Survey on Phishing Issues
June 2008

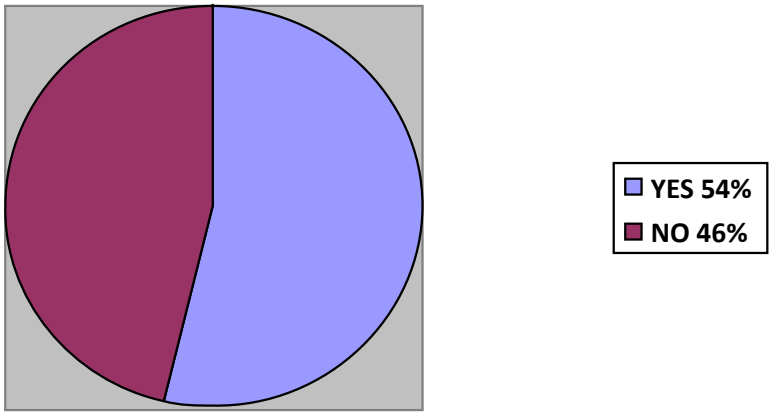
Background

The survey on Phishing issues was initiated by the ccNSO Council in order to find out how the topic affects the ccNSO community and whether the ccNSO is expected to do anything about it (*"…suggested that the ccNSO Secretariat launches a survey on the topic to find out what the community knows on the topic and expects from the ccNSO Secretariat."* Council Meeting minutes 31st October 2007)

The questions were drafted by the .mx and .jp registry, the Anti-Phishing Working Group and the ccNSO Secretariat. The survey was launched on the 25th February 2008 and sent to all available ccTLD email lists.

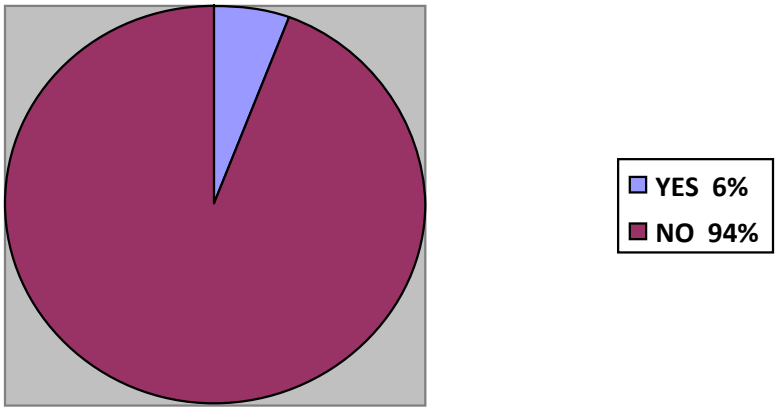
28 replies were received in total.

1) Are you aware of any phishing activity using domain names under your ccTLD?



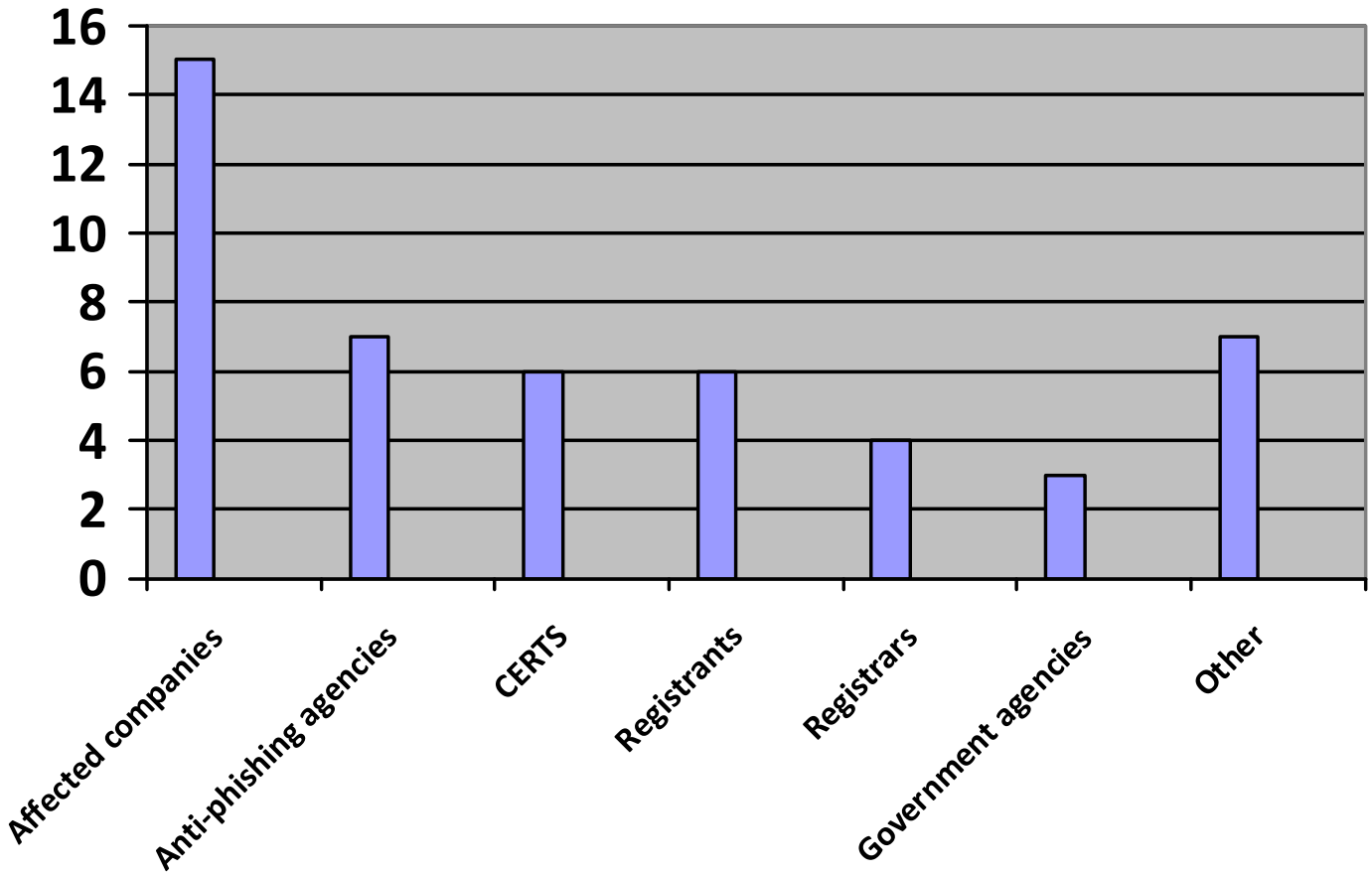
Just over half of the respondents were aware of ongoing phishing activities under their ccTLD.

1.1 If YES – Do you consider the phishing activity under your domain large-scale?



Only 6% - which equals one respondent – considered the phishing activity being “large scale”.

2) Who informs you about a phishing incident?

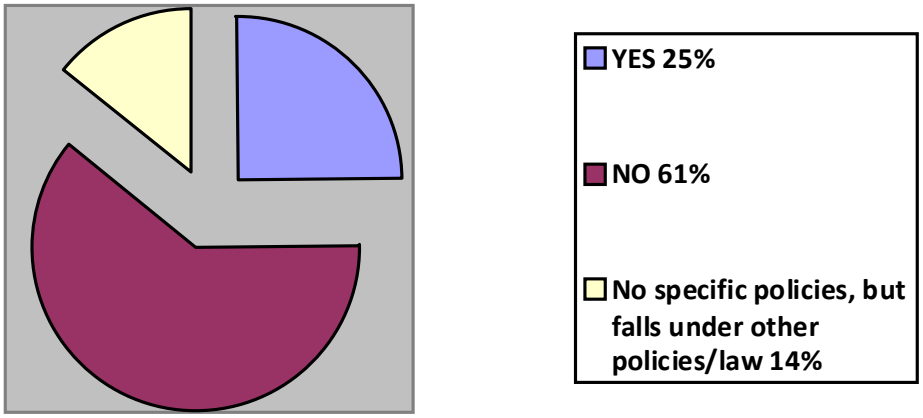


The respondents could indicate several options.

The registries most frequently receive information on phishing incidents from affected companies, almost twice as often as from Anti-phishing agencies.

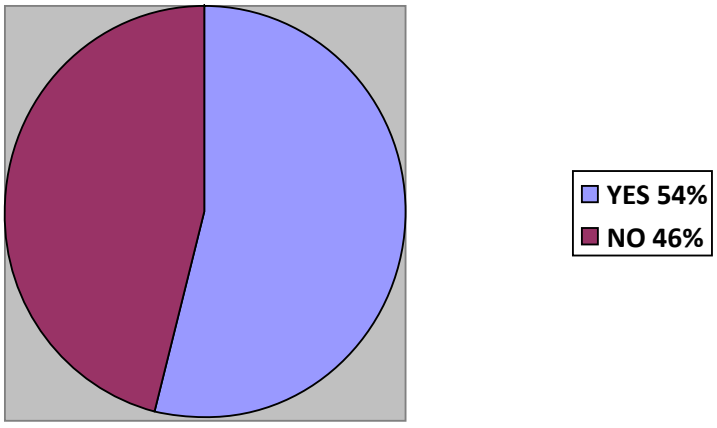
Under “Other”, further mentioned sources were collated, such as academic research, law companies or even spam reaching the registries.

3) Do you have policies in place to suspend domain names used for phishing purposes?



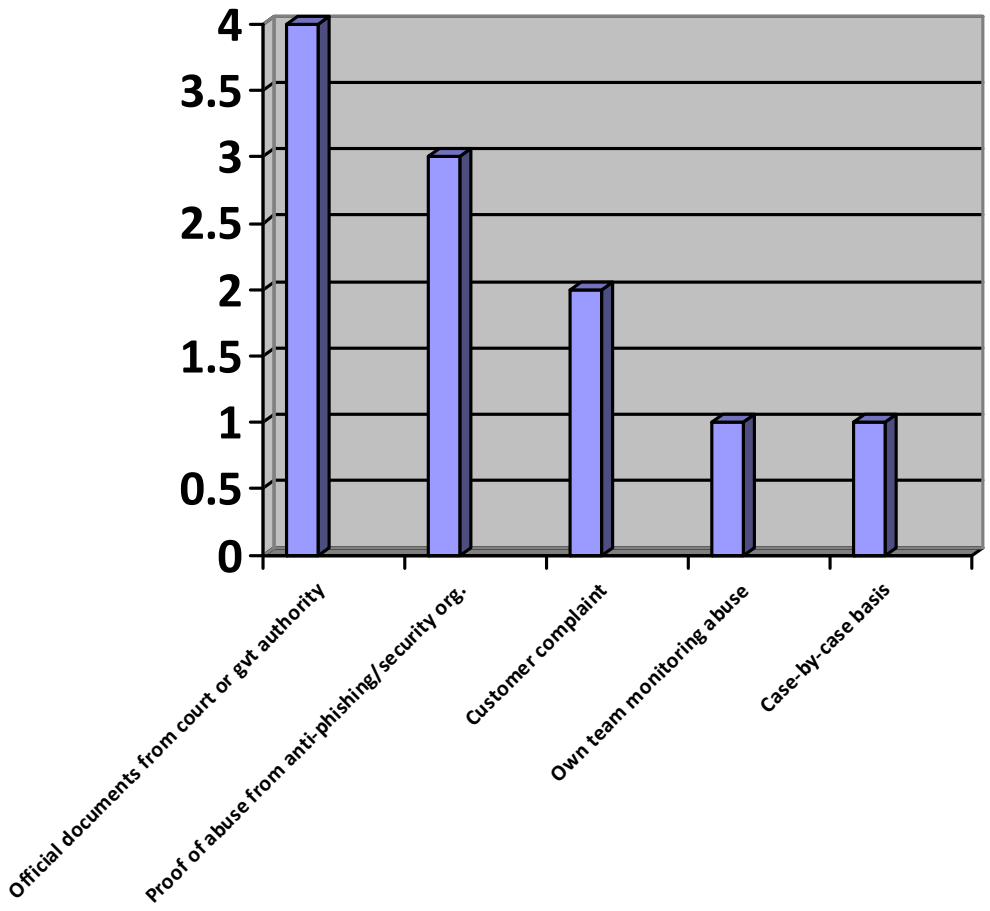
Only ¼ of the respondents have special policies in place for phishing purposes. 14% specified that although they don’t have special policies in place, phishing incidents are handled by other policies in place, or the country law.

3.1) If YES: Are they published?



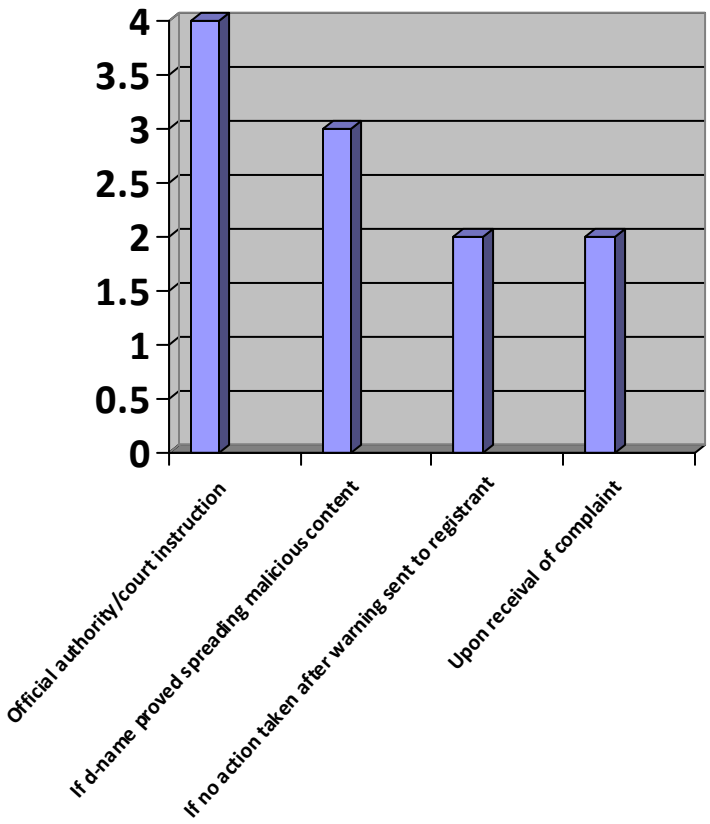
Over half of those who have phishing policies in place are publishing them.

3.2) If you have policies in place: What documentation/proof of abuse is required?



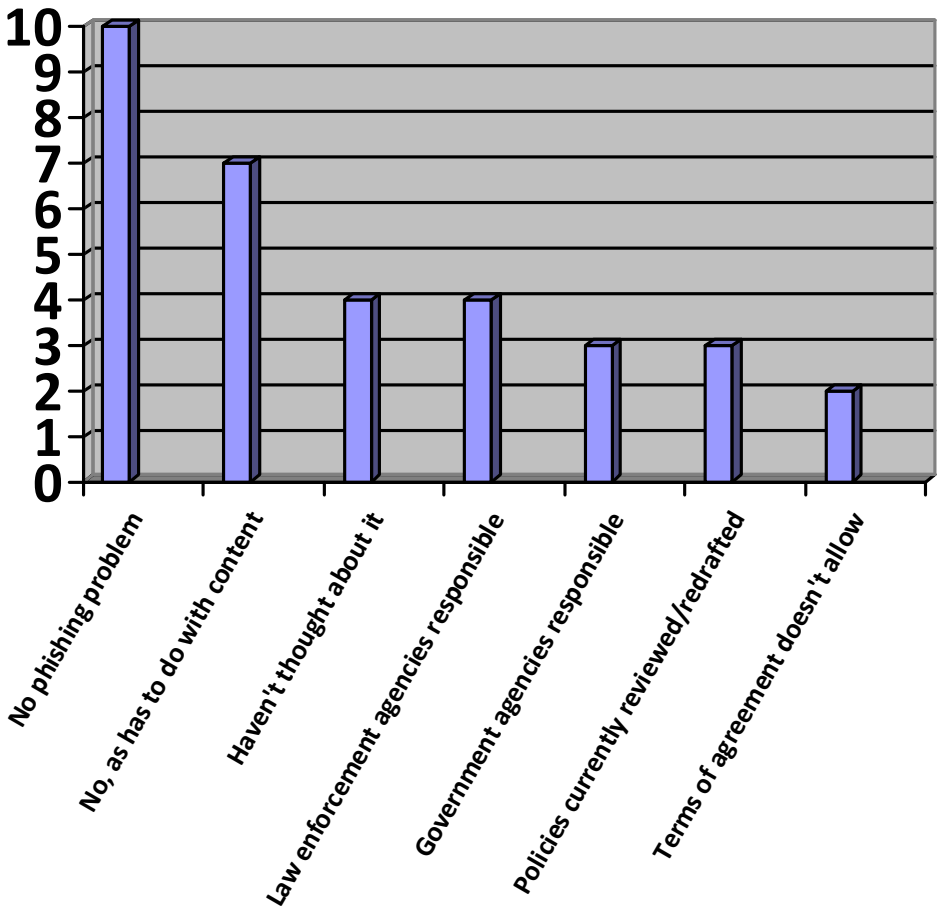
Most required document for registries with phishing policies in place is an official document from a court or government authority.

3.3) If you have policies in place: Under what circumstances will your registry suspend a domain name?



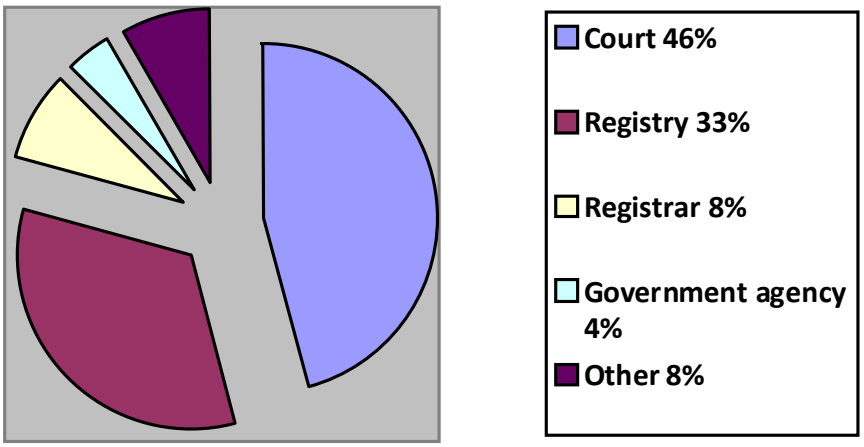
Most registries only suspend domain names upon receiving instructions from an official authority, or court.

3.4) If you don’t have policies in place: Why?



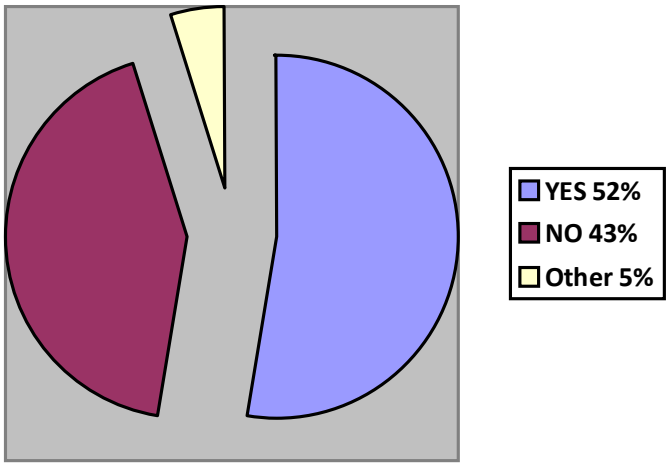
The respondents could choose multiple reasons. The most frequently mentioned reason was that the registry didn’t consider them having any phishing problems. However, many registries mentioned that it was not their role to regulate content on web sites; it is rather an issue for governments and law enforcement.

4) Who decides that a domain has been used for phishing?



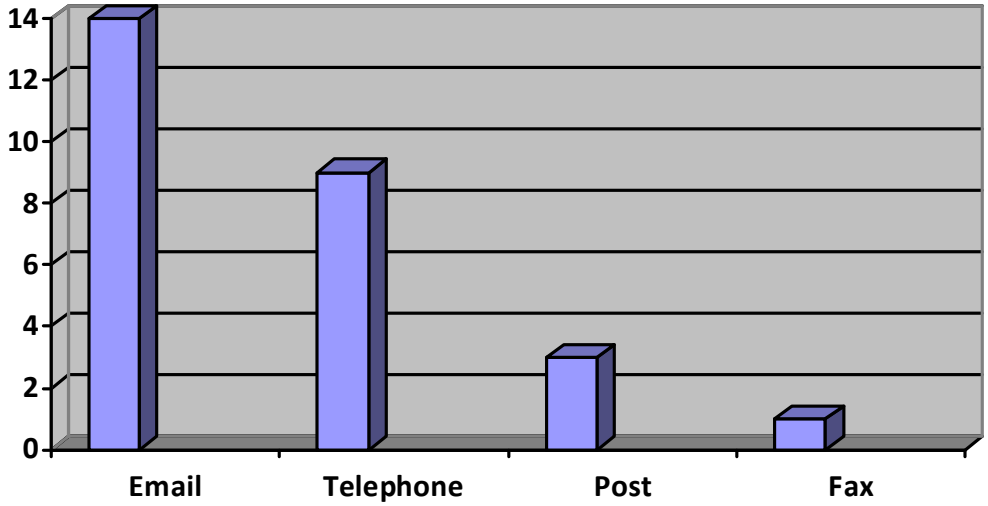
The most common case is that the decision on phishing activity is left to the courts to decide, however one third of respondents stated that the registry would take action if it had determined that a domain was used for phishing.

5) Do you notify the registrant of the pending suspension?



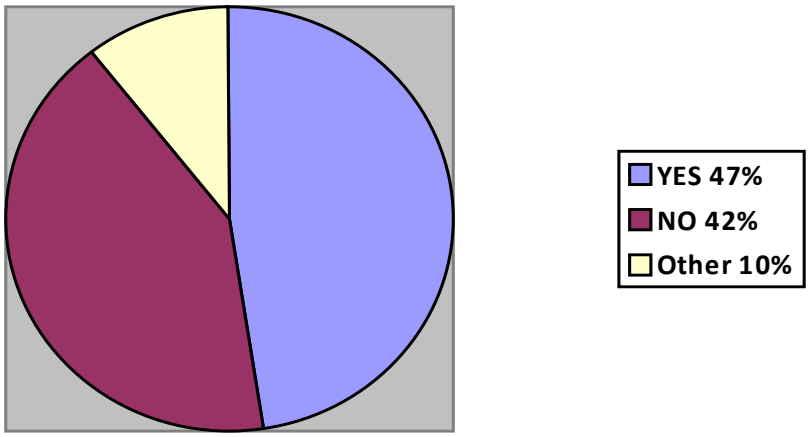
The majority of respondents will notify the registrant in the event of suspension due to phishing activity.

5.1) If YES: How do you notify the registrant?



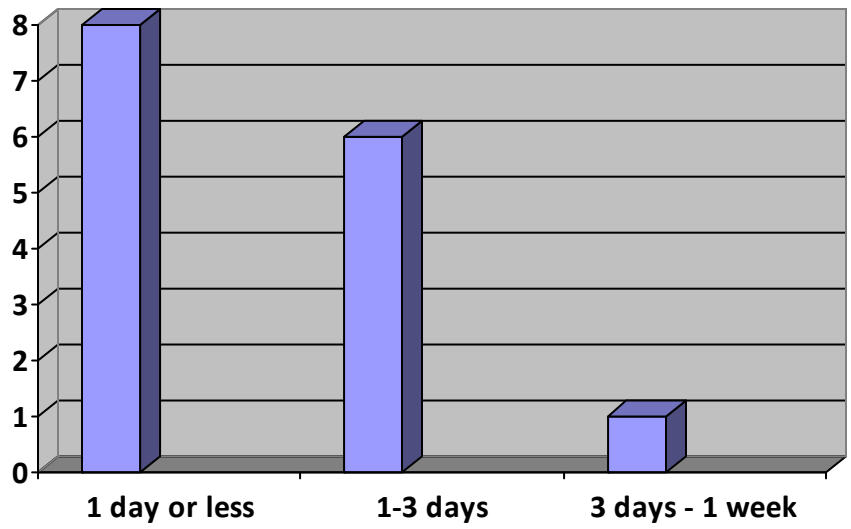
The most common form of notification is email. Some registries will notify using all possible means to notify the registrant.

5.2) Do you provide a grace period to resolve the issue?



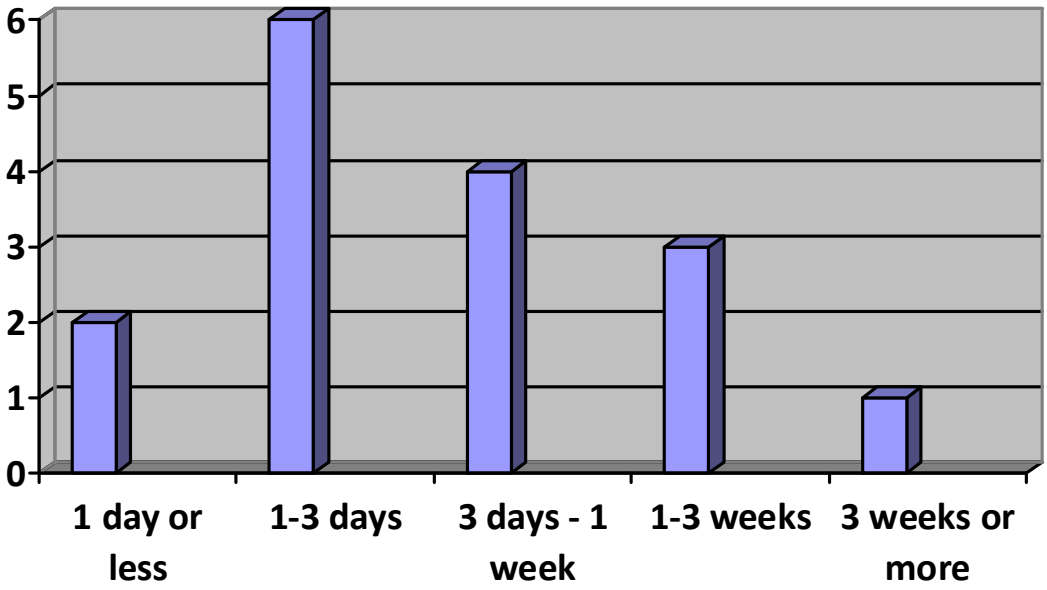
Almost half of respondents provide some form of grace period. Under “Other”, registries let a competent authority such as court decide whether a grace period should apply.

5.3) How much time does it take, on average, to notify the registrant?



Most notifications are done within a day or less.

6) How much time does it take from when a complainant starts the procedure, until final elimination/suspension of the domain name? (If foreseen by the procedure)

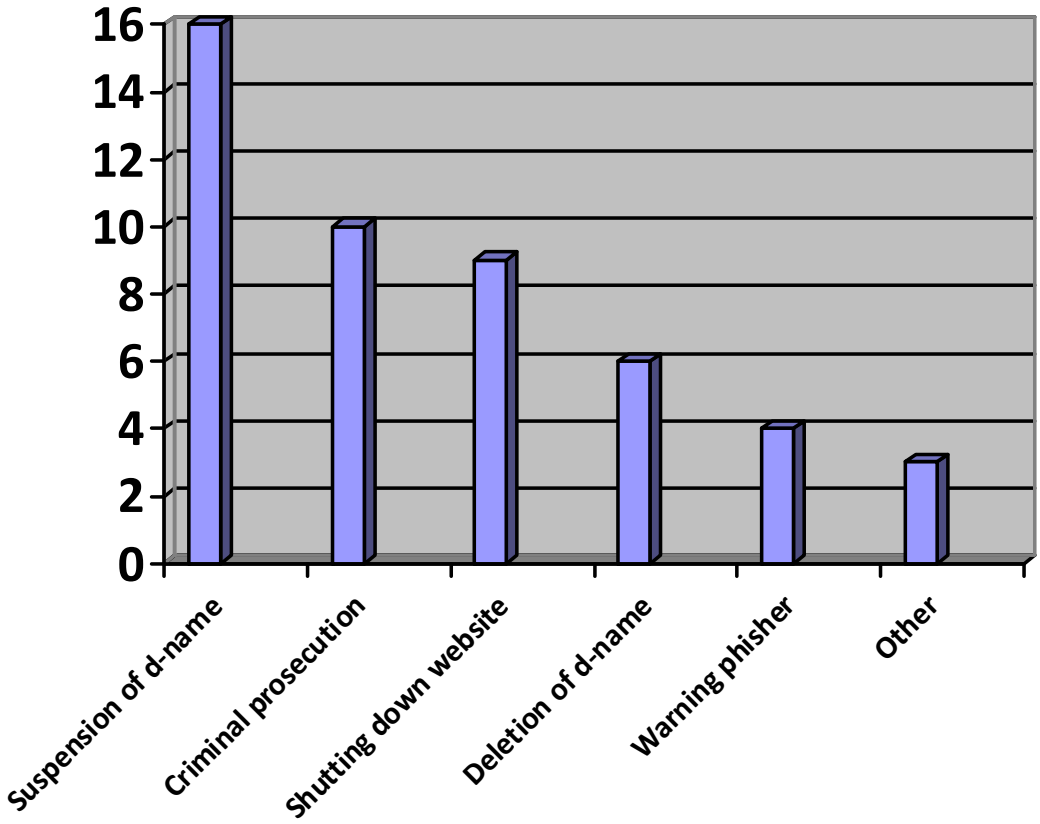


Most actions are completed within a week from the start of the procedure.

7) Please, describe the full procedure the complainant has to follow when dealing with a phishing domain complaint

Some registries did not have a specific phishing policy developed, however the normal procedure seems to revolve around a reactive complaint procedure whereby the registry acts upon a report that is lodged regarding phishing activity. This report is evaluated by staff (either technical or legal) in the registry, and if it is deemed to be a valid complaint, the domain is suspended. In some cases a warning is sent to the registrant or registrar to give them the opportunity to remove any malicious content before the suspension takes effect. Procedures vary at registries as to whether they accepted complaints from anyone, or only from specific competent authorities such as law enforcement.

8) What is the most efficient way to solve phishing incidents in your opinion?

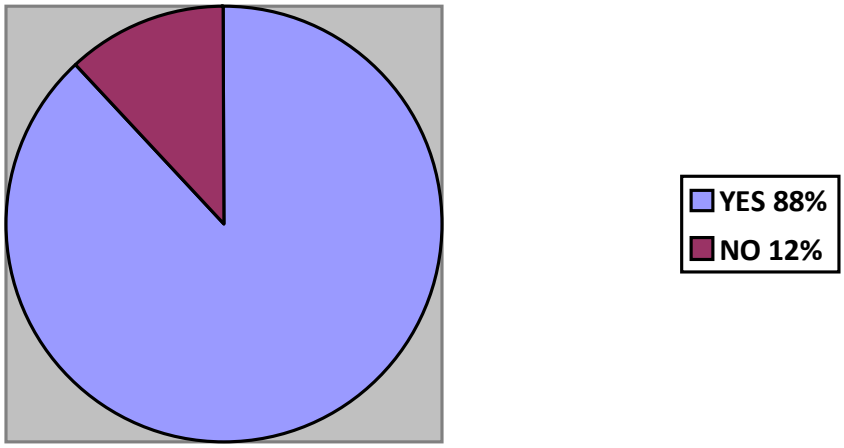


Respondents could provide multiple answers in the response to this question.

The most common view was that shutting down the website, either by suspending the domain or by directly shutting down the website, was the most efficient method. Criminal prosecution was also a common view.

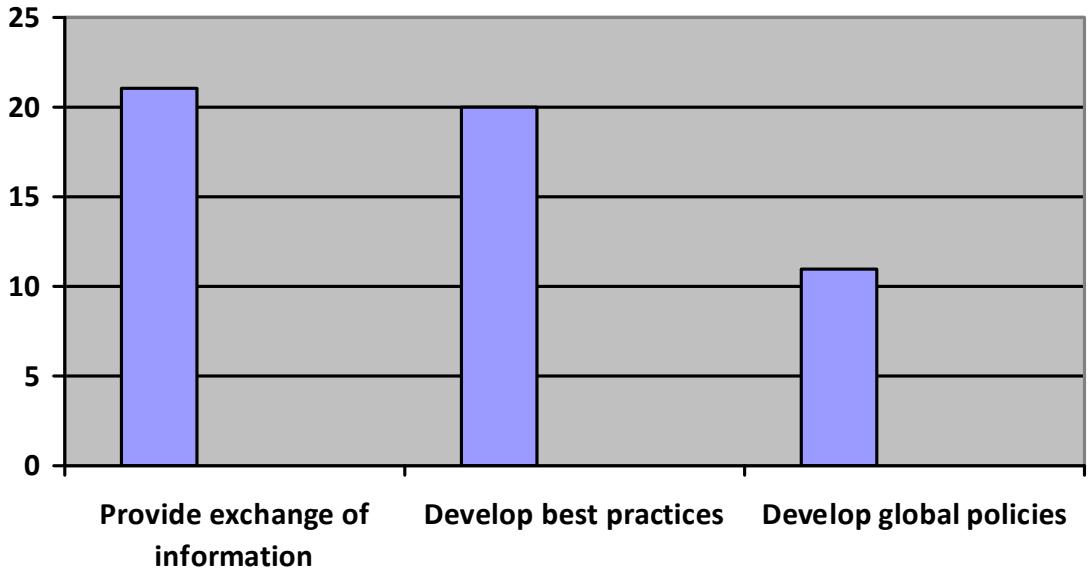
Some additional suggestions were “Education of public on phishing” or “notifying relevant authorities on the phisher” (compiled under “Other”).

9) Would you like the ccNSO to continue to undertake initiatives regarding anti-phishing?



Most believed this should be an item for further work within the ccNSO.

9.1 If YES, which activities should the ccNSO undertake in your view?



Most believed the ccNSO was useful for providing information exchange and developing best practices, with less believing that development of global policies was appropriate.

It was also suggested that ICANN should accredit Anti-phishing agencies so that registries can trust the source, when contacted on phishing incidents by such agencies.