Alresford and District Neighbourhood Watch Association

PHONE & COMMUNICATION SCAMS

Phone fraud, or more generally communications fraud, is the use of telecommunications products or services with the intention of illegally acquiring money from, or failing to pay, members of the public who are customers of these products.

Many operators have increased measures to minimize fraud and reduce losses, however there are still many innocent victims of this ever growing criminal activity.

There are 5 main types of fraud and these are:
- **Fraud against users by phone companies**
- **Fraud against customers by third parties**
- **Fraud by phone companies against one another**
- **Fraud against the phone company by users**
- **Frauds against the phone company by third parties**

We will concentrate on the fraud against customers by third parties, i.e. the scams fraudsters will use. These currently include:

1) 'Technical Support'

Someone calls you claiming to be from Microsoft, Apple, or another tech company and ask if you've had computer problems or tell you they have received 'error' messages from your computer/phone system requiring action. They then request you to allow them access to your system, via some simple steps they will explain to you. Unfortunately the scammers won't fix the problem and will make it worse by installing malware/viruses or extracting personal financial data to steal from you.

2) 'Bank/Credit Card'

Someone calls or messages claiming they are from your Bank or Card Fraud Dept. They then give you a number to call back or, if you answer the call, they will try to verify your identity by asking various questions. Never give out any account or card details unless you have made the call and never call a number given to you. Always call the number off your Bank website, or on the reverse of your Card.

3) 'One Ring'

Ever rush to answer your phone, only to realise the caller hung up after one ring? Don't let curiosity get the better of you and call back. Calling back verifies your number belongs to a real person, plus shows you're the type of person who will return a call from an unknown number. The call back could cost you, even if they don't ask for anything as you might be calling an expensive 'charge' line. Let any unknown number go straight to voicemail. If it's important, the caller will leave a message.

There are a number of variations with the above scams such as fraudsters offering you a prize and asking you to either call a given number or respond by pressing '1' on your phone. Likewise stating your 'Internet' or 'Amazon Prime' subscription payment will renew next month and press '1' to cancel. Remember once these fraudsters know your number is 'live' they will sell it onto other scammers.

WHAT SHOULD YOU DO IF A SCAM OCCURS?

Don't feel embarrassed about reporting a scam; scammers are clever and scams can happen to anyone.
Reporting a scam helps track down and stop scammers, preventing others from being scammed.

Remember to:
- **Always protect yourself from further risks**
- **Gather all the details of the scam**
- **Report the scam**

- **Make a complaint to the regulator - the Phone-paid Services Authority (PSA). Not a request for a refund, to https://psauthority.org.uk or 0300 303 0020.**
- **If you didn't lose money and just want to report a call, you can use the streamlined reporting form at https://www.donotcall.gov/ Report the number that appears on your caller ID, even if you think it might be fake and any number you're told to call back.**
- **Use the 'Action Fraud' online facility, which is the UK's national fraud and internet crime reporting unit at - https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime or 0300 123 2040.**