Holistic approach to combat ID theft

There are very few people that have never heard of identity fraud. With nuggets of personal information such as credit card details, a social security number or bank log in details, criminals can bleed accounts dry as well open up new lines of credit. When one identity's worth is exhausted, they simply move on to the next victim.

Anybody impacted by identity theft will testify that it is far from the 'victimless' crime which its perpetrators label it to be. Although a victim does not have to go through the ordeal of being robbed face to face, they still have the ordeal of coming to terms with somebody having stolen their personal information and pretended to be them in order to defraud credit card companies, banks and stores.

More recently identity thieves have extended their fraud into providing false identity for illegal workers and for fellow criminals who commit crimes under their assumed identity, leaving a bemused victim having to explain their innocence to investigating police officers.

Perhaps most worryingly, identity thieves have started to use stolen personas to claim medical treatment for which they are not covered, not only defrauding the system but also running the risk of a victim's medical history being compromised.

Whatever the intent of the criminals, identity theft is more than a nuisance. It can make people feel violated, leaving them with no money and needing to take personal days off work to reinstate their good name with their bank, credit agency and the police.

MORE SOPHISTICATED

For Michael Stanfield CEO and founder of Intersections Inc., the main problem with identity theft is that criminals are no longer just relying on 'dumpster diving' or stealing wallets to gather personal information. Today's sophisticated identity thieves are becoming adept at launching viruses which can sit on computer hard drives stealing information and gathering sensitive passwords. Alternatively they can produce sophisticated sites which look like a bank or a regular store but are actually 'phishing' sites designed to gather credit card and bank account information for criminal use.

Hence, to Stanfield, the only way to offer protection against identity theft is to take a holistic approach. "You can set up fraud alerts and credit card blocks so you won't be a victim, but a lot of identity theft doesn't come from credit card theft," he says.

"A lot of people are having their bank accounts drained by 'keylogging' software that sits on their computer and tells criminals what their passwords are. So, you can set up fraud alerts but they are not effective unless you secure the PC at home."

In addition to daily checks with the credit reference agencies, records of new mobile phone accounts and details of social security or credit details being sold online, Stanfield argues ID theft protection companies should also offer anti-virus, anti-phishing and anti-spam protection on the PC as well as the ability to block 'keylogging' software.

The sad fact is that no matter how careful a person is in terms of securing their computer and shredding their personal information before it goes into the garbage, they can still become a victim of identity theft, or at least credit fraud, through no fault of their own.

Hackers are becoming increasingly adept at finding ways into corporate systems and stealing credit card details which are then normally sold online to other criminals. Gordon Rapkin, CEO of corporate information security company, Protegrity, believes many businesses need to look at their own data in a new light.

"You just have to look at all the customer records you have and instead of seeing a line of data imagine it as anything between $5 and $100," he says.

"Then they need to think about how many of these they have and how many pass through their systems every day. There are thousands of these records that are worth between $5 to $100 on the criminal market flowing through their hands every day. They only then need think how much they pay the person handling that information to realize the temptations on staff and the need for them to secure systems so staff never see all the records and certainly can't record or copy it."

A few simple security procedures and policy rules regarding how they handle data could solve many leaks of customer information which can end up costing a brand its reputation as well as having to undergo the embarrassment, and expense, of continued annual audits of its systems by the FTC.