PCC urging residents to #BeCyberSmart

As part of Cybersecurity Awareness Month, PCC Mark Shelford is urging local people and businesses to remain vigilant to protect themselves online.

Scammers continue to take advantage of the public's and businesses' use and reliance of the internet. According to Microsoft, in 2022 the most common causes of cyberattacks are still malware (22%) and phishing (20%).

Nationally, the most impersonated organisations in phishing emails reported last year were the NHS, HMRC and gov.uk.

As of 31 May 2022, the public has made more than 12 million reports to the Suspicious Email Reporting Service (SERS), with the removal of approximately 83,000 scams and 153,000 malicious websites.

PCC Mark Shelford said: "Collectively, we all have a responsibility to be informed and up-to-date on how to protect ourselves online, both at work and at home, to stop scammers in their tracks.

"Phishing scams in particular target the most vulnerable in our communities and we need everyone to know that, if they receive a call or message that you think is a scam, do not respond to it. Your bank, police and any other official source will never ask you to supply personal information via email or text message.

"The impact of these crimes can be significant for both individuals and businesses; the more awareness there is around such online scams and how to defend your tech, the more people we can protect to falling victim to these heartless fraudsters.

Here are a few steps we can all take to #BeCyberSmart

- **Don't get hooked on phishing scams**: Be sure to always check the sender's address for verifiable contact information as common phishing errors often include a misspelled or unrelated sender address. If you have doubts about the message, do not open any attachments and contact the organisation directly. If you think an email could be a scam, report it by forwarding the email to report@phishing.gov.uk
- **Practice good cyber hygiene**: To keep all your devices safe, make sure you enable the lock feature on your mobile devices, activate multi-factor authentication on sensitive apps and accounts, and ensure you run antivirus software
- **Question error messages**: Be sure to question unexpected emails or texts that request urgent action. Do not follow any prompts to download software from any third-party website and, when in doubt, open a separate browser page and go directly to the company's website
- **Protect your passwords:** Passwords are the first line of defence to protect ourselves online. You can use a password generator to create a stronger password, use a password manager and make sure you avoid accessing personal and financial data using public WiFi.

Local businesses can also sign up to the South West Cyber Resilience Centre (SWCRC), a police and private sector collaboration run on behalf of regional forces.

The SWCRC provide free guidance and support including information on basic security and how to implement it plus a monthly update on the latest threats. The centre can also provide inexpensive services including website and systems testing using a network of ethical hackers.