



Business Fraud

Network

Keeping a watching brief on
new and emerging threats



TUESDAY 22 NOVEMBER 2022

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 3,291 fraud reports from business in October (up 5.86% on the previous month).** The most common frauds reported were still bank-related (cheque, plastic card, online), followed by retail and online fraud, mandate fraud, online shopping and auction fraud. About 126 reports were received from sole traders and micro businesses, 1,104 from SMEs, and 1,723 from large businesses.
- **Action Fraud received 134 cybercrime reports from business in October (a 4% decrease on the previous month).** About 54% of reports were received from businesses with a turnover of less than £1.5m.
- **Over 15m suspicious emails have been reported since April 2020 to report@phishing.gov.uk.** This has resulted in the take down of more than 184,000 online scams.
- **Cuckooing and misuse of registered office addresses.** Companies House advanced search facility can be used to identify these.

ON THE HORIZON

- **Energy bill frauds associated with the** government's support scheme may give rise to text and phishing scams. Businesses should be alert to possible scams.
- **Online shopping fraud.** In the lead-up to Black Friday (25 November), Cyber Monday (28 November), and the busy Christmas shopping period.

COMING UP ...

- From 05 December until 28 February 2023 the business fraud campaign will be focussing on how to prevent cybercrime. A new guide, checklist, and top tips video will be available to use and share from the website www.lovebusiness-hatefraud.org.uk. [Supporter packs](#) (containing social media cards and suggested posts) will also be available for anyone wishing to get involved.

TAKEAWAYS FOR BUSINESS

1. Business should regularly check their records at Companies House to make sure they are up-to-date and accurate.
2. Watch the Fraud Advisory Panel's on-demand webinar on [how to buy goods and services safely: what to check and how to check it](#) for ways to check publicly available sources.
3. Get involved with NCSC's [Cyber Aware](#) online shopping campaign in the run-up to Christmas to protect your customers online purchases. It will focus on the importance of passwords comprising three random words, using 2-step verification (2SV) and reporting suspected frauds to the police.
4. Creating a strong anti-fraud culture can be hugely beneficial. Evidence suggests it raises awareness about internal and external frauds and leads to increased prevention and internal reporting.
5. Remember: trust isn't a defence against fraud and is not an anti-fraud control.