



Business Fraud

Network

The early warning system
for business fraud



TUESDAY 16 May 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 3,447 fraud reports from business in March.** The most common frauds reported continue to be bank-related (cheque, plastic card, online), followed by retail fraud and Online Shopping and Auction Fraud.
- **Action Fraud received 212 cybercrime reports from organisations in March (up 12% on the month before).** 162 of these reports came from SME's and micro business. There were 82 reports of business email compromise a 4% increase on the month before. The sector with the most reports was construction.
- **Ransomware reports were up 40.6% on March.** Eight new variants have been isolated. However, no losses were reported. This likely does not show the true losses but rather, shows victims reluctance to share loss figures with law enforcement.
- **Fake reviews** particularly on online platforms are being notice more and could be damaging small business.

ON THE HORIZON

- **Failure to prevent fraud offence.** The government's proposed new offence currently applies to larger organisations only, although this is subject to ongoing parliamentary consideration. Keep up to date with this as it progresses.
- **Business email compromise** has doubled from 2021 to 2022. Phishing emails are the leading ways that fraudsters gain access to email and social media accounts. BEC is "the largest monetary threat to organisations".

COMING UP ...

- The [Managing fraud risk guide](#) is now live! Visit www.lovebusiness-hatefraud.org.uk for all the guides and supporter packs.

TAKEAWAYS FOR BUSINESS

1. Check out the NCSC's [cyber advisor scheme](#) that provide cyber security guidance, and practical hands-on help, that small organisations can trust.
2. Keep your team's phishing training up to date and if you are spotting a trend in phishing messages make your team aware.
3. Use the new [Cyber action plan](#) from Cyber Aware to receive a personalised guidance for you and your business.
4. Review the advice from your local cyber resilience centre.
5. Check out the new [Managing fraud risk guide](#).