

■ Software decision makers, complete our survey on digital publishing

- Home
- Hardware
- Software
- Networks
- Management
- Comment
- Research



# Guilty or not guilty?

WELCOME **Joanna Boundy**

LOG OUT | MANAGE MY ACCOUNT

**search**



**Devil's Advocate:**  
Should banks use biometrics?



**Offshoring:**  
"Not proven" for call centres, says HBOS



**Zip it:**  
Equant secures network of fastener giant

[silicon.com](#) > [software](#) > [security strategy](#)

Tuesday 3rd May 2005

### other security strategy stories

- Hackers to test MPs' IT systems
- Biggest security headache just won't go away...
- CIOs asking if it's time to outsource security
- Security bosses seek to dissolve encryption bans

### Phishers still reeling in thousands of Brits

May 03 2005

by **Will Sturgeon**

**And what are the banks doing about it? Guess...**

- **E-mail to a friend**
- **Printer friendly**
- **Reader Comments**  
 Post your comment here

### security strategy comment

- Devil's Advocate: Biometrics offer false hope
- Leader: InfoSec's appeal
- Criminal IT: The crime you can still get away with
- Leader: Sex education – the IM angle

[more](#)

### security strategy white papers

- Get Smart About File Transfer
- Today's Quality Assurance Practices: How can we continue to improve?
- Rules of the Road for CRM
- 8 Golden Rules for CRM Success - Transform your Organization into a Customer-Centric Enterprise

[more](#)

### latest headlines

- Phishers still reeling in

Phishing attacks continue to rise and new research suggests more and more UK internet users are falling foul of the emails which often look to steal personal information relating to online banking and ecommerce.

Many victims also claim their banks aren't doing enough to protect them or compensate them.

According to AOL, five per cent of UK surfers claim to have fallen victim to any kind of online fraud - from phishing scams, fake domain registry renewals and 'Nigerian 419' scams to phoney online auction lots.

In total, one per cent claim to have fallen specifically for phishing scams - a figure which points towards hundreds of thousands of victims across the country.

Of those who have been victims of phishing, 53 per cent claimed not to have received compensation for their losses from their bank or credit card company.

Email filtering firm Postini claims the total number of phishing scams has decreased month-on-month but this may signify a move towards more sophisticated, less scatter gun attacks and may yet be the precursor to a rebound to new highs, according to Scott Petry, founder and senior vice president of Postini.

Petry told silicon.com: "I'm shocked at the number of people who have been victim to these kinds of scams on one level but then I realise how many gullible people there are out there. If people see something in front of them which looks genuine they tend to take for granted it is."

Petry believes the massive rise in phishing attacks was symptomatic of the spammers' attempts to ensure reasonable returns. "The reaction to more pervasive filters was simply increase the volume," he said.

But now he believes sophistication is also increasing - perhaps suggesting fewer emails are required for similar returns.

The drop witnessed by Postini, which claims to have scanned 14.9 billion emails last month, detecting more than nine million phishing scams - a 45 per cent drop month-on-month - may also be due to ISPs blacklisting servers, bot-nets being closed or individual machines being decommissioned in significant enough numbers to have an impact.

But as fresh machines become compromised and the spammers move on to pastures new it's likely the numbers will increase. "We'll continue to see peaks and troughs," said Petry.

Many in the industry believe banks still need to do more.

LloydsTSB, for example, recently announced it will start to contact customers again via email, adding to the confusion over whether banks will or won't contact customers in this way.

Although LloydsTSB's email claimed it will never ask customers to divulge personal data, and provided a freephone number for customers who wanted to check the validity of the email, such a lack of clarity across the industry helps create a culture of uncertainty ripe for harvesting by the phishers.

Petry believes banks simply can't help themselves.

"I believe email is too valuable a marketing tool for the banks to ignore."

But while they can't help themselves, they must help their customers said Petry.

"I think banks need to be more active in driving authentication, validation and certification," he said, referencing authentication services which will query domains and IP addresses.

"They may not want to bear the cost of doing so, or pass those costs onto customers but that's what's happening with the cost of compensation anyway. This way they will at least benefit from the goodwill factor," he added.

- **Biggest security headache just won't go away...**
- **Phishers turn their aim on corporate networks**
- **Reuters shuts down IM system after Kelvir attack**
- **Banks agree to increase web security**

- **E-mail to a friend**
- **Printer friendly**
- **Reader Comments**



Post your comment here

#### Reader Comments



Post your  
comment here

[top searches](#) | [site map](#) | [help](#) | [contact us](#) | [how to advertise](#) | [get silicon news on your site](#) |

[XML](#)



[ABOUT SILICON.COM](#)

[YOUR PRIVACY](#)

[ABOUT CNET NETWORKS](#)

[ZDNET UK](#)

[BUILDER UK](#)

