THE SUNDAY TIMES

Features

YOUR ONLINE SECRETS FOR SALE; The security breach at Sony that put the personal details of 77m users at risk underlines how vulnerable we are to organised gangs of internet criminals.

Jon Ungoed-Thomas reports, Additional reporting: Geoff Berkeley; Jon Ungoed-Thomas; Geoff Berkeley

1639 words
1 May 2011
The Sunday Times
ST
1
22
English

On an online forum last week computer criminals were advertising their wares. At 1.42pm on Thursday a seller identifying himself as Duong from Vietnam was putting up for sale fresh "dumps" of information with dates of birth, addresses and credit card numbers stolen from British consumers.

Duong explained that he had "very affordable and high quality dumps" that could be delivered to a buyer within 15 minutes.

In the world of online theft such dumps have become a thriving trade. A suite of personal details on an individual can be bought for as little as £10. Samples can often be obtained free or can even be viewed on the forums, with the addresses, home telephone numbers and Mastercard details of unsuspecting British bank customers on view.

The prize is not just a stolen credit card but also an individual's online identity — including email addresses, passwords and security questions — which can unlock several accounts.

"This is an organised crime marketplace," said Professor Andrew Blyth, head of the information security research group at the University of Glamorgan. "Once they've got a username and password, criminals can go to sites like Amazon and eBay and see if they can get in."

This illegal trade had a huge fillip last week after it emerged that the personal details, passwords and possibly credit card details of 77m users had been stolen from Sony's PlayStation Network, the online game system. An estimated 3m users in Britain were affected.

The theft of the personal data — one of the biggest in history — is a public relations disaster for Sony. The company took 48 hours to shut down its network after the attack and four days to admit that its system had been breached. It was only last Tuesday when it revealed that a vast cache of customer data had been stolen.

Elita Ogbab, 21, of Edmonton, north London, a victim of the hackers, said: "A week last Wednesday I was playing Zombies and it signed me out. I thought it was the internet connection, so I just left it. I didn't find out until Saturday about the hackers."

Sony, which hires some of the world's leading computer experts, had been entrusted with the information of tens of millions of consumers but had let it spill out into the internet. It had been humiliated by the data thieves. Corporations worldwide will be taking note, anxious to avoid a similar fiasco. But when we rely on our emails and passwords for almost every aspect of our lives, the episode raises serious questions. How safe is our personal information and are we divulging it too readily? TWO months ago a small group of hackers were chatting online about the vulnerabilities of the PlayStation Network. The chatter was obscure but the message was clear. The network had significant security flaws.

One the hackers observed: "You know, watching this conversation makes me think about whether it was a good idea after all to buy a couple of games from [PlayStation Network] using a Visa card."

Whether or not Sony acted on these warnings, its enemies in the hacking community were gathering against it. They were angered that the company had taken legal action against George Hotz, an American hacker who had breached the internal security of the PlayStation 3. A group of hackers known as "Anonymous" warned Sony on April 14 to "prepare for the biggest attack you have witnessed".

Between April 17 and April 19 Sony's systems buckled as it came under attack. Anonymous, though, claims it is innocent. "For once we didn't do it," it said on its website.

British victims are understandably angry. Antony Bennison, 30, a photo editor from London, has been a member of the Sony PlayStation Network for two years. "I'm pretty disappointed in Sony and it's very unlikely I will sign up again in the future. It just hasn't taken care of my personal details so why should I trust it?" he said.

"I use different passwords for every account I have and I will recognise email scams trying to get more information from me. I am most worried about identity theft, which you might not find out about until much later."

Not everyone is as canny as Bennison. Many consumers use just one or two passwords that, once divulged, give access to multiple accounts. A survey last year found more than half of consumers used passwords that are variations of names found on their social networking sites.

Peter Warren, co-author of Cyber Alert and a founder of the Cyber Security Research Institute, said: "Cyber crime gangs are changing their tactics.

They are no longer aiming to just steal financial information: they are aiming to steal personal information."

As the internet has flourished, customers have become willing to provide increasing amounts of their personal data to online services. Such information is a valuable commodity to data thieves.

In Russia and eastern Europe gangs of hackers have been developing malicious software to target computers. Initially banks were the targets, along with the financial data systems. Now it is just as likely to be online shopping and social networking sites that are under attack.

Alan Paller, director of research at the SANS Institute, an American information security training centre, said: "The banks have got much better at protecting their information. Many of the social networking sites don't take security so seriously and they are a target."

One of the aims of the data thieves is to build an individual online identity, harvesting information from different sources. Using that information they can either access existing services or fraudulently apply for new services. CIFAS, Britain's fraud prevention service which collates data on financial crime, published a report last month revealing that identity theft is the fastest growing type of fraud in the country. Out of 217,385 cases reported to the CIFAS database, identity frauds accounted for 47%.

Richard Hurley, a CIFAS spokesman, said people should be far more careful about what they publish online. "If someone has got your name, address and date of birth, they can start to try to impersonate you," he said.

Some people provide so much information online they can even be tracked. One application, called Creepy, checks messages from Twitter and online pictures to create the history of an individual's movements, which can help to identify their address, workplace and the hours of the day they are not at home.

It exploits the fact that many people who regularly post pictures online are unaware that photographs taken by a smart phone, such as an iPhone, can include code containing the GPS co-ordinates of where the picture was taken. Two websites, pleaserobme.com and icanstalku.com, also highlight how people are revealing their locations online.

Yiannis Kakavas, a graduate student at Darmstadt University of Technology in Germany, wrote the Creepy application to highlight the amount of information posted online. "It's human nature for people to show people what they're doing and how well they're doing," he said, "but they're not thinking enough about their privacy."

Even information that individuals may consider confidential can be harvested by hackers. It emerged last week that smartphone users who transmit confidential information in wifi "hotspots" risk their names, passwords and messages being stolen.

Hackers working in such hotspots can create bogus wifi gateways to which many phones will automatically connect. All the information can then be downloaded to a laptop. Security experts say sensitive information should never be transmitted in a public wifi spot.

FOR Sony the damage is already done. The company is hoping to restore its PlayStation Network this week but the fallout is likely to last many months.

It is not yet clear whether the data on the credit cards were stolen or whether the financial data were safely encrypted. The personal email and gaming history of the customers will almost certainly be traded online.

"Just got called by my card company," one of the British victims of the hack tweeted on Wednesday. "Been charged 2 grand for some PayPal account in China. Nice one Sony."

There is also a key lesson to be learnt for the many consumers who use just one or two passwords on the internet: Duong in Vietnam and others like him are waiting to steal and sell your online identity.

Additional reporting: Geoff Berkeley

Biggest thefts of data

The biggest theft of online data is believed to have involved an attack on an American credit card processing company between October 2006 and May 2008.

More than 100m credit and debit card accounts were compromised in the attack on Heartland Payment Systems, a New Jersey company.

Millions of European card holders were affected by the attack.

In March 2007 the American retailer TJX, which owns the British outlet TK Maxx, said hackers had stolen information from 45.7m customers. The data were accessed on the company's systems in Watford, Hertfordshire, and Framingham, Massachusetts.

RBS WorldPay, the American payment processing arm of Royal Bank of Scotland, was successfully hacked into in November 2008. The hackers netted more than $9.5m (£5.7m) in 12 hours using card information stolen in the attack.

Cotton Traders, the British clothing firm, was hacked into in January 2008. It was reported that up to 38,000 customers could have had their details compromised. The business would not comment on the numbers, but insisted the data had been encrypted. " SONY HASN'T TAKEN CARE OF MY PERSONAL DETAILS. WHY TRUST IT?

Document ST00000020110501e751000fo