# COMMUNITY SAFETY BULLETIN

**Cold Callers, Further Scams/Fraud attempts this week**

Here are the latest scams, Tele-Fraud scams/cybercrime incidents reports received this week. Some are new types, some are repeat incidents. Please pass to others, help prevent them from becoming a victim of a scam, cybercrime, or crime.

**Cold Callers at the door**

There have been a number of doorstep cold callers reported this week

- Following last week's bad weather there have been complaints about cold callers pressurising householders into having work done on the property. Callers usually claim to be able to see signs of damage to roofs and offer immediate attention and remedy on the spot. The householders targeted are typically older people living alone. It is not unusual for episodes of bad weather to be followed by opportunistic callers seeking to scare people into having work done. The work often turns out to be unnecessary, poor quality and overpriced and the trader is usually impossible to identify or contact after the event.

If you think work may be needed, seek the assistance of a competent, reputable tradesman and do not be bullied or scared into a rushed decision. Cold callers can be difficult to contact in the event something goes wrong with the service or product you have purchased.

- There have been reports of cold callers offering to sell mattresses. They were also overheard trying to purchase a caravan that was in a driveway, from a resident. This is a useful reminder to be wary of opportunistic rogue traders knocking on doors offering goods to purchase.

**Also, remember identity cards may not be genuine. If you have someone at your door claiming to be from the Council, or saying they are from one of your service providers, check they are genuine by phoning a number obtained from a trusted source, not one provided by the cold caller**

**Cold Calling Telephone Calls**

Below is the latest cold calling telephone calls received this week. Please remember, do not pass on any personal or banking information to a telephone cold caller. Remember, scammers can be well prepared before making their call. This helps them make their story

Flintshire & Wrexham Online Watch Link Association
Mold Police Station
King Street
Mold
CH7 1EF
watch@owlcymru.org Tel : 01352 708118 or dial 101 ask for extension 84144 or 08119

more convincing. They can find information from many sources including Google, social media (ie Facebook/Twitter) and numerous other sources

- Further calls have been received relating to faults on computers. On one call received, when the resident asked which country they were calling from, the phone was put down. One resident has received multiple calls claiming to be from BT regarding their computer, they are not a customer of BT. They put the phone down. Remember, this type of call is an attempt to gain remote access to your computer to steal from you. Enter details of the link below to view further information http://www.actionfraud.police.uk/fraud-az-microsoft-frauds
- We have received another report of two automated calls being received claiming to be from HMRC . The automated message states they are calling from 'Her Majesties Revenue and Customs', and they are informing them that they are failing a lawsuit against them. The direct the resident to press 1 to speak with their case officer. This is an attempt to steal from you. Details are in this link, please enter in your browser if you wish to view http://www.actionfraud.police.uk/news/alert-hmrc-and-itunes-gift-card-scam-may16

**Remember, telephone numbers can be 'SPOOFED' so they can appear to be local numbers or even a number known to you, so unfortunately, you cant trust that the number shown on your caller display is the genuine number.**
**Some nuisance calls can be blocked by Telephone Preference Service. This does not include calls from abroad. For more information visit their website** http://www.tpsonline.org.uk/tps/index.html **. Contact your own telephone service provider to see how they can assist with nuisance calls. Some offer a 'call screening' type service where a caller has to announce who they are before you choose whether you answer the phone or not. They may be able to assist you in other ways.**

**Scam and Suspicious e mails or texts**

The following e mails and texts have been received. Remember, scam and phishing e mails are designed to panic you into reacting, or make you respond without thinking. Never automatically click on a link, or respond without being sure that the sender is genuine. See advice in the section below the incidents reported.

- A resident has received an e mail relating to an order. The e mail actually had the recipients name and address and telephone number thereon. The email appeared to relate to the purchase of skin care items. It asked the recipient to click on a link to

Flintshire & Wrexham Online Watch Link Association
Mold Police Station
King Street
Mold
CH7 1EF
watch@owlcymru.org Tel : 01352 708118 or dial 101 ask for extension 84144 or 08119

view details of the purchase. Enquiries reveal that other people have had similar emails and the link may contain malware.

- A resident has received two texts claiming to be from uk.gov relating to refunds due on a P60. The first amount quoted was for £900, the second was for £200. The text asked the recipient to click on a link to verify their bank details. The resident was aware this was a scam and did not do this. A short while later he received yet another text, this time stating that if he had received a text claiming to be from HMRC he should delete it. The resident states that HMRC do not have his mobile number so the later text may not be genuine either, but there was no request to click on any links so enquiries are ongoing. Below is a link with guidance on helping to identify scam e mails/texts from genuine ones. https://www.gov.uk/government/publications/genuine-hmrc-contact-and-recognising-phishing-emails/genuine-hmrc-contact-and-recognising-phishing-emails
- A resident has had an e mail claiming to be from Skype, relating to a payment made. The email stated that if they hadn't authorised it they should click on the link (which LOOKED like a link to PayPal help centre to make a claim and get a refund. However, when the mouse is hovered over the link, it becomes clear that the actual address it would take you to, is NOT Paypal.
- A resident has received a text claiming to be from PayPal, The text is requesting a payment of £100. Thankfully the resident did not click on the link and reported the text to PayPal and Action Fraud. As a reminder, enter details of the link below for advice from PayPal to help identify phishing emails and texts claiming to be from them https://www.paypal.com/uk/webapps/mpp/phishing
- A resident has received an e mail claiming to be from BT. The e mail claimed that the credit card details they had on file was declined when approached for payment. The e mail asked the recipient to click on a link to update billing information immediately as their account could be suspended. Suspected phishing emails can be forwarded to phishing@bt.com. Below is a link to BT for advice on identifying phishing emails claiming to be from BT http://home.bt.com/tech-gadgets/internet/how-to-deal-with-fraudulent-emails-11363932621450
- A resident has received an e mail claiming to be from a bank stating that his account has been suspended. Another resident has received an e mail stating that a payment has been received via direct debit. It provides a date when the next payment is due and to click on a link to register details. The residents were aware they were scam e

Flintshire & Wrexham Online Watch Link Association
Mold Police Station
King Street
Mold
CH7 1EF
watch@owlcymru.org Tel : 01352 708118 or dial 101 ask for extension 84144 or 08119

# COMMUNITY SAFETY BULLETIN

mails and did not respond. Below is advice to help you in dealing with suspicious e mails.

**If you receive a suspicious e mails - Protect Yourself:**

Do not click on any links or open attachments contained within unsolicited emails.
Do not reply to scam emails or contact the senders in any way.
If an email appears to have come from a person or organisation you know of but the message is unexpected or unusual, contact them directly via another method to confirm that they sent you the email.
If you receive an email which asks you to login to an online account via a link provided in the email, instead of clicking on the link, open your browser and go directly to the company's website yourself.
If you have clicked on a link in the email, do not supply any information on the website that may open.

If you think you may have compromised the safety of your bank details and/or have lost money due to fraudulent misuse of your cards, you should immediately contact your bank, and report it to Action Fraud by calling 0300 123 2040, or visiting www.actionfraud.police.uk

**NEW**
**Change to the Penalty for using a hand-held mobile phone while driving - IMPORTANT CHANGES**

From 1st March 2017 the penalties for using a hand held mobile phone changed, see below information
Using a handheld mobile phone while driving is illegal. It has been since 2003. From 1 March 2017 the penalties for holding and using your phone while driving have increased. It's now 6 points and £200.

It is not illegal to use hands free, but any time a driver's attention is not on the road can be dangerous.Details are available in the link below

http://think.direct.gov.uk/mobile-phones.html

**Visit our online shop for useful crime prevention products**
**http://www.owlcymru.org/shop/shop.html**

Flintshire & Wrexham Online Watch Link Association
Mold Police Station
King Street
Mold
CH7 1EF
watch@owlcymru.org Tel : 01352 708118 or dial 101 ask for extension 84144 or 08119