



Business Fraud

Network

Regular news and updates on the most recent fraud threats



TUESDAY 10 JANUARY 2023

In this update we highlight emerging fraud threats to businesses (especially SMEs) and offer practical advice on prevention. It is based on pooled intelligence shared by members of our Business Fraud Network which meets every six weeks.

We encourage all businesses – and everyone who works with them or otherwise supports them – to read, share and act on these updates.

CURRENT RISKS

- **Action Fraud received 2,901 fraud reports from business in December (down 12% on the previous month).** 100 reports came from sole traders, 830 from SMEs and 1,729 from large business. Reports of retail fraud exceeded online shopping and auction frauds. There were increased rates of reporting in the finance, transport and insurance sectors.
- **Action Fraud received 142 cybercrime reports from business in December (up 8.3% on the previous month).** SMEs made up 87.3% of reports. The most common frauds reported were business email compromise which increased 35% (nearly half of these involved invoice fraud) and/or social media account takeover).
- **There were 33 reports of ransomware attacks in December (up 125% on the previous month).** Three new variants of ransomware have been detected. Last year 39% of cyber-attacks were perpetrated against business; 8 in 10 were phishing emails.
- **Social media adverts promising incredible investment opportunities.** 89 out of 484 investment adverts reviewed showed three or more markers for high-risk misleading content indicating a possible scam. It is extremely difficult to report these adverts and have them removed from social media.
- **There has been an increase in investment fraud, and retirement savings are increasingly vulnerable to investment scams.** There has been a drop in pension liberation scams in recent times. However, reporting of pension frauds remains low.

ON THE HORIZON

- **Business email compromise is a continuing risk.** In some cases, the stolen funds are used to purchase high-value items and goods that can be sold on later.

- **Pension fraud.** Involving firm cloning and crypto currencies are increasingly threatening the retirement funds of staff.

COMING UP ...

- The Fraud Advisory Panel is hosting a free webinar, in collaboration with ICAEW on **why cyber security makes good business sense** (13:00 Tuesday 14 February). Guest speakers include Lauren Coward, Siobhan McCrea and Charlie Morrison from the City of London Police and Esther Mallowah from ICAEW.

TAKEAWAYS FOR BUSINESS

1. Check the **security settings on your business email** and social media accounts regularly to keep your cyber perimeter secure.
2. Make staff aware of the risks they face from pensions-related investment scams.
3. Read the research by *Which?* in partnership with Demos Consulting on **tackling misleading and fraudulent adverts online**.
4. Check out the advice from NCSC on **checking your supply chain security**.