Beware of Scams

There are many scams about at the moment involving phone calls, emails and texts.

With all of these you should **never** respond in any way; the legitimate organisations will always write to you.

Should you click on any link in an email; the scammer will have access to everything on your computer/laptop. Your identity can be stolen should you supply any information or click on any link.

Here are some examples:

Impersonation calls, emails and SMS texts

- Stop and think before you answer anything purporting to be from the government.
- They may be warning you about **a banking scam** and try and persuade you to allow remote access to your computer and give out personal information.

For any email scams purporting to be from **uk.gov**, such as Income Tax refunds, TV licence or Car Tax, you can forward the email to:

phishing@hmrc.gov.uk

For emails from British Gas, forward to

Phishing@ centrica.com

For emails from Amazon, forward to

stop-spoofing@amazon.com

- After forwarding, delete the email selecting ‘Phishing’ or ‘Block’; don’t just ‘Delete’

- There are also calls about renewing Amazon Prime subscriptions – if irrelevant, hang up

- If you receive an unwanted text, these can be forwarded to 7726.

Phishing calls

If you receive a call offering protective face masks, hand sanitiser, testing kits etc. be aware that they may not be legitimate. If you do receive a call, don’t be afraid to hang up and research the company first.

WiFi provider phishing calls

- There has been an increase in fraudsters impersonating WiFi providers such as BT, Talktalk or Microsoft. They ask for personal information, want access to your computer and mobile and would even ask you to install applications like TeamViewer that can give them remote access to your personal devices.
  If you do receive a call like this then hang up immediately

- You can check for clarification from your supplier on a confirmed phone number.