

# Phishing

## 1. Introduction

The PAB discussed phishing at its November 2006 meeting and during 2007 had meetings with experts from APACS (the UK payments association) and the Federation of Small Businesses. In July 2007 it passed the following resolution:

Because Phishing is a criminal activity which can adversely affect Internet users' trust and confidence in the online environment, and because it is highly unlikely to be solved by a single intervention, the PAB encourages Nominet to participate in self- or co-regulatory responses through a series of co-operative activities with other agents to include education of users and improved security measures. The PAB advises Nominet not to duplicate existing efforts by other agencies.

In the light of a serious wave of phishing attacks in May, one PAB member asked for this issue to be put back on the agenda. This request has received support from other members: it is appropriate to consider what specific action Nominet and Nominet members could take.

## 2. Work in Hand

The prime responsibility for action to respond to a known phishing site is with the ISP and/or registrar. Companies have an obligation to respond rapidly to authoritative requests and should have procedures in place to enable them to do this. Nominet could offer to be a repository of best practice to help smaller members identify how to respond to attacks and get access to supporting information.

There has been some confusion about how the three-way contract affects Registrars rights to take down sites being used for phishing or malware distribution. We have issued a clarification: our contract with the registrant should not be any barrier to a registrar suspending and cancelling service for a domain or web site they believe is being used for phishing.

On 23 May Nominet issued the following advice:

Recently we have seen a marked increase in the number of .uk domain names being used for phishing purposes. One phishing syndicate seems to be particularly prolific and may attempt to register domains through you. If you are targeted you may be contacted by various security companies, the police or trading standards about the activity that is occurring on these domains.

If you identify that a domain name has been registered through your tag for phishing purposes, you have a number of options:

1. Remove the nameservers and the web site (if you host it) and lock the customer out. This action is allowable within your contract with us.
2. Delete the domain name - you can do this through the Automaton or EPP up until the 7th of the month following registration.
3. Detag the domain name

Please note: Before taking action you should ensure that you are satisfied that the domain name is being used for phishing purposes or similar criminal activity.

You may also want to ensure that your terms and conditions give you the power to take action in these situations...

Additional information on this phishing activity is available on our technical blog.

The PAB will be looking at this issue further at their next meeting and will look at how we can develop best practice advice that registrars and Internet users can benefit from.

In the meantime we would advise all registrars to be especially vigilant and if you have a current policy that you would be prepared to share, or ideas on what best practice should entail please let us know...

We are exploring the introduction of a facility through the Automaton and EPP that could allow a registrar quickly to suspend a domain name while an allegation of phishing is investigated. (The registrar would also be able to remove the suspension if appropriate) This has been prompted by a request from a registrar for a facility to remove a

domain name from the zone file and trigger actions necessary to lock down the domain during the investigation period.

### **3. Initiatives Following from the Earlier PAB Advice**

The earlier policy advice from the PAB identified that phishing “is highly unlikely to be solved by a single intervention”. It also recommended Nominet participate in self and co-regulatory initiatives, which we have been doing proactively. Since then we have been working on a number of initiatives.

#### **3.1 Registry Internet Safety Group**

Nominet is a founding member of RISG (Registry Internet Safety Group), a new industry group including some TLD registries, security companies and ICANN accredited registrars. The intention is to find means by which domain name registrations made deliberately for the purpose of phishing sites or spreading malware, can be quickly detected and taken down. The areas of work are:

- Identification and dissemination of best practice;
- Legal liabilities with take down;
- How data sharing across different companies can speed up the process; and
- Standard protocols for the exchange of data.

#### **3.2 Clearing-house service**

A second initiative is a feasibility study into a clearing-house service. In this, Nominet might be able to act as a recipient of phishing site notifications from pre-vetted sources, and forward them to members. This would be linked to a monitoring system and possibly some new Automaton/EPP functionality to support registrars in dealing with these sites. We will provide further updates when more details are available.

#### **3.3 Best practice advice**

We have also started work on expanding the best practice advice on our website which should be launched later this year. It is our intention to expand the body of best practice and we will actively seek content for this section from registrars.

### **4. Proposal from the Executive**

As part of the process of working in self and co-regulatory initiatives, we believe that it would be useful to organise a joint workshop involving Nominet, the PAB, APACS, law enforcement and a security company to discuss how best to share information and ensure authoritative and rapid requests for assistance and action.

We have canvassed possible partners and the Home Office and/or SOCA, APACS and Symantec have expressed interest. APACS has offered to host an event.

### **5. Discussion**

The PAB is invited to:

Note the responsibility of registrars in timely and effective action;

Note current work in Nominet to share information and intelligence, in particular to support members’ own work with evidence and best practice;

Work with the Board, the executive and stakeholders in preparing a joint industry-law-enforcement workshop to help improve understanding of options and cooperation with other organisations.