Business Fraud Network

The early warning system for business fraud

Love business Hate fraud

TUESDAY 11 OCTOBER 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 3,114 fraud reports from business in September (down 16% on last month). The most common frauds reported were bank-related (cheque, plastic card, online), followed by retail and online fraud and mandate fraud. About 125 reports were received from sole traders and micro businesses, 1,000 from SMEs, and 1,800 from large businesses. Most reports came from the finance and insurance sector, followed by retail and transport and storage.
- Action Fraud received 140 cybercrime reports from business in September (up 21% on last month). Some of these were reclassified as fraud after assessment. The most common cybercrimes reported were social media and email hacking (38% of reports). Overall, 41% of reports were received from businesses with a turnover of less than £1.5m.
- There has been a 21% increase in reports of ransomware compared with the previous month.
- A lack of regulation and industry standards makes the open display advertising market (online digital advertising) attractive for sophisticated fraudsters. As part of Which?'s advocacy work protecting consumers from online fraud they commissioned Beruku to look into fraudster's behaviour in the online advertising display market. One example showed fraudsters have business models in place that make them $1m in a single day. The research highlighted that industry experts believe less than 1% of the digital advertising industry is fortified against fraud. Fraudsters easily create fake media agencies that place adverts across reputable websites to draw in potential victims. Which? is calling for more statutory regulation, due diligence checks, and information-sharing within the industry to prevent fraudulent online advertising.
- Impersonation of helpline advisers to enhance credibility of investment scam emails. One professional body has received an unusual number of enquiries originating from countries in Eastern Europe about potential money laundering risks associated with money transfers to cryptocurrencies. After

responding to these they have now found their staff impersonated within subsequent emails to potential victims to add an air of legitimacy to the fraud.

ON THE HORIZON

- Staff fraud. As people feel the effects of the cost-of-living crisis on their finances.
- Ransomware, particularly targeting network-attached storage. There has been a recent increase in these types of attack.
- E-commerce / online shopping fraud. In the lead-up to Black Friday (25 November), Cyber Monday (28 November), and the busy Christmas shopping period.
- Supply chain fraud. As some businesses and individuals find themselves in financial difficulty. To boost resilience, government is looking to create standard templates for supply chain contracts.

COMING UP …

- The Fraud Advisory Panel is hosting a free webinar on practical steps to buying goods and services safely: what to check and how to check it (13:00 Friday 14 October). Guest speakers are Laugh Hough from BDO's International Institutions and Donor Assurance Group, and Joanna Kozlowska and Christophe Pflieger from BDO's Corporate Intelligence team.
- The Fraud Advisory Panel is hosting a free webinar on practical steps to avoid staff fraud (18:00 Thursday 27 October). Guest speakers include Tracey Carpenter, the insider threat manager at Cifas, and David Kearns, managing director of Expert Investigations.
- Until 30 November the business fraud campaign is focussing on how to prevent staff fraud and avoid card-not-present fraud when selling goods and services online, over the phone or by mail order. The new guides, checklists, and top tips videos are available to use and share from the website www.lovebusiness-hatefraud.org.uk. Supporter packs (containing social media cards and suggested posts) are also available for anyone wishing to get involved.

TAKEAWAYS FOR BUSINESS

1. Use the new website checking tool www.getsafeonline.org/business/checkawebsite to see whether a website is likely to be genuine or a fraud before you visit it.
2. Listen to the new podcast cybersecurity is everybody's business from Get Safe Online to hear about some of the latest threats to business.
3. If you operate a helpline, be careful about the advice you give and how it might subsequently be used by the recipient. Also consider whether the full names of staff should be included within responses.
4. As the cost-of-living crisis deepens it is important for businesses to review their fraud risk assessments and insurance arrangements. From an insurance perspective, make sure you're clear

what is and is not covered by your policy. Understanding the risks and educating staff about them are key aspects of fraud prevention.

5. Read the National Security Centre's guidance on choosing the right type of authentication for your organisation. This is aimed primarily at retailers, hospitality providers and utility services but will be of interest to any business that wants to authenticate customers who are accessing their online services.

6. Find out how to protect your brand from being exploited online and the steps you can take to remove fake websites and social media accounts, adverts and/or campaigns by reading the NCSC's new guidance for business.

7. Keep an eye out for the NCSC's Cyber Aware online shopping campaign in November to protect your customers online purchases. It will focus on the importance of passwords comprising three random words and using 2-step verification (2SV).

8. Read the NCSC's new guidance to secure your supply chain.