

Coronavirus (COVID-19) related scams escalate

Scams related to the Coronavirus (COVID-19) pandemic have escalated in recent weeks with criminals trying a variety of different tactics through texts, emails and phone calls to defraud members of the public by exploiting fears and anxieties as people self-isolate.

Coronavirus (COVID-19) themed scams including cold calls and phishing emails are being reported where criminals are preying on people isolated from their family and friends to trick them into revealing sensitive personal and financial information. One of the recent scam emails pretends to come from organisations asking for donations to help the HSE treat people affected by the Coronavirus (COVID-19) pandemic. The public have been warned to be on their guard and that any money sent will end up in the hands of criminals not the HSE.

Three steps to protect yourself from scams

Step One – Stop!

Taking a moment to stop and think before parting with your money or personal information. Always be suspicious and on your guard to keep yourself safe and protect yourself from scammers.

Step Two – Challenge

Ask yourself - could this be fake? It's OK to reject, refuse or ignore any requests you receive. Only criminals will try to rush or panic you, and something which sounds too good to be true, probably is.

Step Three - Protect

If you think you have been the victim of a scam on the policy you hold with us please contact us using the contact details provided on your policy documents or by using the telephone number shown on the Phoenix Ireland website. Also notify your bank and report to your local Garda station. You can also report to the **Competition and Consumer Protection Commission**.

www.ccpc.ie/consumers/contact/contact-us/

Scams to watch out for

- **Scammers may cold call you** claiming to represent Phoenix Ireland. Cold calls on pensions are illegal. For any calls that come out of the blue asking you to do something or give your personal information, simply end the call and contact Phoenix Ireland using the number on your policy documents or on our website. Criminals are looking to make money by switching your policies or selling your personal information to other criminals.
- As people self-isolate at home there is an increasing risk that **telephone, texts and WhatsApp scams** will also rise, including criminals claiming to be a bank, mortgage lender, utility company, HSE or government department where criminals are trying to obtain personal data to sell on or gain access to your money.
- **Using market volatility around stock markets**, scammers may advise transferring your investments or pensions or offering a 'free' pension review. Remember cold calls on pensions are illegal.

- **Promoting investment opportunities with guaranteed returns.** These are typically unusual and unregulated investments such as property development, hotel rooms, storage units or car parking lots and can be based in the Republic of Ireland and abroad.
- **Offers to ‘unlock’ cash held in pensions.** As people face financial difficulties this may sound attractive, but under 55, customers’ cannot normally access funds without being impacted by severe financial penalties.
- **Email scams that trick people into opening malicious attachments.** These scams put people at risk of identity theft with personal information, passwords, contacts and bank details stolen. Some emails lure people to click on attachments by offering information about people in the local area who are affected by the Coronavirus (COVID-19).
- **Fake online resources, such as false Coronavirus (COVID-19) Maps** that deliver malware such as AZORult Trojan, an information stealing program which can infiltrate sensitive data. A recent example that has deployed malware is ‘corona-virus-map[dot]com’.

Security tips to protect yourself

- **Never share your financial or personal information** to a cold caller, in response to an email or via a text.
- **Check who you are dealing with.** If you receive a call, get as much information as you can about the caller and the company’s background; try searching the internet, but be wary of ‘flashy’ websites. All regulated financial advisers should be registered with the **Central Bank of Ireland**. (<https://registers.centralbank.ie/home.aspx>)
- **If you have been asked to transfer from us** Check the CBI’s **Warning List** (<https://www.centralbank.ie/regulation/how-we-regulate/authorisation/unauthorised-firms/search-unauthorised-firms>) or telephone the CBI General Enquiries Helpline on +353 1224 6000 to check a person is permitted to give pension advice. For transfers to a non UK scheme check the Recognised Overseas Pension Scheme (ROPS).
- **Take your time.** Never be rushed, pressured or harassed into making a decision about your pension. Make all the checks you need - even if this means turning down what seems to be an 'amazing deal'.

For more information on Coronavirus (COVID-19) scams and fraud visit these websites:

Friends Against Scams

https://www.friendsagainstscams.org.uk/article/505/beware_of_covid_19_scams

National Crime Agency

<https://nationalcrimeagency.gov.uk/news/fraud-scams-covid19>

National Trading Standards

<https://www.nationaltradingstandards.uk/news/beware-of-covid19-scams/>

CBI Coronavirus Hub

<https://www.cbi.org.uk/coronavirus-hub/>