Dear all,

As phishing is becoming a more and more serious problem which many ccTLDs have to struggle with, the ccNSO is trying to find out whether it can take any action on the issue.

In order to get an idea of how many ccTLDs are affected and what countermeasures could be undertaken, we are launching a short survey.

We would be very grateful if you could take a few minutes to reply to the questions. You can also provide your answers in Arabic, French, German, Russian or Spanish, if this is more convenient.

The replies will be correlated by the ccNSO Secretariat and presented to the whole community. The individual answers will not be visible and the information will be treated as private and confidential.

The survey is open for your replies until the 21st March 2008.

Please, send your answers to ccnsosecretariat@icann.org or directly to me.

Many thanks for your help.

Kind regards,

Gabi

Gabriella Schittek
ccNSO Secretariat
gabriella.schittek@icann.org

Anti-Phishing Survey

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

YES/NO

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

YES/NO

2) Who informs you about a phishing incident?

Specially dedicated anti-phishing agents
Government agents
Internet engineering bodies
CERTS
Affected companies
Registry
Registrar
Registrants
Other (please, specify)

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

YES/NO

3.1) If YES: Are they published?

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

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

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

Haven't thought about it
There is no phishing problem under our ccTLD
There are government agencies responsible for that
The Registry decided not to, as it has to do with content and use of the domain name
We are unable to implement such policies because of the terms of our agreement with the sponsoring organisation for the ccTLD.
Other (please, specify)

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

Registry
External Committee
Registrar
Court
Other (please, specify)

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

YES/NO

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

Per email
Per post
Per telephone
Other (please specify)

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

YES/NO

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

1 day or less
1 – 3 days
3 days – 1 week
1 – 3 weeks
3 weeks or more

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)

1 day or less
1 – 3 days
3 days – 1 week
1 – 3 weeks
3 weeks or more

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

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

Deletion of the domain name
Suspension of the domain name
Shutting down the web site (through the hosting provider)
Send a warning to the phisher
Criminal prosecution
Other (please, specify)

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

YES/NO

9.1. If YES, which of the following activities should the ccNSO undertake in your view:

- Providing exchange of information on Phishing issues
- Develop Best Practices on Phishing issues
- Develop global policies on Phishing issues
- Other (please, specify)