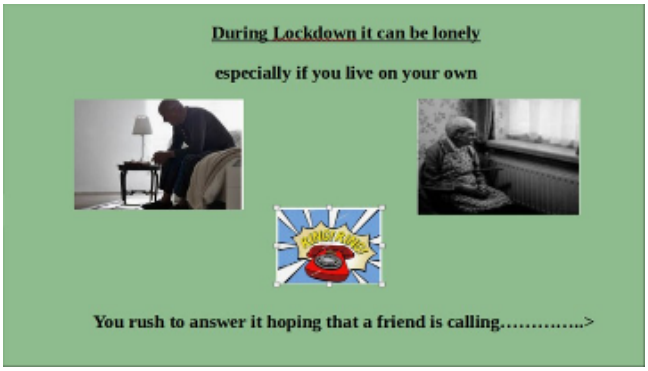
SCAM and FRAUD ALERT

From Hampshire and IOW Neighbourhood Watch

'Don't get caught by a Vishing Scam

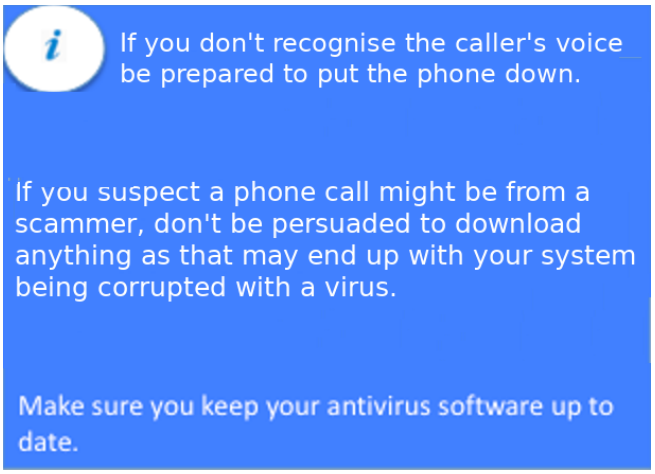
'Phone Phishing' or 'Vishing' is when a cyber criminal phones you out of the blue and convinces you to download a virus that infects your device.
Some callers can be very plausible and convincing – maybe using information gleaned from other data breaches to convince you they are genuine.



One of the current 'vishing' scams starts with a phone call that appears to come from your internet provider and suggests there is a problem with your computer or smartphone.
The caller suggests that you download some software such as Anydesk or Teamviewer. That gives the caller control of your systems to infect them with a virus. Then you will be asked to pay to remove the virus. Responding to these phone calls always results in trouble.

How to keep safe from this fraud

- Don't be rushed into doing something you might later regret – take time to check if the call is genuine.
- Never download software as a result of an unexpected phone call.
- Consider using call blocking



The *Which?* website has useful guidance on spotting and avoiding scam phone calls: https://www.which.co.uk/consumer-rights/advice/phone-scams.

If you get a fraudulent call like this or think you may have been the victim of fraud or have been hacked as a result of responding to a phishing message, you should report this to Action Fraud at: https://www.actionfraud.police.uk/report-phishing

If in doubt about any communication, our Cyber Champions are available to offer free advice. Just go to the Hampshire Cyber Watch Home page at https://hampshirecyberwatch.org/ and hit the red button: Request Support