

Developing a Policy on Phishing and Pharming

Next steps

Introduction

At the November PAB meeting, we introduced the issue of phishing, and asked for your initial feedback.

The feedback we received was not hostile to the idea of a phishing policy, but urged realism (ie a recognition that any .uk phishing policy would be unlikely to “solve” phishing). There was support for coordination with financial services organisations. There was also some warmth towards the idea of Nominet as a point of information, and for us to cooperate with the relevant authorities.

This paper seeks to move the debate on, and presents a number of proposals for possible phishing policies.

2. Comments from Policy Advisory Board

The ‘Developing a Policy on Phishing and Pharming’ paper was discussed at the November PAB meeting. Whilst PAB members did not want to rule out Nominet having such a policy it was felt that it should be minimally invasive in a similar way to the current Child Abuse Image Policy. The comments can be summarised as:

- We are lacking an analysis of the impact that any policy would have on the operation of the registry
- Many banks view phishing as a very small problem compared with credit card fraud
- Recognised that phishing is moving up the Parliamentary group’s agenda
- Potentially Nominet could do something at the point of registration
- Concern over the registry making judgements over what a domain name might potentially be used for
- It was doubtful that restricting registrations would solve the problem – any policy needs to be effective
- Nominet should coordinate with APACS, ISPA and the Internet Crime Forum

PAB members felt that our role should be as a point of information and to educate users rather than attempting to introduce invasive measures to attempt to solve the problem. Many felt it would not be realistic to think that the registry can solve the problem.

3. Comments on nom-steer re .bank.uk

A related debate has been taking place on nom-steer as to whether the introduction of a Second Level Domain for financial institutions (eg .bank.uk) could potentially be an answer to phishing in the .uk space. A number of issues have been highlighted:

- Many phishing attacks are not domain name related – the domain name is masked

- It is easy to spoof any domain (including .bank.uk) – some warned against introducing a domain which promises more security and trust than it can deliver.
- Some feel it should be the responsibility of the registry to ensure sites connected to phishing are shut down.
- Not only banks are affected by phishing – what would be the provisions for Building Societies (or online traders such as eBay) for example.

4. Recommended Next steps

The PAB is requested to agree that the executive should take the following steps:

In order to inform the debate, we will engage with relevant stakeholders to understand (1) the scale and dimensions of the problem, and (2) their expectations of Nominet as .uk domain name registry in relation to phishing. This work has already started.

Relevant stakeholders include:

Financial institutions
Online traders, such as eBay
Consumer representatives
Parliamentarians.

We will give a progress report at the March PAB meeting, and bring proposals to the May PAB meeting.