cifas
The UK's Fraud Prevention Community

Fraudscape 2022

Observations

Identity fraud

- Criminals are taking advantage of the rise in living costs by targeting consumers with smishing campaigns by claiming to be from Ofgem and gov.uk claiming the recipient is entitled to the energy support scheme. Between May and August, research shows that more than 7 in 10 people have been targeted by scams such as false discounts from energy and insurance companies and social media adverts offering money off shopping and bogus investments using celebrity endorsements.

- Criminals have been posing as network providers and/or phone dealers to offer deals for customers such as rewards for loyalty or opportunities to get a better deal on their contract. Once these details are harvested, criminals order devices in the consumer's name.

- New dual attacks are being used to target victims. Known as "call phishing", a victim will receive an email which often has an invoice attached for some goods or services. They are then told to call a number to challenge the invoice, where they are either manipulated into revealing personal and financial information, or download remote access software to give the criminal access to their computer.

- As the new booster for COVID 19 is rolling out, it is anticipated there will be a rise in COVID19 related smishing scams.

- As the public seek to supplement incomes or bolster their pensions, investment scams continue to be a concern. Criminals have been posing as investment firms providing opportunities to invest and harvesting personal and financial information from victims under the guise of opening a crypto-wallet. The criminals then set up a "training" session with the victim and share their screen which shows the victim a fake site to make them think the money is being transferred into their new crypto-wallets.

Misuse of facility

- As households feel the economic strain, many may be tempted to supplement their income. A number of social media platforms, including LinkedIn are being abused to offer opportunities to work from home and make money quickly. There has been an uptick in posts targeting those in financial difficulty, in particular, single parents.

- More companies are looking to expand their portfolio into the Buy Now Pay Later space. For businesses new to this arena, criminals will look to exploit any vulnerabilities within their processes.

- Fraudulent claims for chargebacks have increased by 172% in the first nine months of 2022 as consumers look for ways to recoup money. Some transactions are historic and the use of third party claims management companies have grown. In some circumstances, customers are being coached what to say to support the dispute and instructed to avoid contacting the bank directly.

Facility takeover

- Smishing has been a key enabler to gain access to accounts. Often purporting to be the bank, they are stating a new device has been set up or a payment has been made and they are asking the user to provide further details by clicking on a link.

- The use of BOT technology to target organisations to gain access to accounts continues. 6.7% of UK internet traffic in 2021 was a bad BOT –software applications that run automated tasks with malicious intent. They scrape data from sites without permission and steal customer credentials. Quite often, these are used for the purpose of account takeover and hide as browser extensions and through apps. Over a third of these targeted financial services (34.6%), with other industries including retail (8.1%), telecoms (5%) and law and government (2.8%).

- Not all account takeovers are enabled by the use of technology and cyber. There has been an increase in people trying to access the accounts of others, calling the service provider to state they are the genuine account holder and submitting letters asking for details such as correspondence address and mobile number to be changed.

False applications

- As the rise in living costs takes hold, false bank statements and unverified HMRC returns are being provided to support higher earnings in attempt to gain access to products and services. These documents tend to be manipulated using PDF editor software. As lenders tighten their criteria, there may be individuals looking for ways to improve their acceptance prospects with false documentation.

- The use of unregulated brokers to make applications is of concern, as they may charge higher fees to consumers and then supply false documentation with inflated income to apply for products and services.

Insider threat

- As households struggle with the rise in living costs, employees may look for ways to supplement their income by abusing company processes, such as overclaiming overtime or expenses, and providing false documents to facilitate expense claims. Examples include cancelling hotel bookings and asking for the refunds to be directed to personal accounts or submitting false payment dispute claims.

- As households feel economic strain, individuals may be tempted to take out second jobs to help supplement incomes. As employees look to balance their time, employees have been committing work avoidance with one employer to advertise appointments for their second job during their primary work hours and poaching customers for their new roles.

- With hybrid and remote working, offboarding of staff is just as important as onboarding. There has been an increase in report of theft of equipment, with devices such as laptops or phones not being returned by staff who have left the organisation. In some cases these devices have been sold on via online marketplaces.


cifas
The UK's Fraud Prevention Community
www.fraudscape.co.uk