Coronavirus Scam Warning

Fraudsters may exploit the spread of COVID-19 Coronavirus to carry out various types of fraud.

The three types of fraud to look out for are:

1. **Phising / Smishing / Vishing**
2. **Fraudulent Selling / Trading**
3. **Social Engineering Scams**

If you have been a victim of fraud or cyber crime contact your local Garda Station.

Phishing / Smishing / Vishing

What is Phishing / Smishing / Vishing?

This is where a company or person receives an unsolicited email, text, WhatsApp message or telephone call claiming to be from a legitimate organisation. These communications will contain an attachment containing vital information regarding the Covid-19 virus and prompting the receiver to open the attachment. It can also ask the victim to enter email login details to assess this vital information and in both ways, can lead to malware infecting the computer.

Advice:

Never open attachments in unsolicited emails and ensure your computer has the most up to date anti-virus software installed. Companies are advised to educate staff on the proper procedure for answering and dealing with customers, invoices, direct payments and never change a payment system as a result of an email or an unexpected phone call.

Social Engineering Scams

What are Social Engineering Scams?

This is where criminals exploit the charitable nature of people via social media or in person asking for donations to so called charitable causes. The criminal could be posing as a collector for a real charity or could set up online funding campaigns.

Advice:

People should be wary of unsolicited requests and only ever donate to legitimate, recognised charities. If they encounter a person claiming to be from a charity, look to see their ID and collection permit. If in doubt do not contribute and contact Gardaí.

Fraudulent Selling / Trading

What is Fraudulent Selling / Trading?

In these type of cases fraudsters are selling in demand medical supplies or everyday household goods that may be in short supply .They may offer such goods for sale on legitimate 2nd had sales sites, via fake websites created, via cloned websites created to look like legitimate sites or via social media sites. In all such cases the fraudster will ask for the money to be transferred into a bank account, or seek a deposit or even payment up front. These goods are then not delivered or counterfeit goods are delivered.

Advice:

Only purchase from legitimate vendors. Ensure you are on the legitimate sites and not cloned ones. Do your research, open up websites by searching online yourself rather than following links sent you in emails or messages. People are also advised to be wary of rushed offers, time critical selling as these are indicators of potential fraud. system as a result of an email or an unexpected phone call.