Phishing and Vishing

Part of the Security Awareness article from Driffield's U3A Newletter for November/December 2015. The full newsletter can be viewed by clicking on
http://www.woldsu3adriffield.org.uk/Files/2015%20NL%20Six.pdf

PHISHING

i) Who's had one of those emails telling you've come into some money, but all you need to do is pay some money over to release the funds, You know the ones, with loads of spelling mistakes, perhaps from a princess who needs money to escape the country or access her money held in trust against her will. It may seem like a pretty obvious con but scammers are getting more creative, so we all have to be one step ahead of them.

ii) Or you may have received an email claiming to be from your bank, and asking for your bank or credit card details, or security information. If so, you may have been the target of something called 'phishing'- involving someone trying to trick you into providing your personal details, so they can use them.

The scammers trick you by sending an email that looks like it has come from a company you're probably familiar with, like your bank. They commonly ask you to click on a link that takes you to a fake website where it will ask you to enter your account details.

iii) So how can you tell if it's a phishing email?

- The sender's email address doesn't match the organisation's real website address.
- The email uses a general greeting like 'dear customer' instead of your actual name.
- There's a sense of urgency, e.g. threatening to close your account if you don't act immediately.
- There's a link that may look similar to the proper address but is in fact slightly different and will take you to a fake website.
- You're asked for personal information, such as your username or password. If in doubt, don't reply and don't click on any link!

VISHING

Please be aware of a particularly nasty scam called 'vishing', in which someone will try and trick you over the phone to give them your personal bank account details, hand over your bank card, or transfer money from your bank account into another bank account that isn't yours.

The scammers rely on our very British respect of authority and trust. There has been an increase in the number of complaints, many people have been fooled by vishing, this result is the rise from zero complaints, to around 25 a month

CHECK WHAT HAPPENS!

i) The scammers call you on your telephone pretending to be from your bank. They tell you they are concerned that there's been fraudulent activity on your account. They may tell you to send them your bank card, or that they are about to send around a courier to come and pick your card up.

ii) Sometimes the scammer will try to trick you further into thinking they are genuine by telling you to call them back on the number given on the back of your bank card for their customer services helpline.

iii) The scam is that even when you put the phone down, they stay on the line at their end, which means the line isn't broken. So, when you think you called your bank back, you're actually still speaking to the same person. If you get a call like this, always check the line first. Dial someone else you know to see if the line has been broken. Or call your bank from another telephone to see if they really have called you.

Remember, your bank will never, ever ask to collect your card or send a person round to collect it.