Business Fraud Network

Identifying new fraud threats as they emerge

Love business Hate fraud

TUESDAY 4 April 202

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 3,164 fraud reports from business in February, which accounted for around £32.6 mil in reported losses. The most common frauds reported were still bank-related (cheque, plastic card, online), followed by retail fraud.
- Action Fraud received 189 cybercrime reports from organisations in February. About 80% of reports were received from SMEs. The construction sector saw the highest number of reports. Business email compromise is still the most reported cybercrime. Ransomware attacks were also up 60% on the month.
- A new trend in social media hacking has been identified. Business are receiving emails requesting social media platform verification or response to a copyright strike. Once details are given the hacker(s) are holding the business' social media hostage until a ransom is paid.
- Continuing concerns over insider fraud. Staff fraudulently expensing personal items, ranging from meals to luxury holidays. When the larger expenses were caught it often transpired that the fraud started on a smaller scale.

ON THE HORIZON

- Big changes to the work force. With new staff joining and old staff leaving, corporate knowledge may be lost and a shift in culture could lead to further instances of insider fraud, often arising as a result of staff dissatisfaction.

- The cost of living continues to be a growing risk to staff and business. The deepening financial pressure is already leading to staff making choices they wouldn't otherwise, such as onboarding fictitious companies and adding family members to payroll.

- The proper use of AI has the potential to maximise business efficiencies however, as it rapidly develops, it could also pose a fraud risk. As businesses are increasingly exposed to AI tools, they may starts to access unknown and possibly untrustworthy websites in order to use them. Scammers are also utilising these tools. One recent risk includes use of voice cloning tools to impersonate managers, colleagues or even family members for fraudulent purposes.

COMING UP …

- The Managing fraud risk guide is now live! Check out www.lovebusiness-hatefraud.org.uk for all the guides and supporters packs.

TAKEAWAYS FOR BUSINESS

1. Check your onboarding process, for staff and contractors, are up to date and being followed. Also check your suppliers also have appropriate checks for their staff and contractors to limit frauds in the supply chain.
2. Consider your cyber insurance plan.
3. Creating a strong anti-fraud culture can be hugely beneficial. Take the time to gauge staff satisfaction, it may save you in the future.
4. Use the new from Cyber action plan Cyber aware to receive a personalised guidance for you and your business.
5. Check your cyber security with the NCSC's free new tool.
6. Check out the new guide Managing fraud risk guide.