Business Fraud Network

Identifying new fraud threats as they emerge

Love business Hate fraud

TUESDAY 19 JULY 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 363,000 reports last year. One-in-ten were from business. Of these, c.36,000 reports were related to fraud, another c.3,000 were about cyber-dependent crimes. Action Fraud statistics are available online.
- Reports about fraud on social media and communications platforms have increased 84% in the last year (to 138,000). Overall, 1,200 reports were received from business stating that their social media account had been hacked, with 44% from micro businesses (with 9 or fewer staff). Commonly fraudsters take over a business's social media account and uses it to target customers and suppliers.
- Payment diversion (also known as mandate fraud) is still prevalent and sometimes involves business email compromise as well (in about 37.5% of reports). Fraudsters compromise a business's email system and uses it to target staff, suppliers or customers to divert payments.
- A current increase in purchase scams is thought to be driven by businesses seeking to obtain value for money in the current financial climate.
- Ransomware is the most significant cross-sector threat to business. Reports to Action Fraud have increased by 8.5% in the last year. Increasingly, threats to publish data and/or intellectual property online are accompanying ransomware attacks.
- There has been a re-emergence in cheque frauds involving minor alterations to amounts, names or Magnetic Ink Character Recognition (MICR) lines.
- Invoice fraud and authorised push payment frauds. Overall £100m was lost to cheque, plastic card and online bank account fraud last year.

- Vishing (bank impersonation) frauds. Customers receive a call from a fraudster pretending to be from their bank who asks them to download a remote access tool to gain access to their computer. They are then guided through making a series of payments.
- New variation of the CEO scam. A fraudster pretends to be the chief executive and asks a staff member with a corporate card to purchase vouchers to reward staff. The fraudster then requests the code from the voucher to make purchases of between £800 to £6,000.

ON THE HORIZON

- Staff (insider) fraud is expected to increase with more staff working remotely (with less oversight), and personal finances impacted by the cost-of-living crisis and inflation hitting a 40-year high. This will heighten the opportunities, motives and justifications for committing fraud. Action Fraud received 750 reports of insider fraud last year with losses of £40m.

COMING UP …

- The Fraud Advisory Panel is hosting a free webinar on why preventing fraud makes good business sense (2 August). Guest speakers include SME business owner Paul Mason and Neil Sharpley from the Federation of Small Businesses.

TAKEAWAYS FOR BUSINESS

1. Be cautious about accepting invitations to connect to people you don't know on professional social media networking sites – regardless of who they say they are and who they are connected to. Fraudsters are known to set up fake profiles and seek connections with genuine professionals to make themselves – and their activities – look more legitimate.
2. To reduce the risk of business email compromise and payment diversion fraud, think 'three random words' for password security, independently verify payment requests (using contact details held on file) before making payment, and implement two-factor authentication for fund transfers and account access.
3. Do not rely solely on confirmation of payee to protect against payment fraud. It is still important to conduct independent verbal checks using contact details held on file.
4. Read our guidance on buying goods and services safely.
5. Conduct a fraud risk assessment across your business to identify potential risks. Use your internal audit team to do this (if you have one); otherwise get your managers involved.
6. Encourage your board/audit committee and senior managers to ask more questions about fraud. It is important for everyone to be fraud aware.
7. Encourage your internal audit team to read the Chartered Institute of Internal Auditors new research reports on cyber security and fraud.

8. Consider using the National Cyber Security Centre's (NCSC) 'exercise in a box' tool to find out how resilient you are to cyber-attacks and to test your response in a safe environment. It includes exercises specifically for SMEs.
9. Read the new guidance for business leaders, practitioners and suppliers on protecting your supply chain from the Centre for the Protection of National Infrastructure, Department for International Trade and Chartered Institute of Procurement and Supply. The NCSC also has a helpful infographic.
10. **IT managed service providers (MSPs) and their customers:** read and follow the NCSC's practical steps to protect against cyber threats. This advice is issued in the wake of increased malicious activity targeting MSPs.