Police Scotland

Skirling Community Council Meeting
Thursday, 27th September 2018

Foreword	**Covering the period 30th May to 24th September 2018** PC Craig is unable to attend your meeting on Thursday.
Ward Priorities	**Your priorities in Tweeddale West are** **Rural Thefts** Since your meeting in May there has been an attempt Housebreaking to a property on Skirling Green. **Speeding/Road Traffic** There have been no incidents reported. **Indiscriminate Parking** Nothing to report.

Police Scotland

Skirling Community Council Meeting

Thursday, 27th September 2018

Other Incidents of note/relevant Community Council information	**Other Thefts** • A quad bike was stolen from West Mains Farm. • An attempt to steal a quad bike and an Argo Cat Vehicle were made at Wakefield Farm, West Linton between 22/09/18 and 24/09/18 and quad bikes were also stolen from the Biggar area. • A house and a garage were broken into in West Linton. • Two vehicles were also stolen from Lochurd Farm and Blaircochrane Farm. • Oil Tanks have also been targeted with one being damaged and another being emptied in West Linton. Prevention advice can be found at the bottom of this report. **INFORMATION REGARDING SEXTORTION/BITCOIN SCAM** **Cyber criminals are sending victims their own passwords in an attempt to trick them into believing they have been filmed on their computer watching porn and demanding payment.** There have been over 110 of reports made to Action Fraud from concerned victims who have received these scary emails. In a new twist not seen before by Action Fraud, the emails contain the victim's own password in the subject line. Action Fraud has contacted several victims to verify this information, who have confirmed that these passwords are genuine and recent. The emails demand payment in Bitcoin and claim that the victim has been filmed on their computer watching porn. **An example email reads;** I'm aware, XXXXXX is your password. You don't know me and you're probably thinking why you are getting this mail, right? Well, I actually placed a malware on the adult video clips (porno) web site and guess what, you visited this website to experience fun (you know what I mean). While you were watching video clips, your internet browser started out working as a RDP (Remote Desktop) with a key logger which gave me

access to your display screen as well as web camera. Just after that, my software program gathered every one of your contacts from your Messenger, Facebook, and email.

What did I do?
I made a double-screen video. First part shows the video you were watching (you have a nice taste omg), and 2nd part displays the recording of your webcam.

Exactly what should you do?

Well, I believe, $2900 is a fair price tag for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).
BTC Address: 1HpXtDRumKRhaFTXXXXXXXXXX

(It is cAsE sensitive, so copy and paste it)

Important

You now have one day to make the payment. (I have a special pixel within this email message, and now I know that you have read this e mail). If I do not receive the BitCoins, I will definitely send out your video recording to all of your contacts including close relatives, co-workers, and many others. Nevertheless, if I receive the payment, I'll destroy the video immediately. If you need evidence, reply with "Yes!" and I will send your video to your 10 friends. It is a non-negotiable offer, therefore do not waste my time and yours by responding to this message.

Suspected data breach
Action Fraud suspects that the fraudsters may have gained victim's passwords from an old data breach.

After running some of the victim's email addresses through '**Have I been pwned**?', a website that allows people to check if their account has been

compromised in a data breach, Action Fraud found that almost all of the accounts were at risk.

Last month, fraudsters were also **sending emails demanding payment in Bitcoin**, using WannaCry as a hook.

How to protect yourself

Don't be rushed or pressured into making a decision: paying only highlights that you're vulnerable and that you may be targeted again. The police advise that you do not pay criminals.

Secure it: Change your password immediately and reset it on any other accounts you've used the same one for. Always use a strong and separate password. Whenever possible, enable Two-Factor Authentication (2FA).

Do not email the fraudsters back.

Always update your anti-virus software and operating systems regularly.

Cover your webcam when not in use.

If you have received one of these emails and paid the fine, report it to your local police force. If you have not paid, **report it as a phishing attempt** to Action Fraud.

	OIL TANK THEFTS – PREVENTION ADVICE Following the theft of 1000 litres of fuel oil from West Linton the following advice on how to keep your oil safe. • Locking your fuel tank cut off value with a strong closed shackle padlock and chain • If the tank is situated outside consider building a security cage around it. • Locate your fuel tank in a suitable building where it can be locked away. • Switch off the electricity supply to electrical pumps when not in use. • Be aware of suspicious vehicles nearby when fuel is delivered, thieves may follow delivery vehicles. • Ask the delivery driver if they have noticed any suspicious vehicles or behaviour. • Consider security lights and motion detectors to deter thieves. • Consider fitting a fuel tank alarm. • Consider using a mobile bowser that can be moved to a secure location when not in use. • Regularly check your fuel level and report any losses. For further crime prevention advice follow the link to our website - http://ow.ly/uewa30lAkEH or alternatively phone 101 and ask for your local Community Officer.
Feedback from meeting	Please e-mail any feedback to: - TweeddaleEastCPT@scotland.pnn.police.uk