SPECIAL INVESTIGATION

By Claudia Joseph

HOW MY LIFE WAS STOLEN BY CYBER STALKERS

They took my cash, my job and the keys to my home... simply by hacking my emails. And someone, somewhere this Christmas is planning to do it to you

PAUL VLISSIDIS knows that I am on a pre-Christmas break in Delhi. He can track my every move and even view the pictures I am taking. Thousands of miles away, back in London, Mr Vlissidis is wondering whether to sell my car or pop into my house and have a look around. In the meantime, he sends an email from my address to my boss informing him that I am resigning from my job.

I don't know Mr Vlissidis, but he knows just about all there is to know about me, from the financial to the personal. He has access to everything that I have stored on my computer. Every element of my life has been exposed.

Luckily, Mr Vlissidis is not a hacker. He is the group technical director of the NCC Group, which has been cleared by GCHQ to discover loopholes in security in Government departments, police forces and many FTSE100 companies.

This is one of the busiest times of the year for internet shopping, and many of us expect to end the season with even more electronic gadgets than before. So I put Mr Vlissidis to the test, to see how vulnerable we really are – and the results have left me shocked.

Not only could he stalk me, but he could steal my identity, leaving me with a mountain of paperwork to try to reclaim my life. And all because I back up my emails online.

'A few years ago, you would back up your phone on your laptop and that was the only place it existed,' says Mr Vlissidis, 'but now everybody backs up wirelessly through a "cloud", which makes them much more susceptible. We conduct an enormous amount of business through email and it is available to anybody who hacks into your account. One phishing attack is all it takes. It's like dominos: if one falls, they all fall.

> 'I could send emails in your name and buy gifts with your PayPal log-in'

'I could send emails in your name and log into your mobile phone account and send texts as you. I could buy Christmas presents with your PayPal account, take out credit in your name, even empty your bank account. Identity theft is a real possibility here. Or if you have any enemies, they could remotely erase your phone or laptop.

'It's also a stalkers' paradise: I found your flight tickets and itinerary in your emails, traced you with "Find My iPhone" and then used your Facebook account to work out who you were staying with in India. I then looked at her Facebook page and found out her husband worked for the American Embassy.'

At present, cyber crime is estimated to be worth up to £27billion a year and it has a huge impact on British businesses.

'The blurring between our corporate lives and our home lives is becoming much tougher for companies,' says Paul. 'People often use the same password for work, which is slightly scary for the companies concerned.'

So how do the fraudsters target you? Their first port of call is information we readily put on the internet – on sites such as Facebook, Twitter and LinkedIn – as well as public information such as the phone directory and electoral roll.

I passed with flying colours, although I do have a website which has my mobile telephone number on it. 'We Googled you, looked at your articles, found you on LinkedIn, Facebook and Twitter,' says Mr Vlissidis. 'But we found very little about you in terms of your personal life. It's uncanny how many people use their dogs' names or their children's names, and a bit of Facebook research and LinkedIn research is all you need to come up with potential passwords.'

After finding out my phone number, Mr Vlissidis sent me a text. Even though I did not reply, he discovered that I owned an iPhone. 'The message came up in blue,' he explained, 'which meant it was an iMessage. We got very excited at that stage as it indicated that you probably had an iCloud account to back up everything.'

He then had three options: to target me at a public hotspot, change the password on my iCloud account or phish me.

His favoured option was an internet cafe or hotel – hackers set up a fake wi-fi network, which is identical to the real one, and then download all the information on your laptop. But I was in India so it was unfeasible.

'It's pathetically easy to set up a fake wi-fi network,' says Mr Vlissidis, 'and an easy way to target somebody. Criminals emulate the legitimate wireless network, like an evil twin. The best solution is to only log on when you know a network is secure.'

Then he tried to change my Apple password. But with little information about me, that too was destined for failure.

Finally he sent me a spoof email from Apple, saying someone had tried to log into my account using the wrong password.

As Apple only communicates by email – and the message was incredibly convincing – I fell for it.

'The beauty of a phishing attack is that, if you craft your email carefully enough, when someone clicks on the link they are none the wiser,' he says.

'You came to our website – which looked exactly like the Apple ID website – you entered your details, we hoovered those up, got your password and then logged you on to the real Apple site on your behalf – so that you would never have known that you had gone via us to Apple.

'Phishing emails get more and more convincing. The only way you could have known it was an attack was by looking at the headers – but it is unreasonable to expect the average user to be able to do that.

'It's like saying you have to understand how a car engine works in order to drive it. We as a security industry have failed.'

If phishing had failed, Mr Vlissidis had one last trick up his sleeve – downloading malware such as a

HOW TO GUARD AGAINST CYBER CRIME

DO...

- Choose a safe password combining upper and lower case letters, numbers and keyboard characters.
- Be vigilant in internet cafes – choose secure networks. Be alert for phishing emails, even those that look entirely official.
- Invest in reputable anti-virus software. Sign up to a password keeper system. Set up two-factor authentication on iCloud, especially for Twitter.

DON'T...

- Choose the same password for everything.
- Give away unnecessary personal information on social networking sites: one piece of sensitive data, such as a phone number or address, can open the door to hackers.
- Choose passwords that are guessable from your online history – eg the name of your pet, partner, children etc.
- Give anyone your password!