IDENTITY FRAUD

Specialist police units and fraud prevention agencies are spearheading a campaign to convince consumers to protect themselves from identity fraud. Marcel Le Gouais reports

Identity fraud will remain a potent threat to lenders and suppliers this year, a fact backed up by a 27 per cent increase in cases during the first quarter of 2015.

This figure comes from Cifas, the not-for-profit fraud prevention service that is now leading a campaign to raise awareness among consumers, and to encourage more vigilance by individuals to protect their own data.

The problem is evident in the organisation’s research, which shows that one in four UK adults – 12.275 million people – is believed to have fallen victim to identity crime. Those victims have lost on average £1,200 each, with total losses to UK adults estimated at £3.3bn.

The study, which involved a survey of more than 4,000 UK adults earlier this year, claims that millions of Brits are failing to take basic steps such as updating firewalls to protect their identities. In each case below, it found that one in three people:

- Do not regularly update their firewall or antivirus software;
- Do not limit the amount of information they share on social media;
- Do not shred letters before throwing them away.

Cifas also calculated that the average age of a victim of ID fraud is 46, with men being 1.7 times more likely than women to have their identity stolen. The findings prompted the launch by City of London Police, Cifas and partner agencies, of the Not With My Name campaign to target identity crime.

Campaigners have been urging people to protect personal data by creating safe passwords, protecting internet devices and rejecting unsolicited phone calls. The scheme has the backing of 35 local police forces and organisations such as Financial Fraud Action UK, Age UK and the credit reference agency Experian.

Call for action

Much of the publicity around the campaign, by necessity, has been around convincing consumers of the need to take action themselves. In the social media age however, the agencies are seeking to connect with people in an environment where capturing the attention of an average consumer for enough time is harder than ever, but the leading players sound determined.

City of London Police commander Steve Head, the national police coordinator for economic crime, said: “Identity crime is a serious issue for the country, with some reports suggesting that as many as one in four adults may have been a victim at some time, with the potential costs to our economy running into billions of pounds.”

Cifas chief executive Simon Dukes said: “We know that people lead increasingly demanding and busy lives, with many people reporting password fatigue or struggling to find the time to update their software securely and regularly. We need to change the way we think about our identities and prioritise protecting them.”

The tactics

Phishing scams are still the most common method used to obtain a target individual’s credentials. These could be via online calls, suggesting an individual’s personal banking details have been compromised, and asking the customer to reset them over the phone.

Thomas Brown, senior vice president, financial services, at data solutions provider LexisNexis Risk Solutions, explained that malware is then used to monitor the individual’s genuine activity, and send keystrokes back to the fraudsters, enabling them to replay the bank customer’s online authentication journey.

He added: “Malware can arrive in many forms and fraudsters are using sophisticated techniques to spark a customer’s interest and entice them to download an attachment. For example, this could be a delivery note for a package, which the customer never ordered, but appears to be from a genuine parcel carrier...”
company, or even zip folders which are made to look like financial statements, but in reality contain malware disguised in the folder to bypass a customer’s standard virus and malware checkers.”

It’s a common thread in financial services that effective password management is still a weak area, in terms of the vigilance displayed by consumers themselves. As a result, Brown explained, personal information such as payment details can then be stolen from a retailer’s site to “commit serious attacks against the individual’s credit card or bank account.”

John Marsden, ID and fraud expert at the credit reference agency Equifax, said that ID takeover is often fuelled by underground markets for personal details. It is believed that around 20 million records of stolen data exist in these markets, relating to about five million individuals. Marsden added: “The details for sale vary from simple email passwords to full financial information. These details are used to take over accounts, often where the fraudster fully understands the facilities and defences involved in the application and account management processes.”

The perpetrators
It’s still the case that criminal gangs are behind most identity theft incidents but how the perpetrators are connected lower down the food chain is now very different. Marsden explained: “We still see a large amount of traditional organised crime, where the individuals involved are physically associated, but more often the dark web is being used to connect fraudsters offering specialist elements to an overall orchestrated fraud.”

In these scenarios, he explained, the crime is organised but not in the traditional sense; the individuals do not necessarily know each other.

Brown pointed out that individual fraudsters often play a specialist role in a much bigger, more enterprising scam. Once these individuals have added their specialism to the compromised identity, it’s passed on at a premium.

“The fact that these financial criminals are online, and only one link in a chain, means they are difficult to tie together for an investigation. The criminal enterprises are large, complex and remarkably well run. Many have call centres set up.”

The fightback
As you’d expect, banks have various approaches towards prevention. Brown believes that some banks have a clear agenda for the digital age, usually driven by the need for customer convenience and the appeal of reduced manual costs. He said many banks now employ device recognition as standard, along with device reputation checks, to isolate geographies and physical devices from the fraud check. Several banks have also established one-time password (OTP) checks to authenticate an individual when they transfer funds online. Brown has seen other firms experimenting with biometrics to various levels of success.

The use of voice recognition, device profiling and behavioural analytics looks set to continue.

Credit Risk Roles, Edinburgh
Portfolio | Provisions | Policy | Systems Data

You’re the difference between foresight and hindsight
As an experienced Risk professional, you know the vital part you can play in any bank’s future. But some futures are more inspiring than others. We’re an ambitious business, with a growing customer base and a range of new products in development. Now, we need forward-thinking and inquisitive analysts to join our Credit Risk team and help us explore the possibilities ahead.

Join us and you’ll be part of a team at the forefront of the industry – whether you’re assessing long-term trends, turning raw data into invaluable insight or setting the policy that heads off potential issues. Whatever your role, you’ll find that your voice is heard, your ideas considered and your contribution recognised.

Discover your part in our future at our website.
www.yourethedifference.co.uk