Scammers turn level 5 crisis into an opportunity

Unscrupulous operators will always find a way to exploit fears and steal money, writes John Hearne

Whether it's Brexit or Covid, there's always an angle for scammers.

THU, 28 JAN, 2021 - 15:44
JOHN HEARNE

One thing scammers excel at is turning a crisis into an opportunity. Whether it’s Brexit or Covid-19, there’s always an angle for exploiting fears and hoodwinking the most savvy consumer.

Earlier this week, An Garda Síochána, the HSE, and the Department of Health warned us all to be on the alert for a Covid-19 vaccine scam.

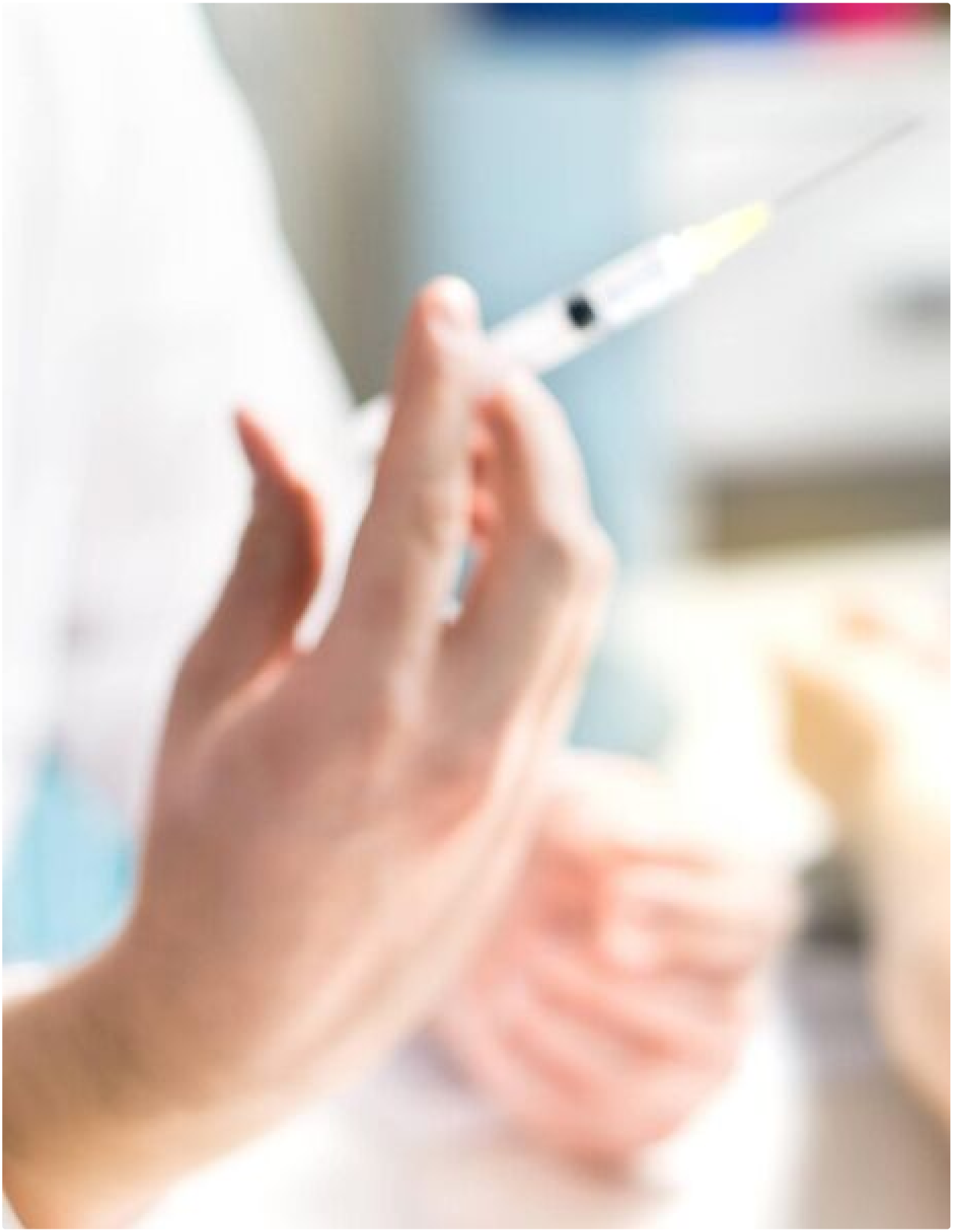
People have been getting fraudulent text messages and calls looking for private information such as PPS numbers, dates of birth, and addresses.

Others have received phone calls asking them to make an appointment for a Covid-19 vaccine jab at a random hospital.

In most cases, these hospitals are distant, and the person will say that they’re not in a position to travel there.

This allows the caller to extract further personal details, and in some cases, people have handed over their home address. In others, they’ve confirmed that they live alone.

It’s at this point that the scammer will offer to come to their home to administer a vaccine.



The HSE will never text or call someone looking for personal information or request payment for a Covid test or vaccine.

The key point here is this: The HSE will never text or call anyone looking for personal information, and they'll never request payment for a Covid test or a vaccine.

Your local GP will be the first point of contact about vaccination or Covid testing. The vaccine is free and is only available through the public health system.

Gardaí are urging the public to make contact with vulnerable friends or family to make them aware of these calls and text messages. And if you get a text of this nature, delete it. Hang up if you get one of these calls.

And if you think you may have given personal information to a scammer, call your local Garda station. If you have questions about Covid testing or vaccinations, contact your GP.

Read More

HSE and Revenue warn of phone scams around Covid-19 vaccinations and wage subsidy

Last week, gardaí issued a warning to online shoppers about further risks to their personal and payment data from a scam which plays on uncertainty around Brexit.

These texts and emails, which look like legitimate messages from courier companies, tell the recipient that they have to pay an additional cost for customs clearance prior to the delivery of their parcel. In some instances, the messages are actually in Irish.

Typically, they'll say something like this: "There is an update on your parcel. Item stopped due to unpaid custom's fee. Follow the instructions here." This is followed by a link, which brings you to a site where you're invited to pay the supposed fee.

> *If you get one of these texts or emails, don't pay, and don't provide any personal details. Take a screen shot and delete the message.*

As before, if you think you may have been a victim of fraud, call the gardaí.

If you get one of these unsolicited messages and you are actually awaiting a package, go and verify the status of their package with the courier. And don't use any of the contact details contained in the message — find them independently.

Never click on links in an unsolicited text or email, never provide payment details or give away personal data like your PIN, card numbers, or passwords. And never open attachments in unsolicited emails.

The upsurge in online buying during the lockdowns has also prompted a lot more fraudulent activity online.

ECC Ireland — which offers advice to Irish consumers shopping in the EU — receives reports, on an almost weekly basis, about online fashion traders who rip off consumers by sending clothes/shoes that are either of inferior quality or the wrong colour/size.

In some cases, people are sent the wrong product altogether, or else they have stains or holes in them.

Not only this, but when consumers try to complain, they often find out that the trader is not actually based in Europe but further afield, then struggle to get a response or adequate refund or replacement.

Some have even returned the offending item, at their own expense, never to hear from the trader again.

Read More

Pandemic prompts 40% surge in new Munster websites

ECC Ireland has also seen instances where bad reviews on sites such as Trustpilot and Scamadviser prompt the scammer to simply change their trading name and carry on regardless.

Always check the domain name when you're buying from a site you haven't used before. This is the central section of the web address.

Dodgy sites

Dodgy sites sometimes use a recognisable company name, but that name may not appear in the domain name itself.

Beware too a domain which ends in .net or .org; these are rarely used for online shopping by legitimate sites.

Make sure the site has a real world address, and not just a web presence. The trader is legally obliged to provide a full name, address, and contact details.

An email address or a contact form is not good enough. If you can't find these details, there may be something fishy going on.

> *Use your instincts, just as you would when buying in any other context.*

It's a good idea to shop from sites based in the EU. That way, you'll enjoy the additional layer of protection EU legislation gives.

Note too that just because a website address ends in '.ie' doesn't necessarily mean the website is based in Ireland. Check the postal address of the seller before buying.

ECC Ireland and the rest of the ECC-Network has also received numerous reports from consumers who have been blindsided by dodgy social media pop-ups and other similar advertising.

While the majority of these complaints have involved beauty products, others have been in relation to health-related items and even credit cards.

Pop-up ads

In a bulletin, ECC Ireland says: "The modus operandi is that consumers are attracted by this shiny enticing pop-up ad, which maybe promotes a 'special offer' or 'free trial', or it's something that you can only get from these guys, and maybe for a limited time.

"The consumer is interested, clicks to find out more, might enter details such as a name, email and address, but then doesn’t continue with the purchase and doesn’t enter into a contract.

"However, some time later, unsolicited goods arrive on the doorstep along with a demand for payment and sometimes even a threat of debt collectors if this is not paid."

"Some consumers have not even provided the trader with a postal address, only an email, and then they receive an email with an invoice claiming that a contract had been entered into and that payment needs to be made."

If you’ve fallen victim to one of these special offers, remember that you do not have to pay for or return a package that you haven’t ordered.