

From Times Online
November 21, 2007

Guide to the dangers of ID theft

Could a criminal really open your bank account and withdraw money with the details lost by HM Revenue & Customs?

Rhys Blakely

What if those records lost by HM Revenue & Customs (HMRC) are not tucked down the back of Alistair Darling's sofa but are in the hands of serious cybercriminals?

How much danger is the British public really in?

The data lost by HMRC includes the names, addresses, children's names, dates of birth, national insurance numbers, bank details (account numbers and branch addresses) for more than seven million families, about 25 million individuals.

By itself, that information is not enough to, say, access a bank account and withdraw money – it does not provide what cybercriminals call “the full deck”.

Customers with online accounts, for instance, also have passwords.

Moreover, it does not allow for the present con of choice, which exploits “customer not present” transactions, where fraudsters make a copy of a credit or debit card and then use it in a shop (usually overseas) that doesn't have a chip-and-pin system in place and does not ask for the three-digit security number on the back of most cards.

Similarly, walking into a high street bank and opening an account has been made much harder in recent years by anti-money-laundering laws.

HSBC, for example, requires new customers to present a full passport or national ID card in person at one of its branches – or a tax letter from HMRC.

To verify your address the bank would require a bank, building society or credit union statement or passbook or a utility bill.

But serious would-be fraudsters have access to these type of resources, tools that help to complete that “full deck”, according to Graham Cluley, of Sophos, the technology security group.

He said: "Identity thieves often work closely with credit card cloners and forgers of other ID material."

That makes the HMRC information extremely valuable.

Mr Cluley estimates that the average package of information for one person could fetch between £20 and £100 on the black market.

Prospective thieves will expect to receive discounts for buying in bulk – but if a cyberthief is confident of being able to use the information to access an account, or if the person holds a sensitive position – say a security-related job with a large company – prices could reach several hundred pounds.

It is thought that if the data were to fall into criminal hands they would be parcelled out and sold on via the black market brokers who also deal in information such as vast lists of e-mail addresses – with which the HMRC data could be cross-referenced.

That means that the HMRC data could be leaked on to the market over several years.

Meanwhile, more intensive criminals could attempt to have mail redirected to get hold of some of that crucial documentation needed to open a bank account.

If a victim's workplace is known (a Google search would often deliver this information), a fraudster may call an employer's HR department, assume the victim's identity and try to get hold of the address of the tax office that handles their accounts.

The criminal could then ask the taxman for the victim's mail to be redirected.

On that call they would be asked by HMRC for details such as the victim's mother's maiden name – information that was leaked in the latest breach.

They would then have all the elements needed to open a bank account or to apply for a credit card.

There is also the old-fashioned method of rooting around people's bins.

“Refuse is by far the most common source of documentations and information for fraudsters,” David Hill, a senior security for red24, a security specialist said.

There may not be the need for those kind of measures, however. One high street bank executive admitted that among the biggest fears is that criminals in possession of the lost HMRC data will launch a massive direct-mail scam.

“A con could involve fake letters being sent out appearing to come from a victim’s bank and quoting their account number,” he said.

The letter could ask customers to call a bogus call centre number or log on to a fake website. Customers could then be tricked out of their security codes.

Other experts believe that the greatest threat is posed by criminals who do not have access to the HMRC data, but who will prey on public sentiment in the wake of the massive amount of publicity the breach has provoked.

Jonathan Armstrong, a partner at Eversheds, the law firm, said: “Even if the data on the CDs does not get into the hands of fraudsters, it is likely that even now a large e-mail campaign is being planned to prey on the British public.”

Blanket bogus e-mails campaigns are expected to be launched that will invite bank customers to reconfirm security details for online accounts.

Nordia, a Scandinavian bank, lost about £800,000 this year when 250 victims fell for an e-mail scam.

Customers who clicked on e-mails had their computers infected by malicious software that logged keystrokes and picked up details of passwords.