Corona Virus Scams

Those who seek to abuse the elderly and vulnerable are now using the Corona virus as a vehicle for their abuse. The Scams are both on line and cold callers.
As the fear escalates people will take risks and perhaps suspend usual judgements. Anything that offers 'hope' may be accepted.
Many elderly or vulnerable people will be susceptible to these scams – maybe even more so if they are self isolating and experiencing increased loneliness and fear.
If it seems too good to be true it probably is.

There are a number of fraud variations using Coronavirus as a 'hook' - eg:

- **Fraudulent sellers** – victim purchases a large amount of masks, sanitisers, or other products which are never delivered.
- **Malicious attachments and links** – offender claims to be from the World Health Organisation (WHO), NHS or other health organisations claiming to have a list of infected individuals in the victim's area and prompts them to click on a link or open an attachment to access this information
- **Fraudulent charities** – fraudsters set up fake charities claiming to raise money for people affected by the pandemic. They may visit people at home or stop them in the street, or contact on line.
- **Covid-19 tax return scam -** a convincing, yet grammatically incorrect, email sent to victims claims that "as a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan".

  The email tells the recipient that they are owed money as a tax rebate, and instructs them to click on a link that redirects them to an official-looking page. It then asks for all of their tax and financial information.

Tax scams are common in emails, but **HMRC will never contact you this way regarding a potential tax refund. HMRC will never ask you for private details in an email format.**

- **'The virus is now airborne' -** an email designed to look like it is from the Centres for Disease Control and Prevention (CDC) claims that Covid-19 is now airborne. This is the more devious type of phishing scam, as it uses legitimate email addresses from the CDC, but these have been sent via a spoofing tool.

  The link in this email directs recipients to a fake Microsoft log in page. If they add their details, they are diverted to the CDC's official advice page - adding to the feeling of authenticity.

  By this point, hackers already have control over your email and Microsoft password.

- **'Click here for a cure'** - up to 200,000 emails claiming to have a cure for the current coronavirus outbreak are being sent at a time. The email says it is from a mysterious doctor claiming to have information about a cure that has been covered up by the Chinese and UK governments.
- **Little measures that 'save lives'** - an email has been circulating that appears to be from the WHO, claiming that attached documents provide information on how to prevent the spread of the disease.

  It reads, "This little meaure can save you".

  The attachments contain malevolent software that charts your keystrokes and monitors your computer use.

- **Cold Callers - a**ccording to Trading Standards cold callers have been knocking on doors and claiming they are checking houses for coronavirus.

This is a scam to gain access to your property. Do not, under any circumstances, let them in. If you have elderly or vulnerable relatives / friends / neighbours - please do make them aware.

If you are approached do not let people in, call trading standards at your local council and call police on 101 or 999 if you feel threatened.

To minimise a chance of becoming a victim of fraud or a scam follow simple advice:

- Only buy from reputable sources – not door to door salespeople or unknown websites.
- Do not click on any links sent to you from an unknown organisation or person and don't open any suspicious email attachments
- Only use trusted sources, like the Government website, for updates and information. Go directly to the website do not click on any links.
- Avoid emails from the CDC and WHO - they will not email the general public. To give any vital updates, they will post on their website.
- Never reveal your personal or financial information in an email, text or over the phone. No reputable organisation will every ask you to do this.
- If you wish to make a donation check the legitimacy of any organisation on the government charity register or use a well known and trusted charity either local or national – such as local food banks etc.
- If you are making purchases online do a thorough research of the seller, and when making payment use a credit card as most major providers insure online purchases.
- If you have any concerns about any suspicious messages or you have been targeted by a fraudster, report it to Action Fraud. You can also report crime to Police online or by calling 101.

Trading Standards websites have up to date info on the latest scams.

Consider advertising or putting people in contact with Silver Line - https://www.thesilverline.org.uk/