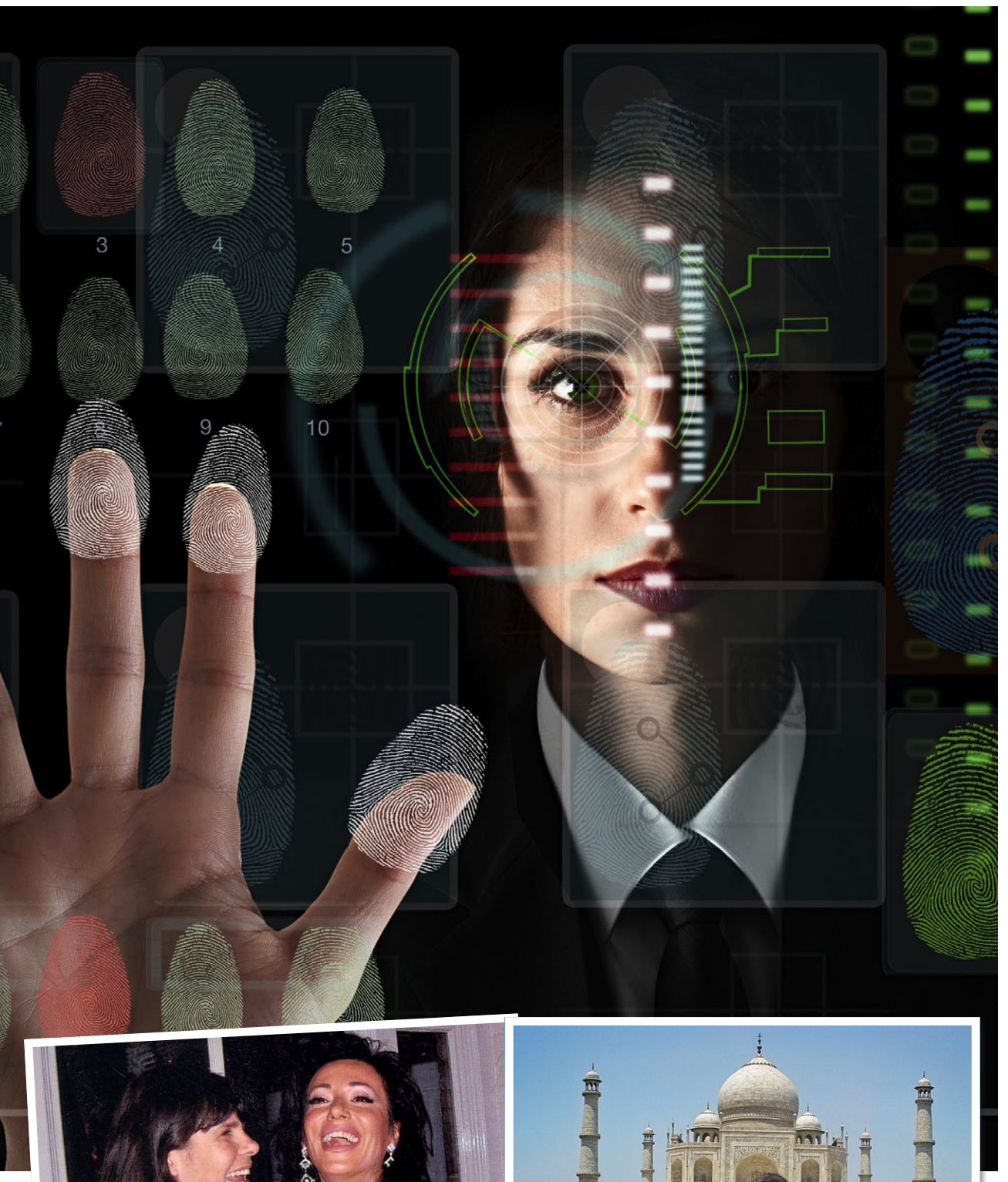


Well-off wives at highest risk of web scams

By **Martin Beckford**
HOME AFFAIRS EDITOR

MIDDLE-CLASS housewives are at the highest risk of falling victim to internet fraud, Ministers say.

Well-off women aged between 36 and 55 have been identified by Government researchers as a target for internet fraud and will be the focus of a £4million advice campaign in the new year.

Because they are 'new to the internet', they are said to be 'lacking knowledge and understanding' of how not to be duped by fake shopping sites or emails asking for bank details.

Officials say the vulnerability of these 'high net worth' women means they may lose as much as £4.2billion a year despite being fearful and cautious online.

As a result, they are the first group to be addressed – along with small businesses – by a Home Office drive to encourage safer internet behaviour.

Its theme is that there is a 'parallel world existing in cyberspace' where people shop, bank and socialise just as they do in the physical world, and its 'residents' should take the same precautions with money and personal details.

The Cyber Street campaign, developed by famed agency M&C Saatchi, will be a 'soap opera set in the internet', backed by billboards and radio and TV commercials. A dedicated website will host animations showing how careless behaviour can lead to fraud, and will provide security advice.

Fraud is estimated to cost the UK a staggering £73billion a year, with internet scams among the fastest-growing types of crime as people spend ever more time and money online.

Police are struggling to cope with demand from victims and can lack the expertise to track down the gangs behind internet scams, often based overseas.

The Metropolitan Police has resolved just three per cent of the 7,393 reports of online fraud received this year.

Security Minister James Brokenshire told The Mail on Sunday last night: 'The threat of cyber crime is real and growing.

'As part of our efforts to protect the UK we are launching a major new awareness-raising campaign in January to help people use the internet securely and confidently for business, exploration, convenience and recreation.

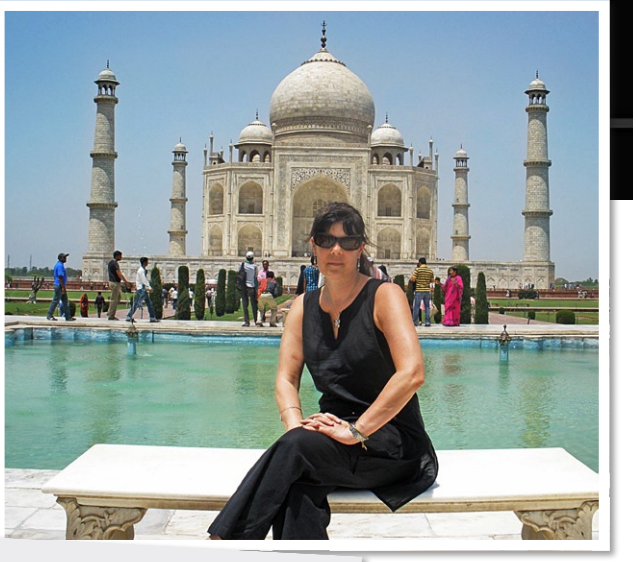
'We have already strengthened our enforcement arm with the newly created National Cyber Crime Unit. This will bring law enforcement experts into a single elite unit.

'This campaign will help close the net on sophisticated cyber criminals and protect the public from identity theft, scams and online fraud.'

As the MoS has reported, ministers recently passed control of the failing Action Fraud hotline from the now-defunct National Fraud Agency to the City of London police, which is experienced in tackling financial crime.

A report by the NFA already identified middle-aged, middle-class housewives as suffering the biggest losses to fraud.

It concluded: 'Though they aren't risk takers and are unlikely to act impulsively, their lack of knowledge around how fraud is perpetrated and what it "looks like" places them at risk.'



Dear Claudia Joseph,
Because too many invalid attempts have been made to log into your Apple ID account, your account access has been temporarily limited. During this period you will only be able to login from previously used devices and no new purchases can be made.
If you believe you have received this email in error, or that an unauthorized person has attempted to access your account, don't worry - your account is still secure and no one has been given access to it.
Temporary limitations can be removed by verifying your account below.

Verify Now >

Thanks,
Apple Customer Support

STOLEN IMAGES: Claudia, left with Nancy Dell'Olio, and in India. Top: ID scanning and, left, the scam email

Trojan horse, or virus – to my laptop, although I might have been alerted if I had some anti-virus software.

'If we hadn't phished you, we wouldn't have got your password very easily at all,' he says.

'We would have had to download malware on to your computer, which we could have done by guessing your browser and software. But we weren't sure if you ran anti-virus software and it wouldn't have worked if you connected from your phone rather than your laptop.

'This is the thing about hacking. You actually need quite specific information about the person you are targeting because the malware is very specific. We decided we didn't want to go that route in case it alerted you and freaked you out. So we decided to go for a straightforward phishing attack.'

It was breaking into my iCloud account that gave Mr Vlissidis the key to my online life. 'That really was the breakthrough moment,' he reveals. 'Once we could log on to your iCloud account, we could see all of your emails, your diary and contacts book. In fact it was slightly daunting because there was so much information in there.'

However it is not only people with an iPhone and MacBook that need to worry about cyberfraud: Android and PC users are equally vulnerable to hackers if they have an online account. They too could fall prey to spoof emails.

Even if you have different passwords for each account, you are not safe. Mr Vlissidis trawled my accounts to find emails containing the word 'password' or 'welcome' and then used a password-cracking tool to fill in the gaps (I had 66 emails containing the word 'password' and 85 emails saying: 'Welcome.').

'With many sites you get an email, which says, "Welcome Claudia" containing your username and password,' he explained.

'We then went through your emails collecting your passwords. Finally we used password-cracking software to gather up the missing ones. We gave it a dictionary of the words and numbers we knew about you and it came up with a list of variations. From our point of view it wasn't a big challenge because many of your passwords were similar.'

Once Mr Vlissidis had cracked my passwords, the sky was the limit.

He could send emails on my behalf, get a copy of my energy bill to use as ID and log on to my Oyster card to find out my regular bus and Tube timetable in London.

'I suppose if somebody was stalking you, they could build up a pattern of your movements,' he said.

Although he didn't have access to my mobile telephone, he could still send messages from me by logging into my O2 account.

He managed to track me down using the app Find My iPhone, downloaded all my photographs from Photo Stream (including one of me with Nancy Dell'Olio) and then tracked my movements through my pictures. However, being stalked was the least of my worries.

By hacking into my emails, Mr Vlissidis could have eventually bankrupted me: he could have bought things on eBay and had them delivered wherever he wanted; taken money out of my PayPal account (he transferred a token £10 to his account) and even opened a bank account in my name at his own address.

'I did try to buy something from Amazon and M&S and have them delivered to me, but I needed your credit card details which, interestingly, was the one thing I didn't have. I found your card number but could not use it because I did not have the CCV numbers from the back of the card.

'You are quite security savvy, compared to many I have come across over the years. A lot of people aren't that disciplined.

'They quite happily store their CCV details with the card details because it's easier to do so.'

Mr Vlissidis sent my neighbour a text purportedly from me asking her to leave my spare key out. She fell for it.

And had he pressed ahead and broken into my house he could have then sold my possessions – and even my home.

'It would have been a tall order,' he admits, 'but not impossible.'

In the meantime, I have bought some early Christmas presents for myself – some anti-virus software for my laptop and membership of Last Pass, a password keeper, which will hopefully protect my passwords and make my web browsing more secure.

> 'My house could have been broken into and my goods sold'

I have changed the password on my iCloud account and set up two-factor authentication, which means that I have to key in a four-digit code texted to my mobile as well as my password.

And I have invoiced Mr Vlissidis for the £10 he owes me.

Oh, and I have also withdrawn my resignation from work.