or phone call is genuine
3. Don't be rushed
4. Listen to your instincts
5. Stay in control

TAKE FIVE
TO STOP FRAUD

PAYPAL SCAMS

PayPal have a long list of the types of scams that they are aware of.

Here are some helpful tips on how to spot Scam Emails:

The Senders Address
The "From" line may include an official-looking address that mimics a genuine one.

Generic Greetings
Be wary of impersonal greetings like "Dear User", or your email address. A legitimate PayPal email will always greet you by your first and last name.

Typos/Poor Grammar
Emails sent by popular companies are almost always free of misspellings and grammatical errors.

False Sense of Urgency
Many scam emails tell you that your account will be in jeopardy if something critical is not updated right away.

Links
Check where a link is going before you click on it by hovering over the URL in an email, and comparing it to the URL in the browser. If it looks suspicious, don't click it.

Attachments
A real email from PayPal will never include attachments. You should never open an attachment unless you are 100% sure it's legitimate, because they can contain spyware or viruses
Tracking number
The email/SMS asks you to provide the tracking number of the dispatched item, before you've received a payment into your PayPal account.

Clicking on links
Never click on a link in an email that requests personal information. Any time you receive an email about your PayPal account, open a new browser, type in www.paypal.co.uk, and login to your account directly.