**COVID-19 RELATED SCAMS**

The World Health Organisation (WHO) has reported a [fivefold increase](https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance) in cyber attacks and scam emails since the start of the COVID-19 pandemic. The public are urged to be wary of emails claiming to be from the WHO asking for donations to fake charities - read more about charity scams below.

The National Cyber Security Centre's [Cyber Aware](https://www.ncsc.gov.uk/cyberaware) campaign offers advice to the public on staying safe online - suspicious emails can be forwarded to their [Suspicious Email Reporting Service](https://www.ncsc.gov.uk/information/report-suspicious-emails).

Stay safe while online at home and report all scams to [Advice Direct Scotland](https://coronavirusadvice.scot/) on 0808 164 6000.

**Business Scams**

The [Highland Council](https://www.highland.gov.uk/news/article/12466/highland_council_warns_of_business_grants_scam)has warned local businesses about scam emails which inform the business that their grant application has been processed and that they will receive a payment soon. The email provides bogus contact details to use if the payment is not received in the hope that companies will call and provide their financial details. A number of similar scams have been reported across the UK, with fraudsters contacting businesses by email, text or phone to tell them that they qualify for a particular grant or tax refund.

The UK Government have published a [list of their current messages](https://www.gov.uk/government/publications/genuine-hmrc-contact-and-recognising-phishing-emails/genuine-hmrc-contact-and-recognising-phishing-emails) so that you can recognise genuine contact. The website also includes advice on recognising fraudulent emails and [examples](https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples)of the most common phishing messages which claim to be from HMRC.

Always question unexpected emails which request payment details or changes and report fraudulent emails to Advice Direct Scotland on 0808 164 6000 or through their [website](https://www.consumeradvice.scot/).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Useful Guidance for Businesses**

With more and more people working from home, online security has become a pressing issue, particularly when using video conferencing.

The National Centre for Cyber Security (NCSC) has published [security guidance](https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations) to help organisations choose, configure and safely use video conferencing services. They also have separate guidance for [families and individuals](https://www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely) using these services.

The [Scottish Business Resilience Centre](https://sbrcentre.co.uk/) (SBRC) have a variety of resources to support and protect Scottish businesses, including:  [Guidance on using Zoom](https://www.sbrcentre.co.uk/media/4944/sbrc_zoom_conferencing.pdf) for business and [video conferencing basics](https://www.sbrcentre.co.uk/media/4947/sbrc_video_conferencing-1.pdf), [Recordings of webinars](https://www.sbrcentre.co.uk/news/2020/march/catch-up-on-the-latest-sbrc-webinars/) on subjects such as counterfeit goods and cyber scams

[Business Gateway](https://www.bgateway.com/) have advice and a range of useful resources to help you keep your business safe online.

[Electrical Safety First](https://www.electricalsafetyfirst.org.uk/media-centre/press-releases/2020/04/how-safe-is-your-work-from-home-setup/) have published guidance on working safely at home. Remember that 98% of counterfeit chargers do not conform to UK safety standards and could cause a fire or electric shock. Use the[Vistalworks](https://vistalworks.com/blog/keeping-consumers-safe-vistalworks-update)checker to make sure that electrical products purchased online are genuine.

Find [guidance on accessing support](https://www.gov.scot/news/lifeline-support-for-business-confirmed/) for the newly self-employed and firms suffering hardship from the Scottish Government.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**National Cyber Security Centre (NCSC)**

**Joint Advisory issued**

The National Cyber Security Centre (NCSC) and Cybersecurity & Infrastructure Security Agency (CISA) continue to see indications that Advanced Persistent Threat (APT) groups are exploiting the COVID-19 pandemic as part of their cyber operations and have issued a second joint advisory. The joint NCSC/CISA advisory from 8 April 2020 detailed the exploitation of the COVID-19 pandemic by cyber criminals and APT groups. This joint NCSC-CISA advisory provides an update to ongoing malicious cyber activity relating to both national and international COVID-19 responses. Organisations at risk include healthcare bodies, pharmaceutical companies, academia, medical research organisations, and local government. The document describes some of the methods criminals are using to target organisations and provides mitigation advice.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Trending Topics**

**Communicating online during COVID-19**

We all remain separated from loved ones due to physical distancing, and many of us are keeping in contact with each other through online communication; for example, through video chats. We have heard of people lending devices to older relatives, or dropping them in to care homes, for example, to enable this contact.

Please remember that devices should be secured with a password (ideally three random words), and that care should be taken when joining WiFi. WiFi in public settings should be password protected as well.

The NCSC offer a wealth of advice and guidance relating to such matters as the use of passwords and the use of devices such as mobile phones and tablets; and specific guidance relating to common questions (for example, relating to the use of WiFi).

**NHS Covid symptom tracker app – NCSC security**

Experts from the National Cyber Security Centre have been supporting the development of the NHS COVID-19 contact tracing app, which will be launched on the Isle of Wight this week. The privacy and security of app users’ data is a priority and the NCSC has been advising on best practice throughout the app’s development. They have published three documents relating to the work, including a technical paper which provides a high-level overview of the security and privacy characteristics of the app.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Doorstep Scams**

Despite the lockdown, doorstep scammers are still active in communities across Scotland. In addition to scams related to COVID-19 such as offering to disinfect driveways or posing as charity workers and NHS staff, more traditional doorstep scams are continuing.

We are aware of fraudulent aerial installers who are continuing to visit consumers and overcharge for work. The [CAI have guidance](https://cai.org.uk/index.php/contact/news/256-coronavirus-update-cai-members-update)for telecommunications engineers who are working during the quarantine period. If you require the services of an installer/engineer, find a trusted local professional through the [Get Me Viewing](https://www.getmeviewing.org.uk/) or [Get Me Digital](http://www.getmedigital.com/) websites.

If you need to call a trader for emergency repair work during the quarantine, find someone who has been vetted and approved through a national or local authority [trusted trader scheme](https://www.tsscot.co.uk/consumer-advice/approved-trader-schemes/).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 **General Advice for Avoiding Doorstep Scams**

Remember - you are not being rude if you shut the door on unsolicited callers. Don't agree to make any payments for goods or services offered by cold callers.  If you feel feel uncomfortable or suspicious, call Police Scotland on 101. If you feel threatened or unsafe at any time, call 999.

Report rogue traders to Advice Direct Scotland on 0808 164 6000 or through their [website](https://www.consumeradvice.scot/)

Sign up for [Neighbourhood Watch Alerts](http://www.neighbourhoodwatchscotland.co.uk/sign-up-for-alerts) to stay up to date with what is going on in your community. Keep an eye on vulnerable neighbours.

Keep an eye on vulnerable neighbours and sign up for [Neighbourhood Watch Alerts](http://www.neighbourhoodwatchscotland.co.uk/sign-up-for-alerts) to stay up to date with what is going on in your local area.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Charity Scams**

There have been reports of calls claiming to be from the 'Corona Charity Fund' which make claims about the expected death toll in UK and ask for a donation to charity.

As well as cold calls, there are numerous websites posing as charities who are fundraising to help victims of COVID-19 or to support health services. Consumers are also receiving emails and visits from fraudsters posing as charity workers. Emails may seem genuine, with official-looking Government or NHS logos and seek to exploit the public's desire to support NHS staff. They may ask for donations to help purchase medical supplies or to fund mental health support initiatives for NHS staff.

Be particularly wary of bogus charity emails which request donations via bank transfer or gift card - genuine charities will not ask for donations in this way.

**Find Genuine Information**

The World Health Organisation have only issued one appeal for donations: to the [COVID-19 Solidarity Response Fund](https://www.who.int/emergencies/diseases/novel-coronavirus-2019/donate). Any other charity appeals which claim to be related to the WHO may not be genuine.

If you're unsure whether a charity is genuine, search for it through the [Scottish Charity Register](https://www.oscr.org.uk/) or the [Charity Commission](https://www.gov.uk/government/organisations/charity-commission)

Report scam messages to Advice Direct Scotland on 0808 164 6000 or through their [new website](https://coronavirusadvice.scot/) dedicated to COVID-19

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Supplier Mandate Fraud**

Businesses, charities and individuals should be wary of fraudulent emails which appear to be from trusted suppliers or companies advising that their bank account details have changed. The recipient is asked to make future payments to a new bank account, which is often run by fraudsters.

The UK Government has issued [advice for charities](https://www.gov.uk/government/news/coronavirus-covid-19-increased-risk-of-fraud-and-cybercrime-against-charities) to help them avoid cyber crimes and mandate fraud.

**What to Do**

Confirm requests for changes to payment details with the person or company who has supposedly sent them, using contact information that you know to be correct.

Always question unexpected emails which request payment details or changes and if in doubt, get a second opinion from a colleague or manager.

Report fraudulent emails to Advice Direct Scotland on 0808 164 6000 or through their [website](https://www.consumeradvice.scot/).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Official Contacts**

If you feel threatened or unsafe, contact [Police Scotland](https://www.scotland.police.uk/keep-safe/personal-safety/shut-out-scammers) on 101 or 999 in an emergency.

Report scams to [Advice Direct Scotland](https://coronavirusadvice.scot/) on 0808 164 6000.

Sign up to the [Neighbourhood Watch Alert](https://www.neighbourhoodwatchscotland.co.uk/sign-up-for-alerts) system to receive localised information and updates.

**Get genuine information and updates about the COVID-19 pandemic from official websites:**

[Scottish Government](https://www.gov.scot/coronavirus-covid-19/) - Coronavirus in Scotland

[NHS Scotland](https://www.nhsinform.scot/coronavirus) - Coronavirus information and advice

[UK Government](https://www.gov.uk/government/topical-events/coronavirus-covid-19-uk-government-response) - Response to Coronavirus

[World Health Organisation (WHO)](https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance) - Technical Guidance

PC6444A Mike Urquhart

Crime Reduction Officer

Aberdeenshire South

Stonehaven Police Station

Dunnottar Avenue

Stonehaven

01224 304101

Website: <http://www.scotland.police.uk/>
Twitter: @policescotland
Facebook: [www.facebook.com/policescotland](http://www.facebook.com/policescotland)