|  |
| --- |
| **THURSDAY 30 APRIL 2020****CURRENT COVID-19 FRAUD RISKS**  |
| * Payment diversion / mandate fraud
* Identity fraud
* Misinformation campaigns (esp. ‘cure’-related)
* Malware attached to coronavirus trackers
* Online shopping fraud (esp. pets who the fraudsters claim are in quarantine)
* Investment fraud
* Pension liberation fraud
* Data breaches (esp. unsecure video conferencing systems and failing PCI DSS)
* CEO fraud
* Phishing emails (generally)
 |
| **ANTICIPATED AND/OR EMERGING ISSUES** |
| * Spread of misinformation about coronavirus cures. For example in the Middle East an email purporting that methanol is a cure led to at least 700 deaths.
* Government support scheme frauds (incl. business interruption and the small business fund).
* Serious Organised Crime Groups using COVID-19 as a hook for future frauds.
* Increases in pension and investment frauds linked to the economic recovery.
* Phishing emails related to the Self-Employment Income Support Scheme (SEISS).
* Bogus claims for the CV Job Retention Scheme (CJRS).
 |
| **SOME SIMPLE PREVENTATIVE TIPS …** |
| * Suspicious emails should be sent to the NCSC at report@phishing.gov.uk
* Fraud Advisory Panel helpsheet on invoice fraud. Available [here](https://www.fraudadvisorypanel.org/wp-content/uploads/2019/04/Invoice-Fraud-April-2019.pdf).
* The ICAEW IT Faculty is running a free webinar on 12 May on ‘five steps to cyber hygiene for the smaller firm’ which will include the latest COVID-19 guidance from the National Cyber Security Centre, available [here](https://events.icaew.com/pd/16730).
* When using video conferencing platforms:
	+ Use additional security (such as 2FA).
	+ Do not share confidential information.
	+ Follow Zoom [guidance](https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf) on best practice.
	+ Follow the NCSC best practice [guidance](https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations).
 |