KCS Group Europe

Identity Theft

4th September 2016

A recent news report by the BBC states that identity fraud has increased by 33% with the fraud prevention agency Cifas stating that the thefts are becoming easier to facilitate online. Internet forums have been created selling information to open bank accounts, obtain credit cards and commit fraud in other people's names. A person's identity can be purchased online for as little as £5.

Media coverage of identity theft appears to focus on the individual looking at stolen bank accounts and using the information to go on shopping sprees on someone else's dime. The reported crimes look at the more physical means of stealing identity such as stealing the victim's mail and even dustbin diving. With lots of personal services and amenities being increasingly hosted online it is getting easier for fraudsters to steal our personal information, as we increasingly provide our details for apps like food delivery and taxi services, which can (and are) breached to obtain customer data. It is pointless to advocate a Luddite approach of not using technology and modern amenities. People should however, remain vigilant and have a number of passwords for their accounts to avoid falling victim to scammers should a particular app or company be breached.

Very little has been written about the dangerous implications towards businesses that identity theft presents.

Businesses can present appealing targets for fraudsters, particularly smaller businesses which cannot afford the state of the art protection afforded by a conglomerate. Businesses are appealing targets because of the customer data that companies can possess and which can be obtained with comparatively little effort.

However, there are numerous other methods of business identity theft employed by fraudsters which does not require extensive cyber capabilities. One such scheme is called the 'man in the middle'. The scheme is implemented by the fraudster masquerading as a member of the finance team responsible for outgoing payments. Using a falsified email which has been created to look as convincing as possible, the fraudster then redirects payments to a different bank account under the guise of an update in banking details. It is a simple method and can easily be countered with a phone call, however companies have lost thousands to this scheme due to complacency.

Identity fraud does not even have to be conducted for monetary gain. The Trump White House was subjected to a scam artist who, masquerading as a senior White House staffer, sent confrontational emails to the then-director of communications Antony Scaramucci. Fortunately – this time at least - no lasting damage was done other than persuading a senior security advisor to divulge his private email. It is disturbing to see that even those in one of the most secure places in the planet can fall for such simple methods. The simplicity of identity fraud is one of

Heading

the reasons why they are successful - relying on human complacency and ignorance rather than coding skills.

Companies must develop a ‘siege mentality’ when it comes to communication as the theft relies on human error to facilitate the scam. Companies should encourage caution from their employees as many thefts are run from email accounts that are made to look like a genuine account but are revealed by a misplaced letter or similar. There is no permanent solution for this particular problem as only an educated and informed workforce that is aware of the dangers can prevent a theft.