

# Developing a Policy on Phishing and Pharming

## Contents

1.	Introduction .....	1
2.	Points to consider.....	1
3.	Conclusion.....	2
4.	Appendix: What are Phishing and Pharming? .....	2
4.1	Phishing .....	2
4.2	Pharming.....	2
4.3	419 frauds .....	3

## 1. Introduction

Earlier this year, a PAB member requested that Nominet develop a policy on phishing, and the issue was also raised during recent discussions on Internationalised Domain Names.

Phishing is a process of obtaining confidential information via emails that look like they are from a trusted source (usually a bank or related body such as PayPal). A background note on phishing and related frauds is set out in the Appendix.

The purpose of this paper is to present a framework for discussion as to whether Nominet should have a policy on phishing and related frauds.

The PAB is not being asked to develop a specific policy at this stage, but is asked to give the executive guidance on the basic issues.

The PAB's work programme has scheduled this topic to come to three meetings. Our objective is to get general guidance from the PAB at the first meeting, to get comments on a draft proposal at the second meeting, and to finalise a policy (if appropriate) at the third meeting.

## 2. Points to consider

- Do the PAB consider phishing to be a problem?
- Should a domain name registry concern itself with phishing? If so, why?
- What is currently being done about phishing elsewhere?
- Are end-users sufficiently protected?
- Are end-users sufficiently well educated about phishing?
- Would the introduction of Internationalised Domain Names require a phishing policy to be in place? If so, why?
- If a policy were introduced, we think key considerations could be:
  - Timeliness – most phishing frauds are over within hours
  - How are decisions made?
  - Who makes decisions?
  - What comeback is there in the case of errors/false accusations?

### **3. What's the scale of the problem, and how is it projected to grow?**

The DTI has kindly offered to circulate materials to PAB members in advance of the meeting.

### **4. Conclusion**

The PAB is asked to discuss and provide feedback on these, and related principles to guide the executive in preparing for the next stage of discussions.

### **5. Appendix: What are Phishing and Pharming?**

#### **5.1 Phishing**

Phishing is a process where a (spam) email is sent out which seeks to encourage the recipient to hand over sensitive information, usually banking information. This is usually done by asking the recipient to (a) confirm security details or (b) re-establish passwords by logging onto a website or (in some cases) emailing a separate address. There is a new variant, dubbed "spear phishing" where the emails sent are much more targeted, which decreases the ability of anti-phishers to spot and disable them.

The purpose of these scams is primarily to obtain financial information, but police tell us that the scammers are just as interested in any other hard information they can get, such as valid email addresses and any personal data (name, address etc) that can be used in identity fraud at a later date.

The websites used are usually copies of "real" websites (e.g. copies of ebay/paypal, banks etc) but in some cases are 'secret' sections of real sites (usually ones hacked into).

These emails are usually sent at a time of day (after 5.30 pm) or time of the week (Friday afternoon, Saturday) when response times are likely to be poor as many organisations can take no action during this time.

The emails typically have obfuscated, faked or misleading email addresses within them. The classic example of this is to use "www.barclays.co.uk@112.23.34" where the link is actually to the website at the IP address starting 112... not to Barclays bank. Other tricks, such as using codes in the format "%23" instead of characters help to hide addresses further. It is normal, therefore, for most users to not know the real "from" or "to" addresses – and if asked they would report the wrong domain name (usually that of the bank, ebay etc). One of the concerns raised with Internationalised Domain Names (IDN) was that the different character sets would aid phishing: at the moment it is already possible to register <NOMINET.CO.UK> (second character is a zero), but the increased number of possible characters increases the possibility of confusion. For example, it would potentially allow <internet.co.uk>, for example, and even reasonably keen-eyed users might not spot that this was different to <internet.co.uk>.

Banks always say that they will not send out emails asking for personal information, but they confuse matters by sending out newsletters (which may encourage to log into your account), and these newsletters are often not from the bank's domain name.

#### **5.2 Pharming**

Pharming uses "poisoning" attacks on the domain name system. Essentially, the nameservers that direct traffic on the internet have false data put into them (either through bad set up or malice). This misdirects users who have typed in genuine web addresses to false sites. Pharming is therefore similar to phishing, except that it does not require a lead email – instead it requires the compromise of the nameservers. They can be combined, with emails used to encourage people to visit compromised sites. This is even harder for the user to spot, as they would still go to the wrong site even if they typed the URL into the browser by hand (which is usually a defence against the hidden links).

Note that the word “pharming” is also used for the process of getting animals to produce pharmaceuticals, usually in milk.

### **5.3 419 frauds**

Phishing should be distinguished from 419 scams (aka “advanced fee” or “Nigerian email scams”). These are generally in the format of “Mr X has died, leaving behind US\$49,000,000 as proved by this [BBC/CNN/etc] news story. If you give me your bank details, you can have 30% of this”. While these scams also seek to obtain personal information by reference to a website they operate in a different way, because the website is genuine and used to add credibility to the story. Personal data is then stolen, and used in later identify fraud/theft.