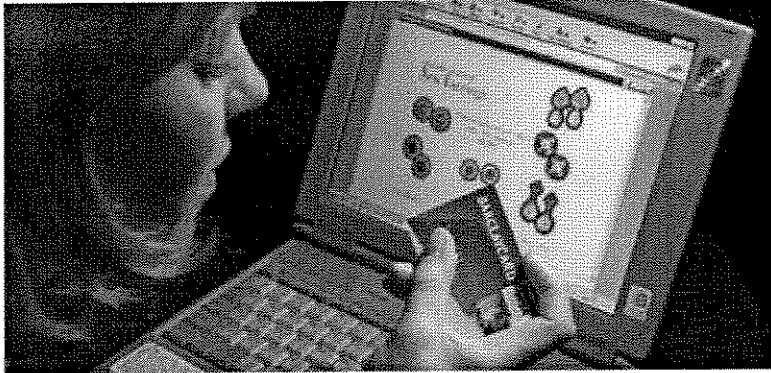


February 19, 2007

Striking back at identity thieves

Online identity theft is becoming increasingly sophisticated and prevalent, causing consumer confidence in internet transactions to plummet. Our writer explains how businesses, governments and individuals can combat this growing phenomenon



Tom Rowland

There is one worrying aspect of online identity theft that has recently been filling the papers in the United States but has so far received little exposure in the UK. However the evidence is that it is also a growing phenomenon this side of the Atlantic.

In November it was reported that Houston construction worker Eric Wagenhauser, had been a victim of identity theft, or rather his family had. His ex-wife had used their children's Social Security numbers to apply online for credit cards in their names; she subsequently pleaded guilty.

The story shone a light on a little-publicised fact: although most identity theft victims never learn who stole their identities, when the source is known, half of the victims say the thief was a family member, a friend, a neighbour, or an in-home employee. They then use the stolen identities to obtain credit and goods on-line.

This figure comes from surveys by the Federal Trade Commission and Javelin Strategy, a private research firm. The surveys estimate that 9-10 million Americans have their identities stolen each year.

Whilst in this country, a January survey by the Information Commissioner's Office found that almost a quarter of UK adults have had their identity stolen or know someone else who has fallen victim.

But although stealing identity information of someone you know might be the most successful way of committing this crime, in volume terms most attempts at ID fraud originate as phishing attacks, says Hitesh Patel, director of fraud services at consultants KPMG. This is where bogus emails are sent to an organisation's users requesting details of their credit cards and pin numbers.

"It is hard to know what the success rate is for those behind phishing attacks but there can be advantages to not knowing the

person under attack, it makes the criminal harder to find," he says.

But how the data is obtained might appear academic for organisations who increasingly feel under siege. For the first time in nine years, companies are listing privacy and data protection as a significant issue in an annual information security survey of 1,200 organisations by accountancy consultants Ernst & Young.

Its head of technology and security risk services, Richard Brown, said this is the result of growing consumer concern and awareness. Identity theft is no longer something they just hear about, but has probably happened to someone they know. He said this "intensifying pressure" from the consumer has forced companies to re-evaluate their data risk practices and procedures, particularly in the financial services sector. Waking up to the potential consequences for business, government agencies too are beginning to establish guidelines for consumer protection.

Recent studies from Harris Interactive show that fear of identity theft has stopped 53 per cent of internet users from giving personal information to web sites and 14 per cent from paying their bills online. In addition, Symantec's latest Internet Security Threat Report found that in the first half of 2006, nine of the top 10 phished brands were in the financial services sector.

"As the internet becomes more prone to the menace of threats designed to steal information for financial gain, consumer confidence in conducting business online has become eroded," says the Symantec report.

Sophisticated initiatives are now emerging. VeriSign has developed VeriSign Identity Protection (or VIP), a raft of authentication services designed to protect internet identities. Using a trusted shared network, VIP helps manage reputational risk for financial services, e-commerce companies and other operations that use consumers' personal data online.

"The VeriSign system essentially authenticates merchants so that consumers know they are dealing with a reputable organisation and not a con," says Patel.

The VeriSign Fraud Detection Service also protects against consumer impostors, detecting fraudulent logins and transactions by adapting to customer usage habits unique to that individual. It flags potentially fraudulent activities based on known types of fraud and behaviour not associated with the user.

Meanwhile Symantec has announced its own security solution – Norton Confidential Online Edition. This enables banks and other financial institutions to extend protection to their customers' computers from phishing, pharming (a type of attack in which hackers redirect a website's traffic to a bogus site in order to harvest sensitive data such as usernames, passwords and bank account details) and other password-stealing programmes.

Norton Confidential Online Edition authenticates the bank's web site at every login so customers know they're on a legitimate

site; it also alerts customers if they've arrived at a phishing site. The software protects customers when they enter passwords, make purchases or bank online, and will block key logging and screen-capture programs.

Symantec has also launched the TransactSafely website, helping consumers understand internet threats in simple terms and offering practical tips on measures users can take to protect themselves.

Consumers are encouraged to keep all personal information private, save a copy of their credit report and check bank statements regularly. It is also recommended that they take steps to ensure the safety of their computer and to shred all promotional offers and confidential information before disposing.

With hackers becoming ever more adept at evading online security measures – and, as the evidence from the United States suggests, increasingly close to home - the lessons are clear. Internet identity theft is a phenomenon that nobody – individuals, companies or governments – can afford to ignore if the online business environment is to thrive.

PRINT

EMAIL

POST TO
DELICIOUS

POST TO
NEWSVINE

ALSO IN IDENTITY MANAGEMENT

The future of identity management
Can you trust what you read on-line?
Retailers seek continuity in profiling of shoppers

YOU LAST READ

Brewer braced for new order after ban