Alresford and District Neighbourhood Watch Association

BEWARE OF SCAMS – THE CROOKS ARE GETTING BETTER.

The police are spending more and more time these days on what is called 'cyber crime' as distinct from physical crimes such as house burglaries and thefts from sheds and other outbuildings. The criminals who commit 'cyber crime' are often very good at it because it's their day job. We can help ourselves and the police by not falling for the tricks that these criminals often use.

STRANGE PHONE CALLS.

Have you had an unexpected phone call from someone claiming to be from Windows who tells you that they have detected a fault on your computer and they can help you fix it? If so, it's a scam because there is no company called 'Windows'. Microsoft Corporation is a genuine American company whose computer operating systems are called Windows XP, 7, 8 and 10. Also, you will almost certainly not have given your phone number to Microsoft so the call cannot be from that company. The criminals have obtained your phone number from elsewhere and will want you to give them remote access to your computer so that the 'fault' can be fixed. If you do so, they will put some software on to your computer which will send them any financial account numbers and passwords that you use. Thereafter, they will take money from your accounts and you will have been robbed.

PHISHING SCAMS AND SUSPICIOUS EMAILS AND TEXT MESSAGES.

Have you received a strange email or text message from a company you know well, like Lloyds Bank, Visa, Apple or HMRC? It's urging you to act, asking for personal information. It might claim there is something wrong with your account. Or that your details need to be updated. Fraudsters use a scam called phishing for email, and smishing for texts. They copy emails and texts from real companies to try to steal your data or send your computer a virus. Is the email asking for financial and personal info? Genuine companies never ask for Internet Banking log on details or card details in an email . **Don't reply, and don't click on any links or attachments.**

Do you know who really sent the email? If in doubt, phone the company on a trusted number or visit their website by typing their web address directly into the address bar. Don't click on a link or copy and paste from the email itself.

Is the email trying to scare you into action? Emails from reputable companies should sound reasonable and calm. Phishing emails often contain threats of account suspension or immediate risk of fraud. If you're not sure about an email that looks like it's from your bank, you can always phone the bank using the number on the back of your card.

Banks will never ask you to carry out a test payment online or move money to a new sort code and account number, even if it's described as a "secure", "safe" or "holding" account.

REPORT IT TO ACTION FRAUD

Call telephone number 0300 123 2040

They'll be able to log the incident and provide you with a Crime Reference number if needed. Action Fraud collect data from across the UK to help banks and other businesses combat fraud.