Business Fraud Network

Regular updates on new and emerging fraud threats

Love business Hate fraud

TUESDAY 21 February 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 3,192 fraud reports from business in January (up 9.73% on December). 1,197 reports were made by SMEs and sole traders. The most common frauds reported were cheque, plastic card and online bank account, mandate fraud, online shopping and auction fraud. Sole traders saw a high percentage of Consumer Retail Fraud reported.
- Action Fraud received 1,855 cybercrime reports from business in January (a 12.6% increase since December). There was a 75.5% increase in business email compromise compared to December. Of the reported cybercrime 41.8% was Invoice Fraud. The construction sector was the most targeted sector.
- There is continued under reporting from SMEs when it comes to Social Media Hacking making up only 7.1% of reports.
- Firms are seeing a continuing risk of misappropriation of assets, often driven by fraudsters need to maintain their lifestyle.

ON THE HORIZON

- Businesses are expected to be targeted by an influx of 'tax refund' phishing scams. A scam posing as HMRC has already been seen targeting the public on social media platforms like Facebook.
- The cost of living crisis continues to be viewed as an emerging risk that could drive increased fraudulent behaviour.

COMING UP …

- From 06 March the business fraud campaign will focus on how to manage the risk of fraud. A supporter's pack and new guidance will be available shortly from website www.lovebusiness-hatefraud.org.uk.

TAKEAWAYS FOR BUSINESS

1. Check out your businesses IP address and browser security with the NCSC's new cyber security service (it is free and easy to use). https://checkcybersecurity.service.ncsc.gov.uk/
2. Check your company accounts regularly. Whether it's a bank account or payment service take the time to check the money coming into and out. If something seems odd question it!
3. Keep an eye on your invoices. If prices seem to be inflating rapidly, question it. Inflation may not be the only cause.
4. Business is encouraged to report fraud or cybercrime to Action Fraud.