



Alresford and District Neighbourhood Watch Association



AGM NOTICE

The AGM of Alresford & District Neighbourhood Watch Association will be held at Alresford Golf Club at 7:30pm on Tuesday 11th September. Speakers will be PCSO Rhys Griffiths and Julie Gallagher from Trading Standards. All are welcome.

PHISHING

There are frequent warnings in the media and from Hampshire Alert about suspicious emails which are intended to solicit personal details about you and how you access organisations that you do business with. These are generically called *phishing emails* ... a play on the word fishing, but these emails have a malicious intent. But, how are you supposed to tell the difference between a genuine email from an organisation and one which is not. As with many things ... if it doesn't look right or feel right, then it's probably not genuine and should be deleted. However, there are some key things to look out for.

- Phishing emails don't address you by your name, instead, they use a general address like- Dear Customer or Dear Subscriber or Hello.
- Check the email address of the sender. If this is a genuine email, the address will be directly related to the organisation.
- Check the email for spelling and grammatical errors.
- Phishing emails use scare tactics, like threats to close accounts, to create a sense of urgency and cause you to make hasty or impulsive decisions that can prove disastrous.
- Look for grammatical errors in the text ... comma instead of a full stop ... capitalisation in the middle of a sentence ... repeated word.
- If there are links in the email which you are directed to follow, do not click on the link but just let your mouse hover it so that the actual address is displayed. In a phishing email the address will not be anything you would expect.
- If the email is in any way suspicious do not, under any circumstances, open or save any attachments.

If ever you receive an email from an organisation which is not expected, and which is demanding some action from you, just take a minute or two to examine it a bit more closely, using some of the tips above and you may well save yourself from problems later.

If you suspect you have received a phishing email, just delete it or forward it to the organisation which it is supposed to have come from and then delete it. Most companies have email addresses for receiving phishing emails, for example, phishing@bt.com ... phishing@rbs.com.

If anyone has suggestions for topics that they think would be suitable for future Neighbourhood Watch articles in the Forum, please get in touch - e-mail contact.adnwa@gmail.com

Alresford and District Neighbourhood Watch
Association website-
www.neighbourhood.watch.alresford.org
e-mail – contact.adnwa@gmail.com

**CRIME IN PROGRESS – 999
NON URGENT – 101
CRIMESTOPPERS – 0800 555 111**