

# PAB executive paper

## *Phishing*

### 1. Update on activities

In January 2007 the PAB agreed that the executive should engage with relevant stakeholders in order to understand the scale and dimensions of phishing in the UK. Throughout January and February, Emily Taylor held meetings with industry representatives including APACS (the UK Payments Association, representing 31 UK clearing banks), HSBC, ebay, and Vizuri (consultants representing the Royal Bank of Scotland). Their key points as well as their expectations of Nominet are summarised in the following progress report.

#### Phishing meetings

Main themes to emerge

- Phishing is damaging the reputations of banks (£23m in losses last year)
- Phishers are building portfolios of neutral-sounding domain names, making it desirable to cut the problem at the registry level
- Most phishing takes place abroad or out of hours, registry help needed
- Banks require quicker “take down” action on fraudulent websites
- Organised crime has control - view it as “risk-free” - tipping point could be reached soon – banks could call for tighter security
- Integrity of data is very important

#### Telephone call: Alistair McGowan of eBay

EBay has developed a free, downloadable toolbar which alerts users to dodgy sites using a traffic light system.

Very little take up amongst customer base, despite it being free, and numerous links from the eBay website.

Ebay’s instances of phishing attacks have declined, however. Similar toolbar now included in Internet Explorer 7.

#### Meeting: Richard Martin, Amit Parmar, APACS (The UK payments association, 31 members, all UK clearing banks)

Phishing cost £4m in 2003/4, £12m in 2004/5 and £23.2m 2005/6 (half of all compromises to online banking). Phishing is moving into the domain name space (rather than extra folders on hacked genuine sites, which was the previous trend).

Banks need to close down domains in minutes. They use WHOIS facility, phone the registrar and apply their “Acceptable Use” policies. Domain registrations often paid for with a stolen

credit card. Registries/registrars could require identification and “**much tighter security**”.

APACS recommend Nominet re-write policy so it can react faster to banks’ needs.

APACS interested in making a presentation to PAB at 14 March meeting.

**Vizuri (independent consultancy)**  
**Matthew Pemble (ex RBS), Steve Collins (RBS)**

Registries need to encourage or impose sensible regulation on registrars.  
Registry must maintain up-to-date and accurate WHOIS data.

Nominet could require registrars to have an Acceptable Use Policy and could require them to offer 24hrs support. If not, registries should be able to take down sites involved in fraud in their absence.

Most useful would be to have “temporary suspension” of sites if the requesting organisation could be liable. **“Registry (and registrars) could be culpable of aiding a fraud if they don’t.”**

**Brendan Pickering, and Pete Bonner, HSBC**

85 % of attacks are genuine sites, with hacked or false pages.

HSBC has 120m customers, 20m on Internet banking (growing fast).  
Cites APACS’ figures for phishing in the UK – but there is not an even spread of losses across banks.

HSBC’s attitude is to look after its customers’ data, know their customers, educate and work in partnership with them, and pursuing a partnership approach.

Links between phishing and identity theft, which is a growth industry.

Expectations of the registry? Are “ashamed” that it takes longer to shut down phishing sites in the UK than in Brazil or China. Cert.br handles things in a very coordinated manner, the US is very good.

Larger ISPs are now 24/7 in the US, in the UK this is not the case.

There is scope for a central reporting role, to contact ISPs and get sites taken down. Many international models are doing this through automated email processes.  
It is the larger, not smaller ISPs that are the problem. The smaller ones are usually “brilliant”, but there are some large UK ISPs for whom they can’t establish contact.

Banks are good at sharing security information with each other and with law enforcement. ISPs could do something similar – sharing information eg about fraudulent credit cards. Many don’t know that they can get free online checking of “hot plastic”.