Internet & doorstep scammers

We would like to urge our residents to be vigilant against criminals using the publicity around coronavirus as a chance to target their victims with fraudulent emails, phone calls, text messages or social media posts. Always follow advice of the national Take Five to stop fraud campaign and take a moment to stop and think before parting with your money or information in case of a scam.

Tips for recognizing and avoiding phishing emails

Here are some ways to recognize and avoid coronavirus-themed phishing emails.

Like other types of phishing emails, the email messages usually try to lure you into clicking on a link or providing personal information that can be used to commit fraud or identity theft. Here's some tips to avoid getting tricked.

- Beware of online requests for personal information. A coronavirus-themed email that seeks personal information like your Social Security number or login information is a phishing scam. Legitimate government agencies won't ask for that information. Never respond to the email with your personal data.
- Check the email address or link. You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses. Delete the email.
- Watch for spelling and grammatical mistakes. If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email. Delete it.
- Look for generic greetings. Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal an email is not legitimate.
- Avoid emails that insist you act now. Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information — right now. Instead, delete the message.

Doorstep scamming

There have been reports that people may be taking advantage of vulnerable people by posing as door-to-door government officials, police or Coronavirus testers to gain access to people properties. Nobody is conducting coronavirus tests. This includes the NHS and the police. Doorstep fraud is a crime. It happens to a wide range of people with all sorts of backgrounds. Please report it if it happens to you If anyone attends your property and claims to be testing, call police on 999.

Action Fraud and Age UK are working together to combat doorstep fraud and offer some helpful steps on ways in which you can protect yourself. They suggest this easy way of remembering how best to protect yourself and your loved ones if someone comes to your door offering help.

Stop – never do anything you don't want to or make any decisions on the spot

Check - Check for ID but remember most of these are community volunteers so wouldn't necessarily have ID. There is no way of knowing whether they are legitimate

Ask – Ask someone you trust for a second opinion, or ask them if they can provide the support you need.

Mine – If they ask for your card or your pin, remember this is very personal information which should not be shared

Share – If you come across a scam, share your experience with others if possible to prevent them from being scammed.