

## **CRAIGIEBUCKLER & SEAFIELD Community Council Report**

This report covers progress we have made in dealing with your priorities for the Craigiebuckler & Seafield Community Council area during December 2019.

The report aims to highlight emerging issues in your area, and to provide crime prevention advice and guidance to Community Council members and residents you represent. Our focus is to reduce crime and disorder, help create safer communities and respond effectively to local concerns.

Your local policing team wishes you a happy and safe New Year!

# **Community Policing Priorities**

## **Antisocial behaviour, Violence and Disorder:**

Damage was caused to a road sign on Springfield Road and enquiries are ongoing to determine if this has been a wilful act or potential accidental damage.

#### **Acquisitive Crime:**

There has been no acquisitive crime during the period.

#### Road Safety & Road Crime:

The festive drink drive campaign continues and local officers are conducting regular patrols in conjunction with our Roads Policing colleagues. We continue to work with partners in response to specific complaints in terms of road traffic offences and to make use of antisocial behaviour legislation. Residents in the areas affected by antisocial driving are encouraged to contact Police on 101 at the time to report incidents in order for us to take positive action.

# **Community Engagement & Reassurance**

We hope you enjoyed the Christmas period. As the post-Christmas sales have begun, increasingly more of us are turning to internet shopping to purchase goods and services. As part of our commitment to deliver Safer Virtual Communities, this serves as an opportune time to give some guidance and advice in relation to internet safety, specifically in relation to internet shopping.

# **Phishing and Internet Shopping**

## What is Phishing?

Phishing is when criminals use fake e-mails or web links to acquire sensitive personal information, such as passwords, usernames, or bank account details. This is used to commit fraudulent or even criminal acts in your name, leaving you responsible for the consequences. Such emails and linked websites often appear genuine but are designed to trick people into entering personal details to access your identity, steal from your bank account or infect your computer with a virus which allows them to control your system.

## What kind of things might indicate Phishing?

- When shopping online, make sure your web browser and internet security is up to date. Look for the padlock in the address line before you enter any card details
- Be aware of seemingly genuine emails requesting to open attachments if unsure or not expecting anything, do not open any documents. If in doubt contact the sending company over the phone by using the genuine number
- Be aware of seemingly genuine e-mails advertising a win of some sort these
  usually involve requesting the sending of money to 'release' the prize or
  requesting your bank details
- Be especially cautious of emails that try to upset you into acting quickly by threatening you with frightening information
- Do not click on links, download files or open attachments in emails from unknown senders. It is best to open attachments only when you are expecting them and know what they contain, even if you know the sender
- Never email personal or financial information, even if you are close with the recipient. You never know who may gain access to your email account, or to the person's account to whom you are emailing
- Beware of links in emails that ask for personal information, even if the email appears to come from a company you do business with. Phishing web sites often copy the entire look of a legitimate web site, making it appear authentic. To be safe, call the legitimate company first to see if they really sent that email to you. After all, businesses should not request personal information to be sent via email

 Check your online accounts and bank statements regularly to ensure that no unauthorized transactions have been made

Another variation on this type of scam is known as **Vishing**, when you are contacted on the phone by someone claiming to be from your internet provider or bank for example. The same general rules apply.

- Don't ever give personal information like banking or credit cards over the phone to someone who has called you
- If you get a call from someone claiming to be your bank or credit card, hang
  up, and ring the number on the back of your credit card or your bank using a
  different phone from the one they called you on
- Do not divulge personal information over the phone unless you initiate the call

And yet another form of this type of crime is known as **Smishing**, which is when the source of the scam comes via text message. Text messages from unknown numbers should raise alarm bells, but often banks do text their customers for a variety of reasons. If you receive a text regarding your account details contact your bank using a number found on your bank statement, not the number provided in the text.

More information in relation to online safety, including safe internet browsing and social media and internet dating can be found online via our website at:

https://www.scotland.police.uk/keep-safe/keep-secure-online/cybercrime

What to know more about how we measure up, this is where to find out.

http://www.scotland.police.uk/about-us/our-performance/



Follow us on Twitter @NorthEPolice #HazleheadCPT

Also available are the three following contact email addresses for the Hazlehead Policing team:

HazleheadAshleyQueensCrossCPT@Scotland.pnn.police.uk LowerDeesideCPT@Scotland.pnn.police.uk KingswellSheddocksleyCPT@Scotland.pnn.police.uk The primary purpose of these e-mail addresses is for residents to report non-criminal queries, such as passing attentions, information, advice and non-criminal quality of life issues, such as youth annoyance. These e-mail addresses are not for reporting crimes or offences. The process for reporting any crimes or offences is to call 101 (Aberdeen Service Centre) who will log the call on our Command and Control system and allocate the incident to our area. Using this process negates the possibility of the report being missed and also ensures that the caller's details, addresses and telephone numbers are noted for our awareness and response.

Should you have any concerns or questions, please do not hesitate to discuss these with the Officer attending your Community Council Meeting or by emailing the above e-mail addresses or our Service Centre. It is not necessary to wait until the meeting and your local CPT Inspector, PI Sim welcomes your contact.

### **Contact Us**

Please also remember you can communicate with us using any of the following:

- ➤ 101 Non emergency;
- Twitter @NorthEPolice;
- Facebook www.facebook.com/NorthEastPoliceDivision;
- ➤ Meb www.scotland.police.uk;
- > 2999 Emergency;
- 28 0800 555 111 Crimestoppers.