***Fraudulent Requests for Payment***

Fraudsters are targeting members of the public who are expecting to make payment for property repairs. The fraudsters (via e mail) will purport to be a tradesman who has recently completed work at the property and use a similar e mail address to that of the genuine tradesman. They will ask for funds to be transferred via bank transfer and once payment is made the victims of the fraud soon realise that they have been deceived when the genuine tradesman requests payment for their services

**Protection Advice**

* Always check the e mail address is exactly the same as previous correspondence with the genuine contact
* For any request of payment via e mail verify the validity of the request with a phone call to the person who carried out the work
* Check the e mail for spelling and grammar as these signs can indicate that the e mail is not genuine
* Payments via bank transfer offer no financial protection; consider using alternative methods such as credit card or PayPal which offer some protection and avenue for recompense

……………………………………………..

***Community Alarms Fraud***

Fraudsters are using “VISHING” techniques to gather bank account details of vulnerable people. VISHING is when fraudsters obtain personal details of a victim by phone. Fraudsters can then go on to use this personal information to commit fraud

In this instance fraudsters are targeting members of the public who use pre-paid services which provide community alarms to residential properties. This service is paid for via direct debit. The victim receives a phone call from the fraudster purporting to be from the company used for this service. The fraudster asks for the victim’s bank account details due to existing bank records being out of date. The victim will provide the relevant information allowing the suspect to collate their bank details for use in a future fraud.

**Protection Advice**

* Never provide ANY personal details to cold callers (don’t confirm your name address or even your phone number)
* If you are concerned about the source of a call, hang up and call the company back on the legitimate phone number which will be printed on official correspondence from them, such as e mails or letters
* If a call is received asking for personal information tell the caller you will verify their identity with their company and that you will call them back