APTLD & MYNIC JOINT SURVEY

INTERNET SECURITY
& CCTLDS
SURVEY RESULTS

24th June 2008, Tuesday
ccNSO meeting, Paris, France

Survey Objectives

Survey Summary:-

For APTLD members to examine the roles and responsibilities of ccTLDs in Internet security. This survey is on security-related issues when it comes to the registration and renewal of domain names, with a particular focus on fast flux & phishing.

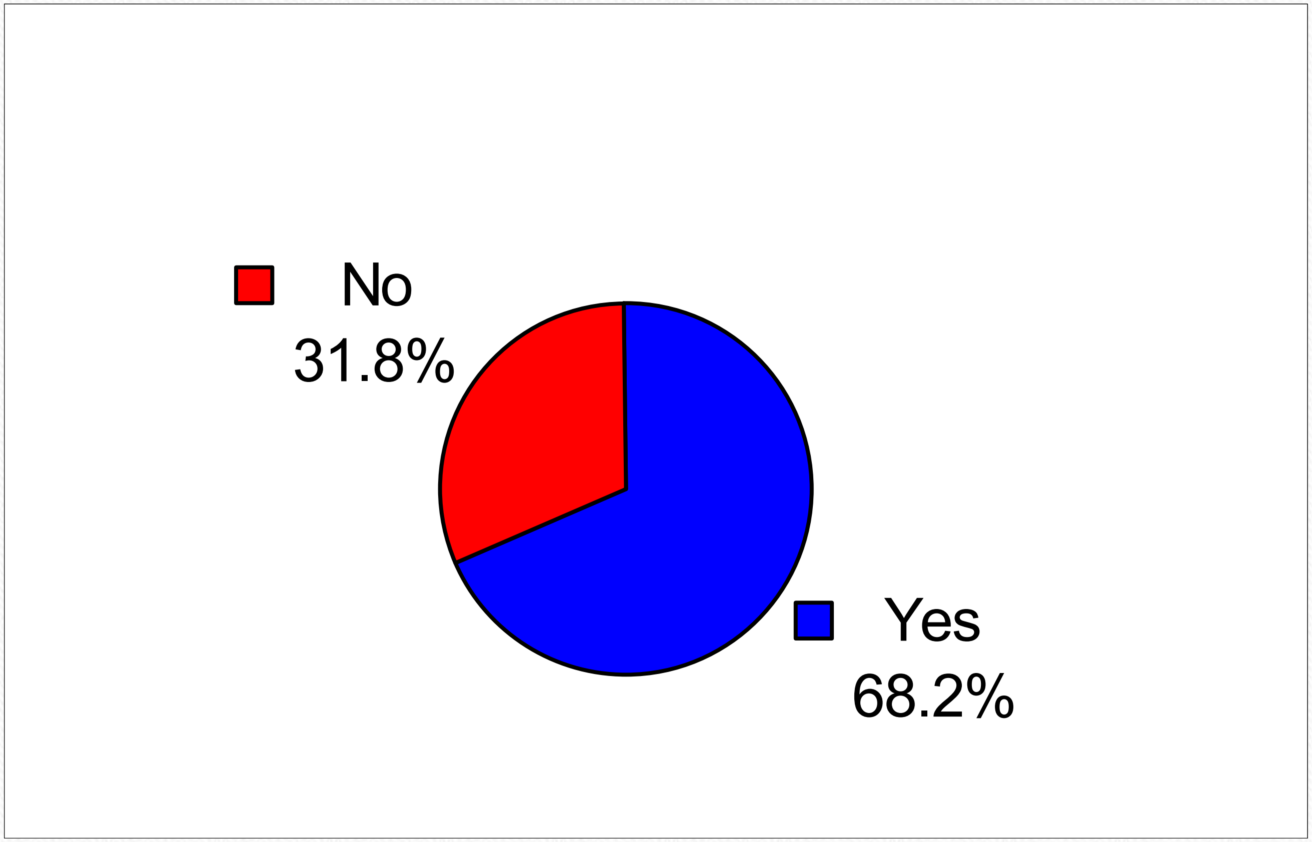
The objective of this survey is to

- facilitate an exchange of information
- share best practices
- Assess how ccTLDs can cooperate & work closely with their respective CERTs on preventing & tackling phishing incidents
- Assess how ccTLDs can improve on the security level for customers of domain names
- Assess what are the security issues currently faced by ccTLDs

APTLD & MYNIC JOINT SURVEY

Q1

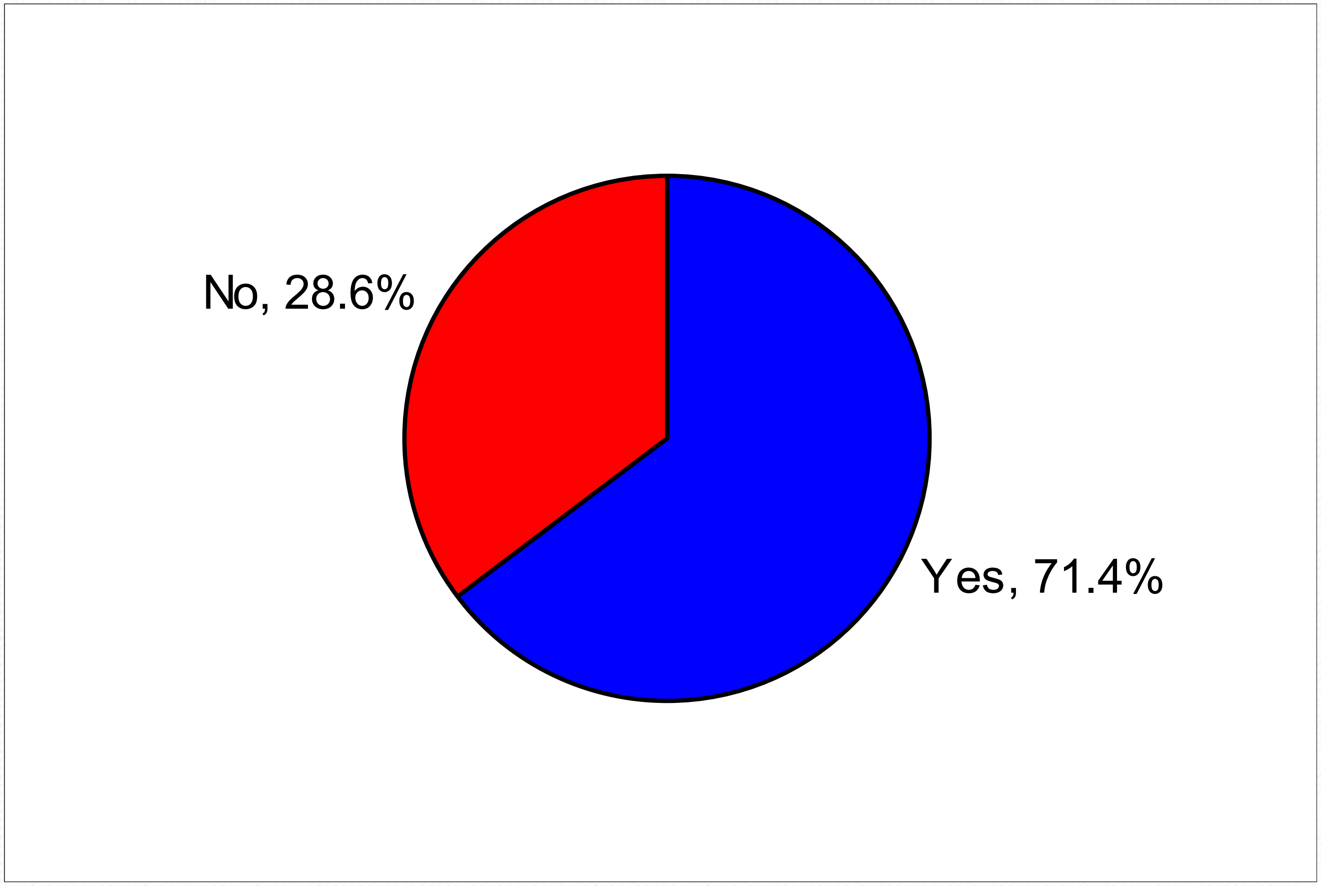
Do you have restrictions on who can register a name?



APTLD & MYNIC JOINT SURVEY

Q2

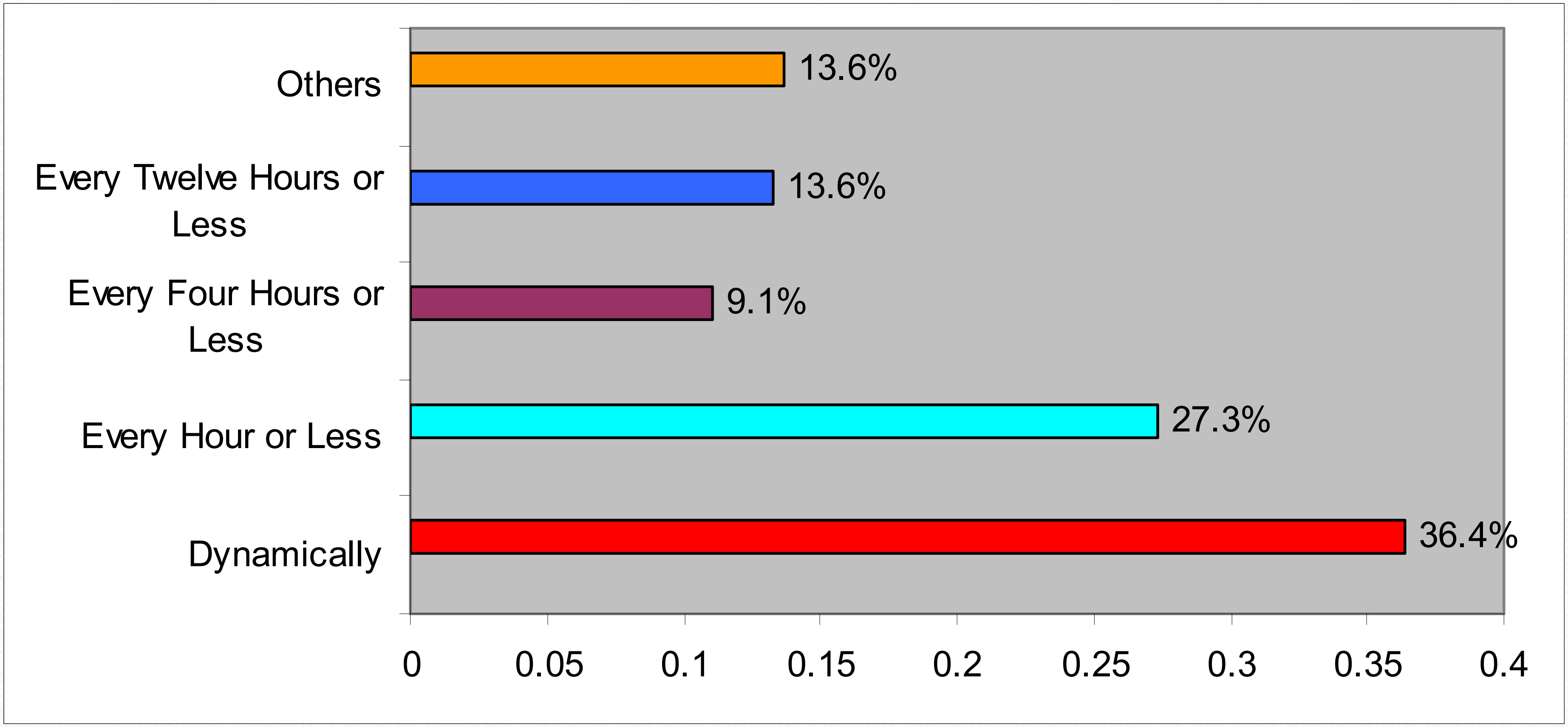
Do you or your Registrar or Reseller validate the details of registrants?



Q3

How often do you update your zone file?

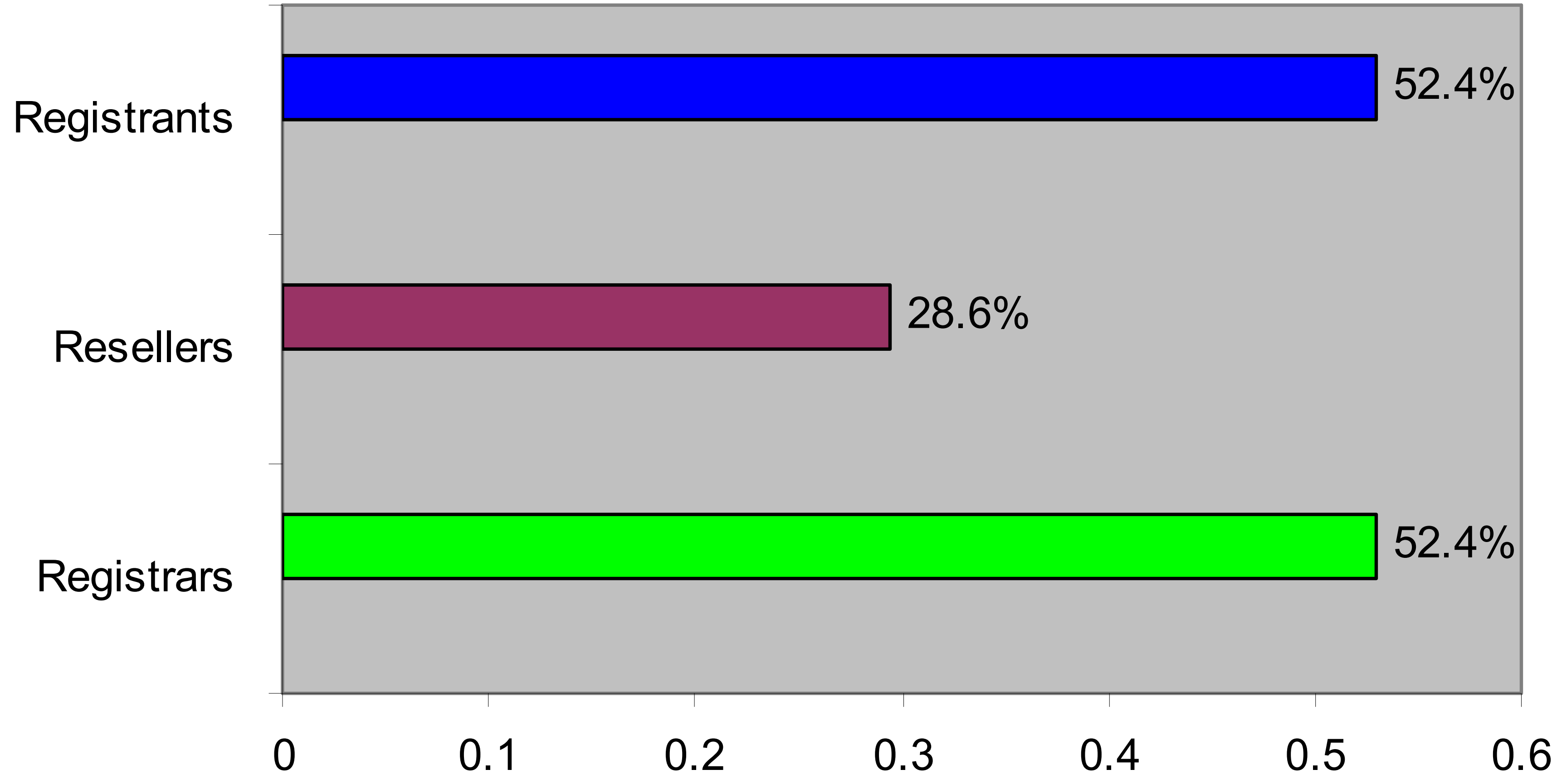
APTLD & MYNIC JOINT SURVEY



Q4

Which of the following do you validate?

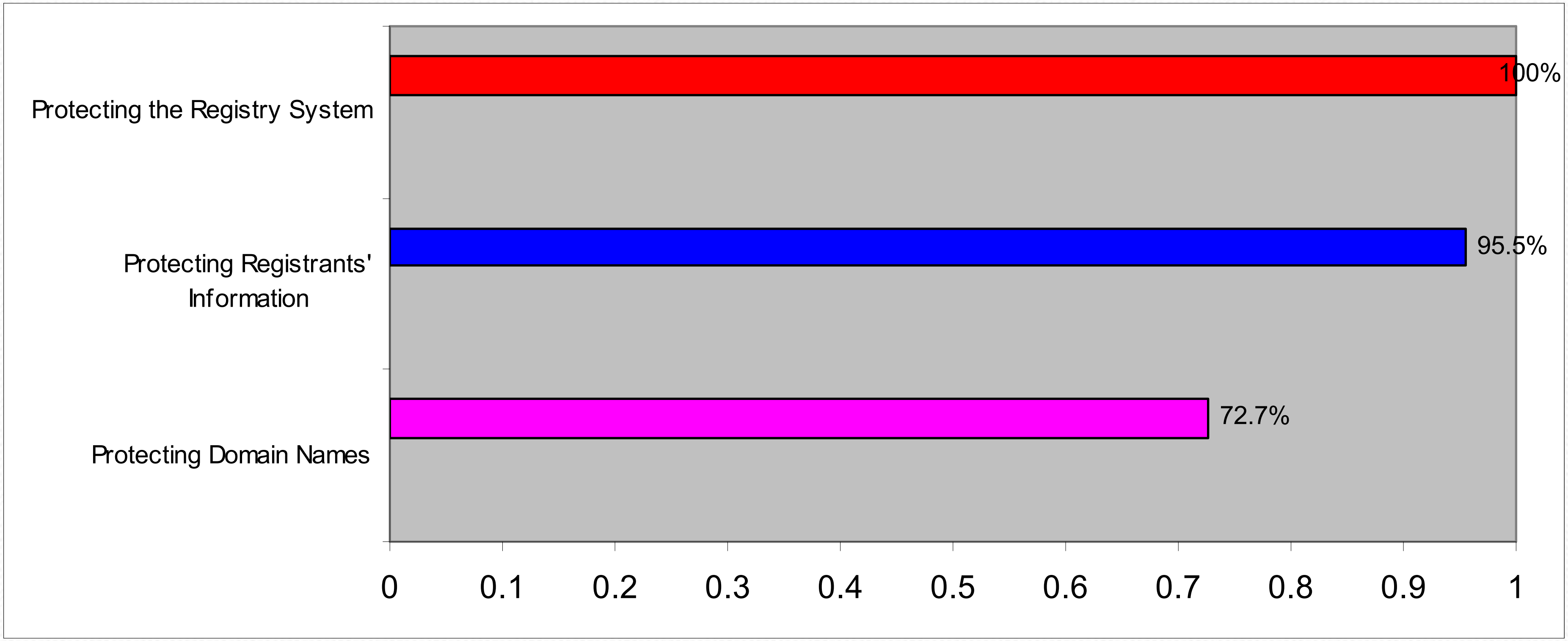
APTLD & MYNIC JOINT SURVEY



Q5

What does Internet Security mean to you?

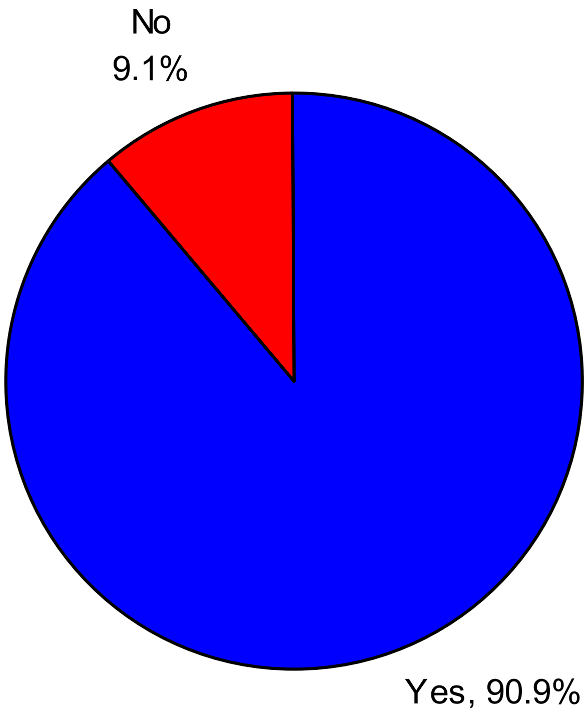
APTLD & MYNIC JOINT SURVEY



Q6

Does your ccTLD provide security as to who can change the Registrants' contact information?

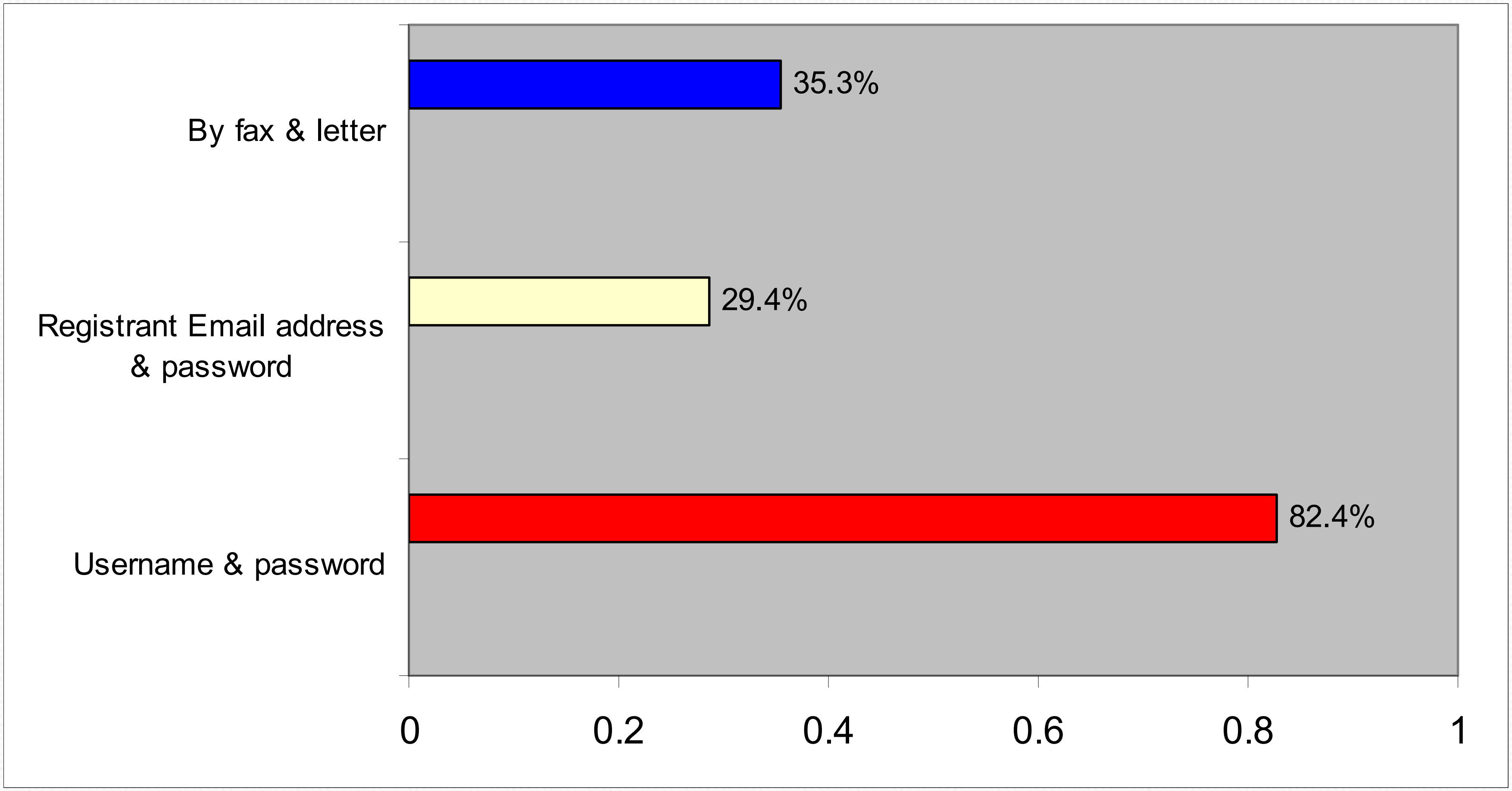
APTLD & MYNIC JOINT SURVEY



Q7

What are the security measures your ccTLD provide to allow changes to Registrants' contact information?

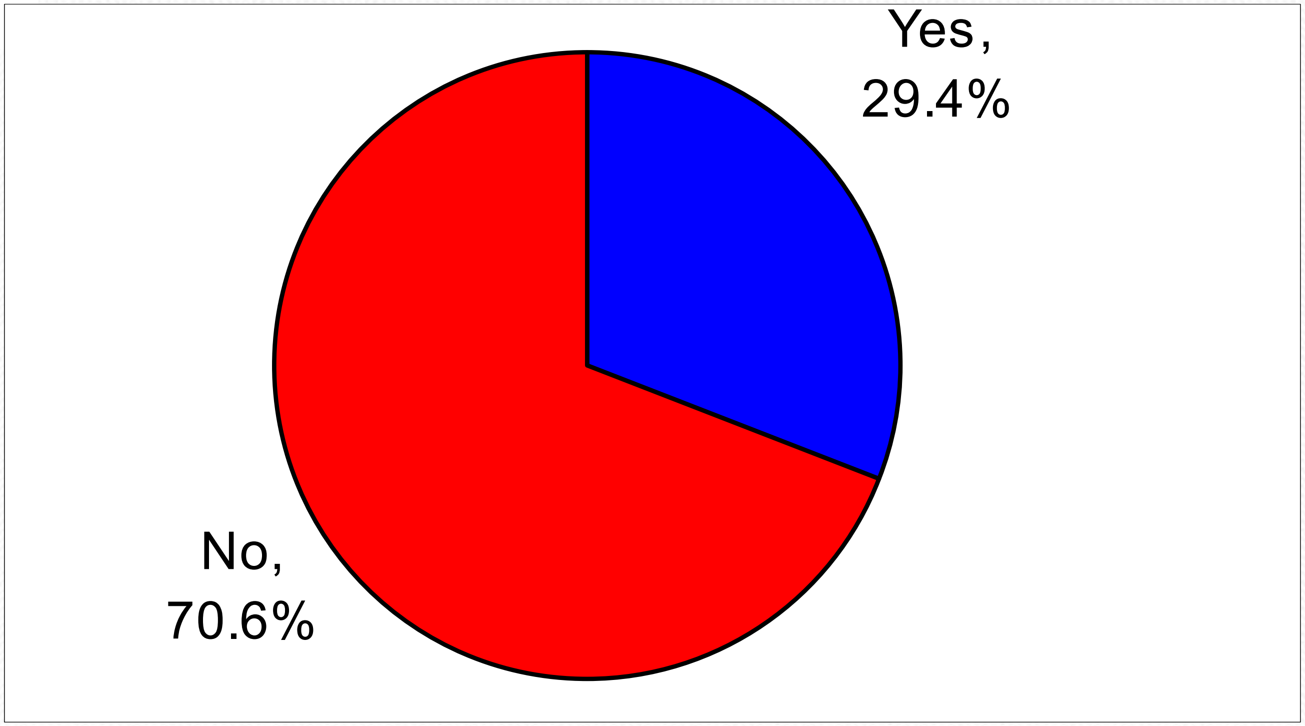
APTLD & MYNIC JOINT SURVEY



Q8

Does your Registry system put in place a security feature to bar access to registrants' contact information after three (3) unsuccessful attempts using password?

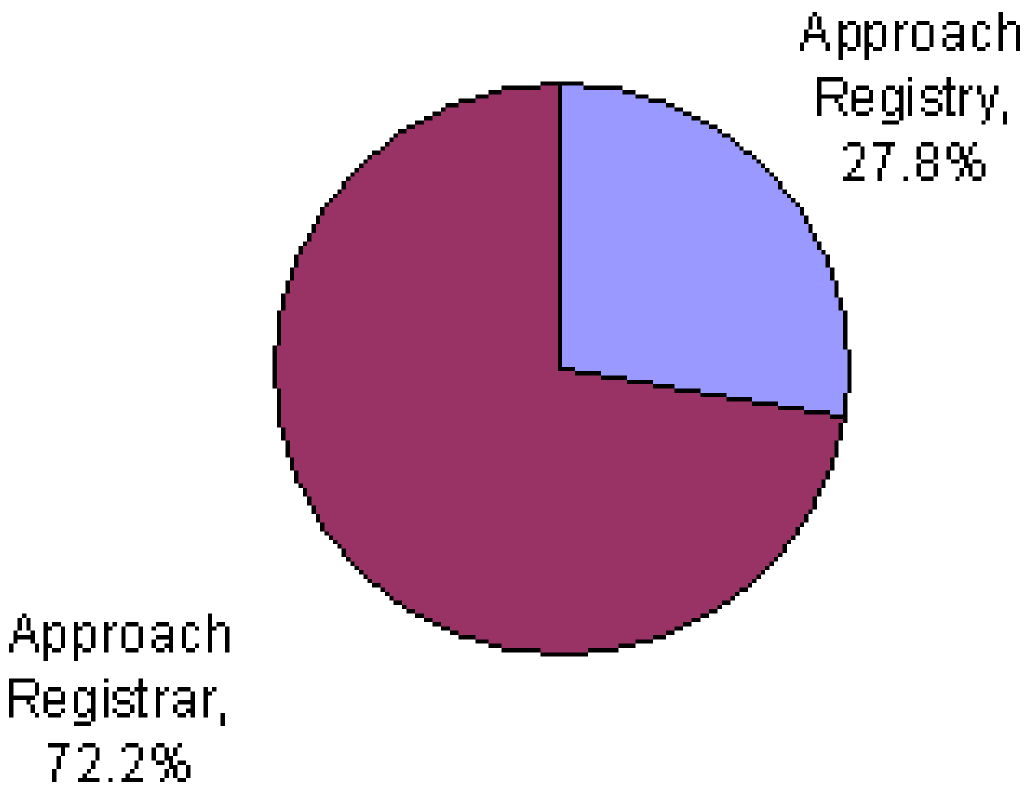
APTLD & MYNIC JOINT SURVEY



Q9

What can your Registrant do if they forget their username and password?

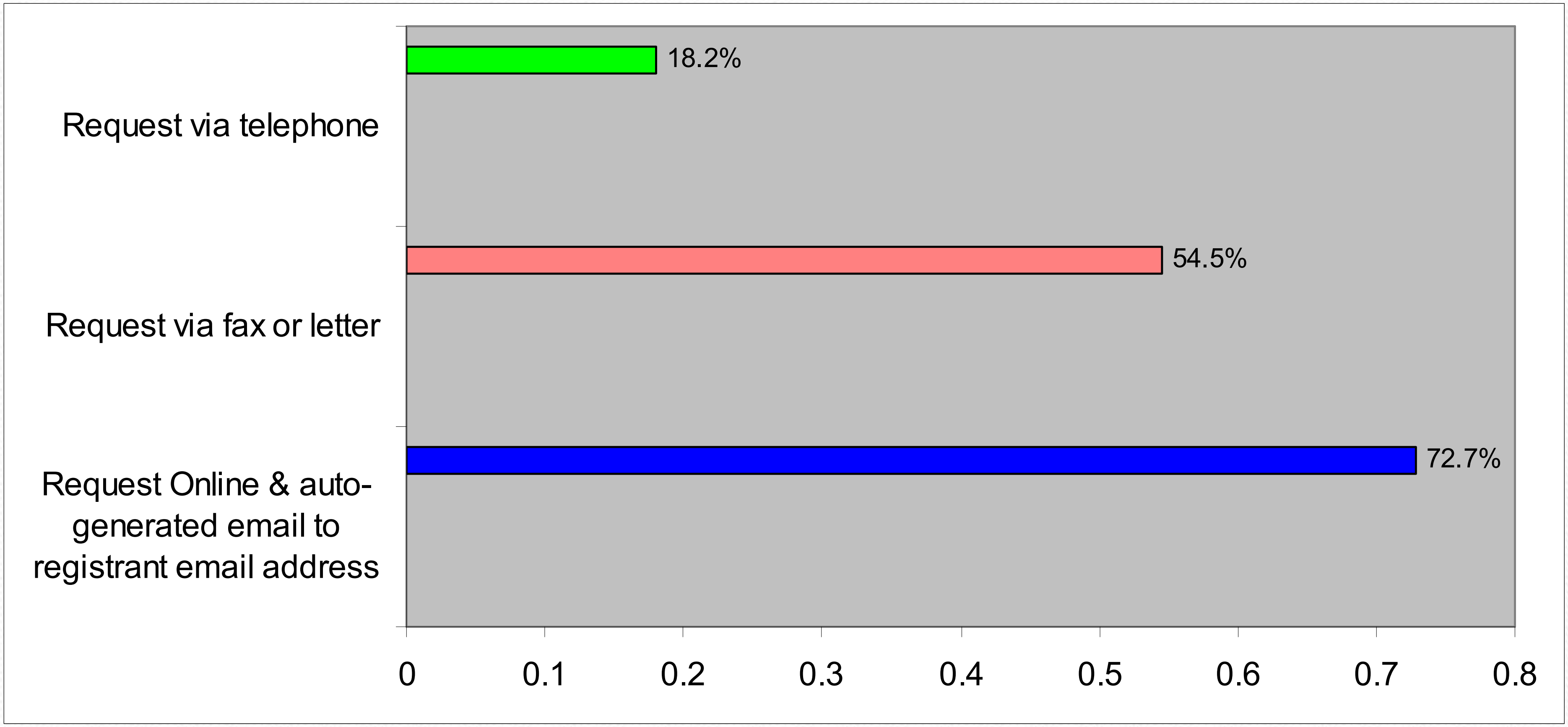
APTLD & MYNIC JOINT SURVEY



Q10

How can the Registrant retrieve the username and password?

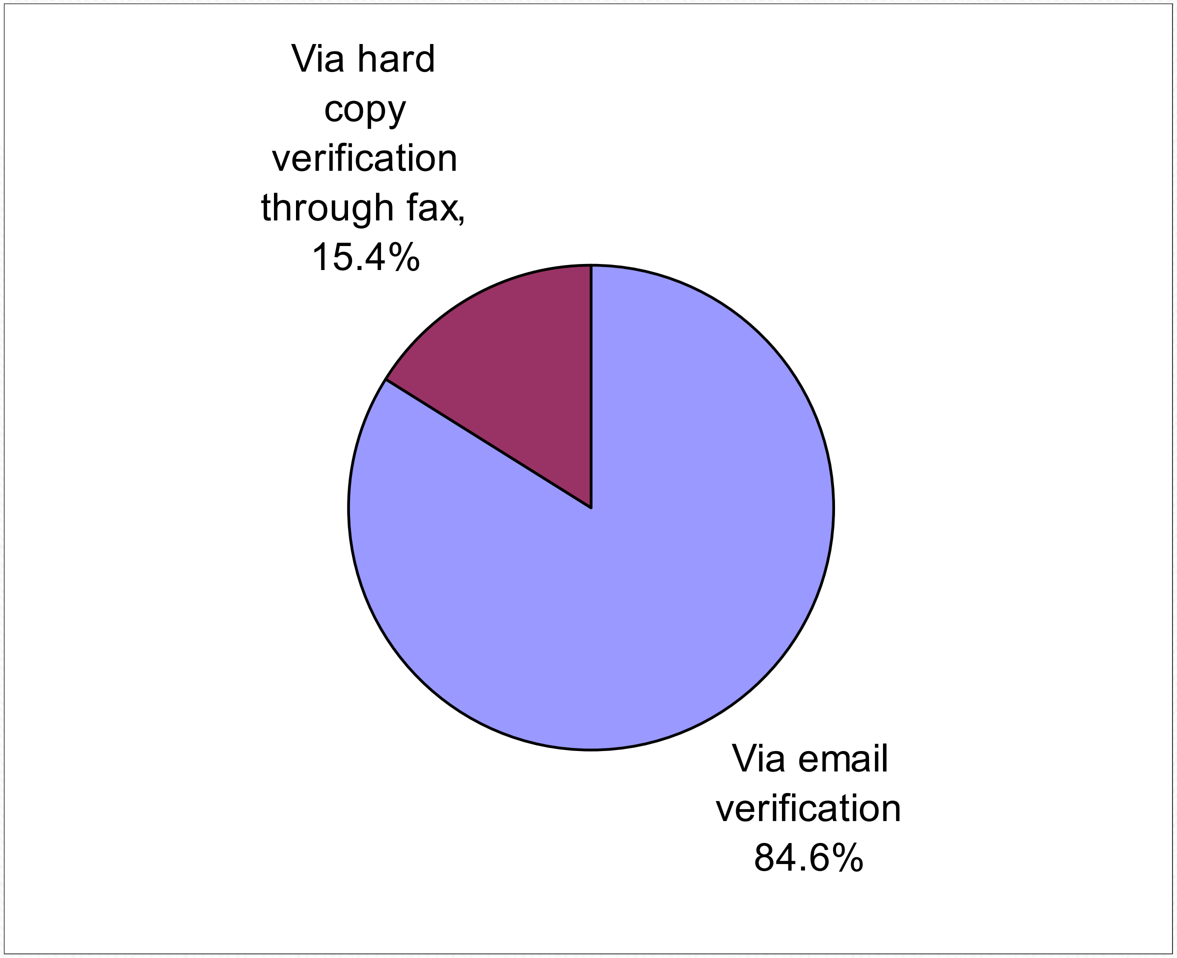
APTLD & MYNIC JOINT SURVEY



APTLD & MYNIC JOINT SURVEY

Q11

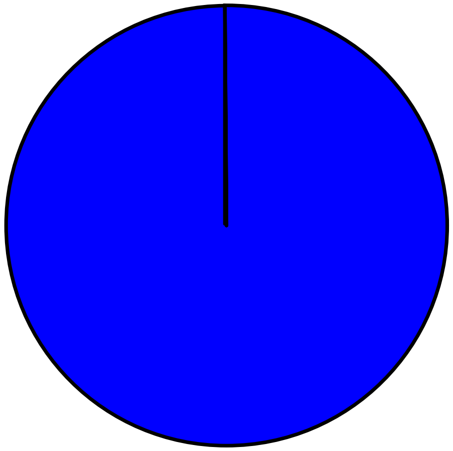
How are the security measures (e.g. username & password) provided to your Registrants?



Q12

Do you allow your Registrant/ Contact Person to use as their email address, those obtained from free services?

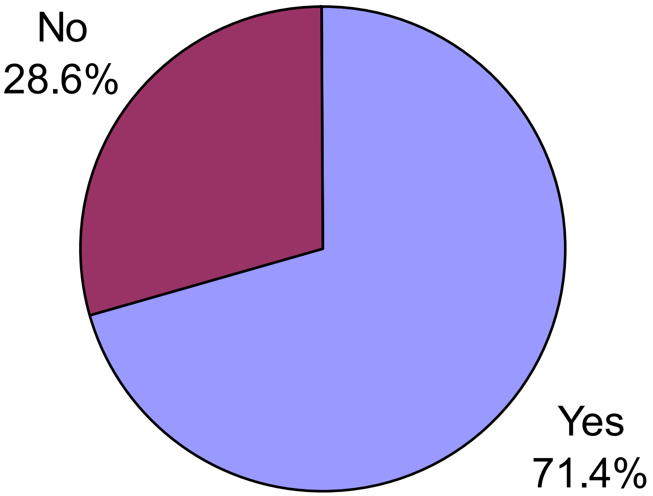
APTLD & MYNIC JOINT SURVEY



Q13

Can your Registrant change their organization name (e.g. business or company name)?

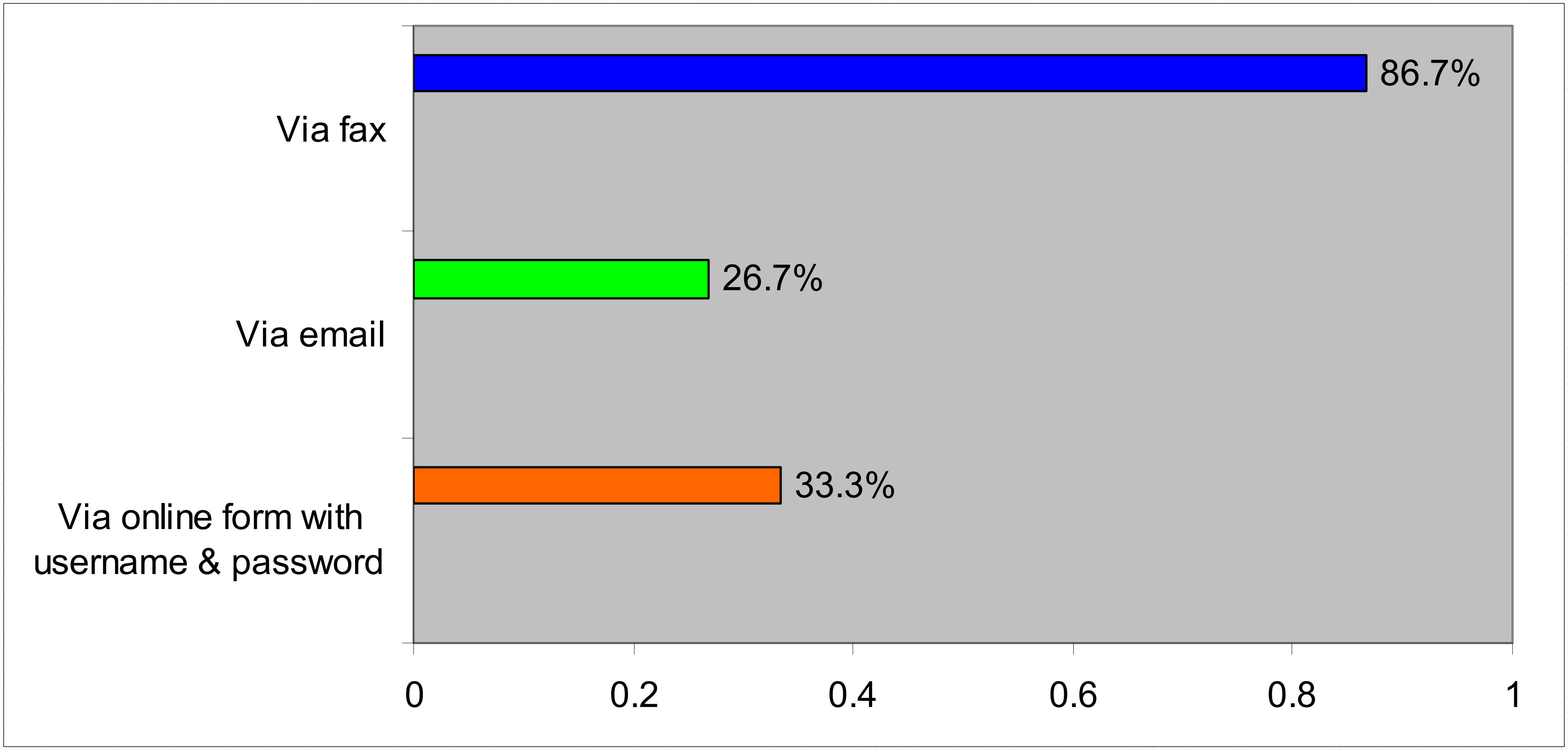
APTLD & MYNIC JOINT SURVEY



Q14

How does your Registrant request the changes to their organization name?

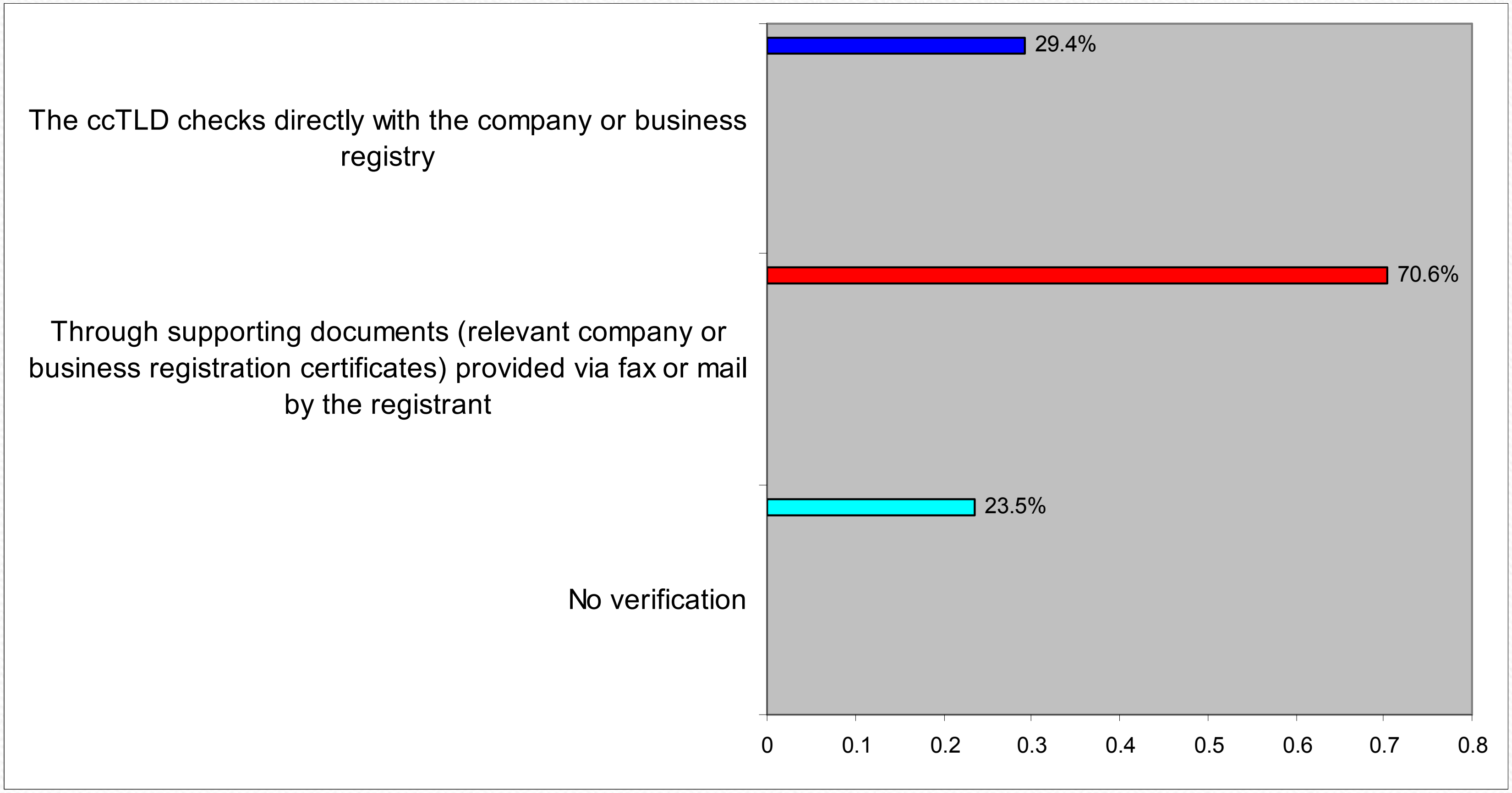
APTLD & MYNIC JOINT SURVEY



Q15

How does your ccTLD verify the changes in the Registrant organization name?

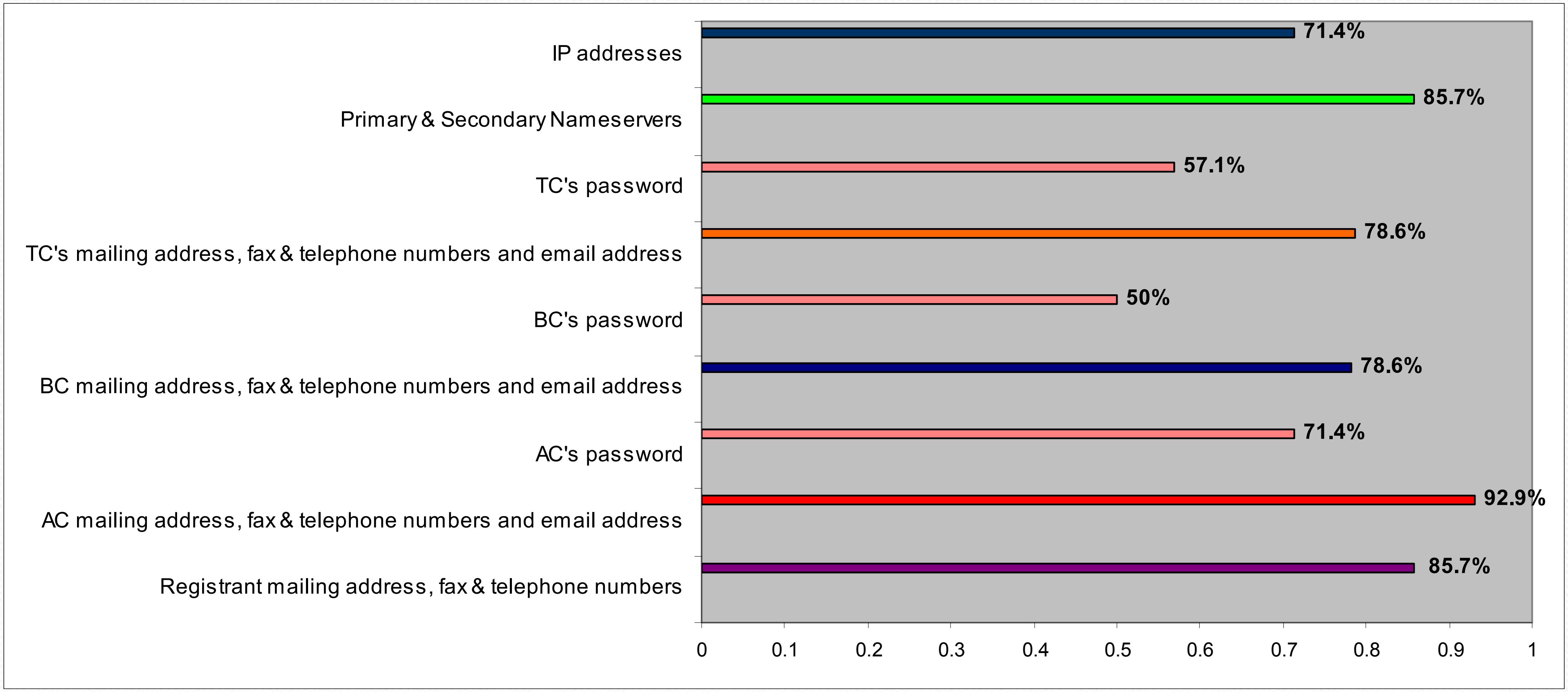
APTLD & MYNIC JOINT SURVEY



Q16

What contact information can be changed online using the password provided to the AC?

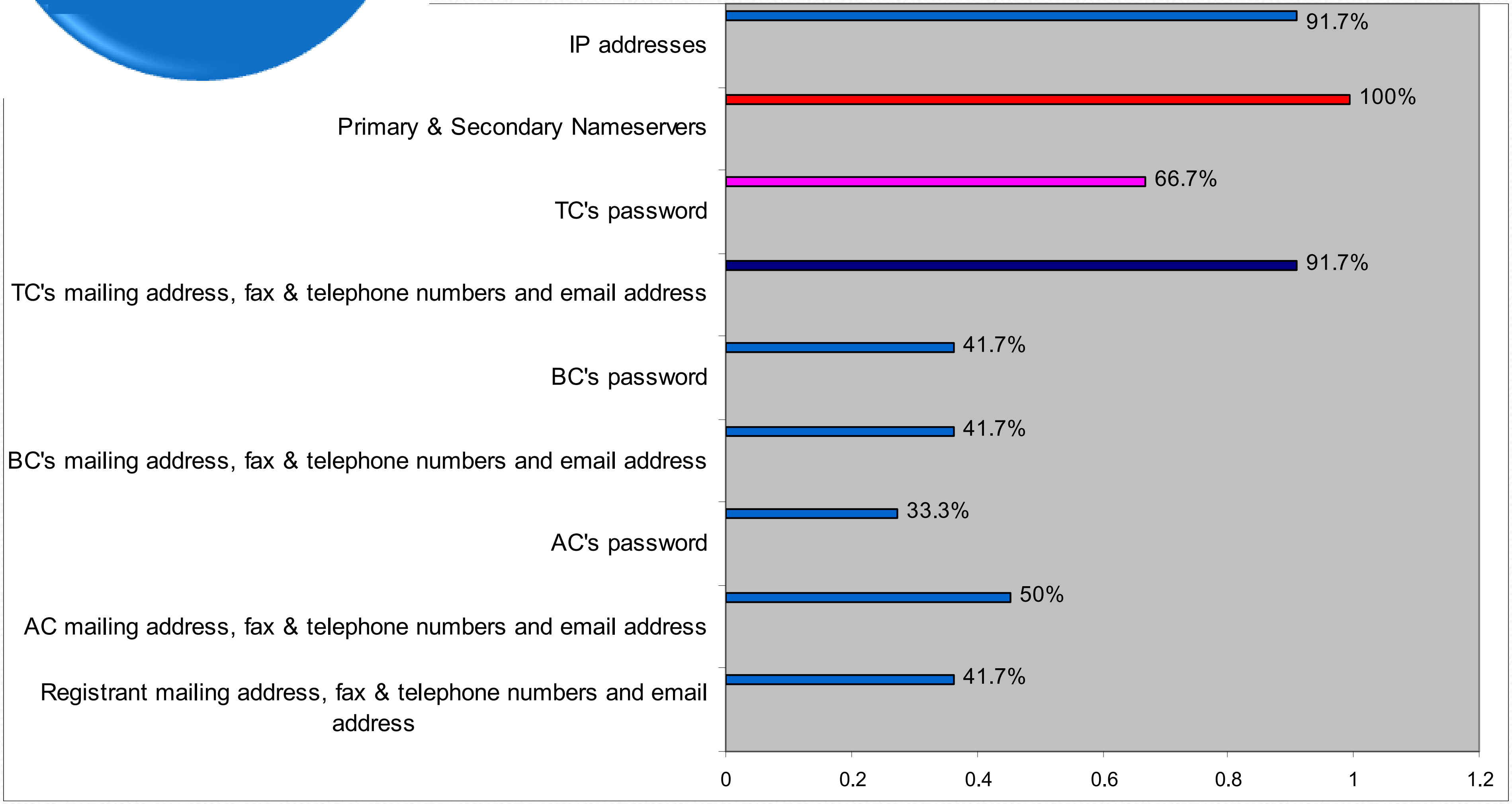
APTLD & MYNIC JOINT SURVEY



Q17

What contact information can be changed online with the password provided to the TC?

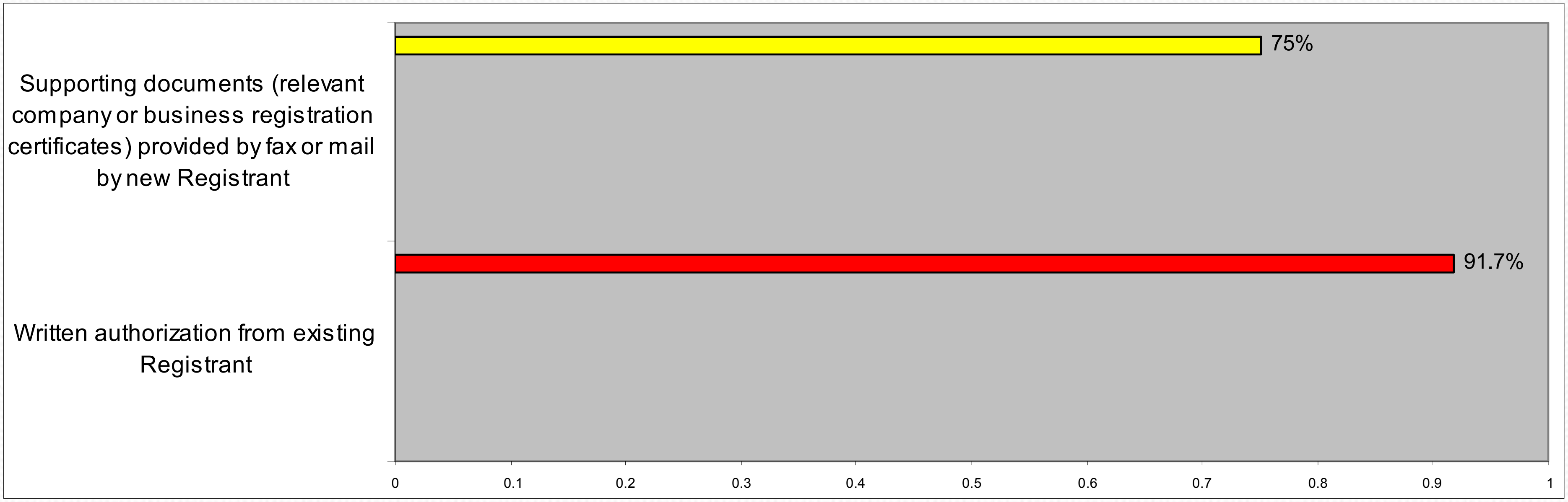
APTLD & MYNIC JOINT SURVEY



Q18

What are required to transfer the domain name from existing Registrant to new Registrant?

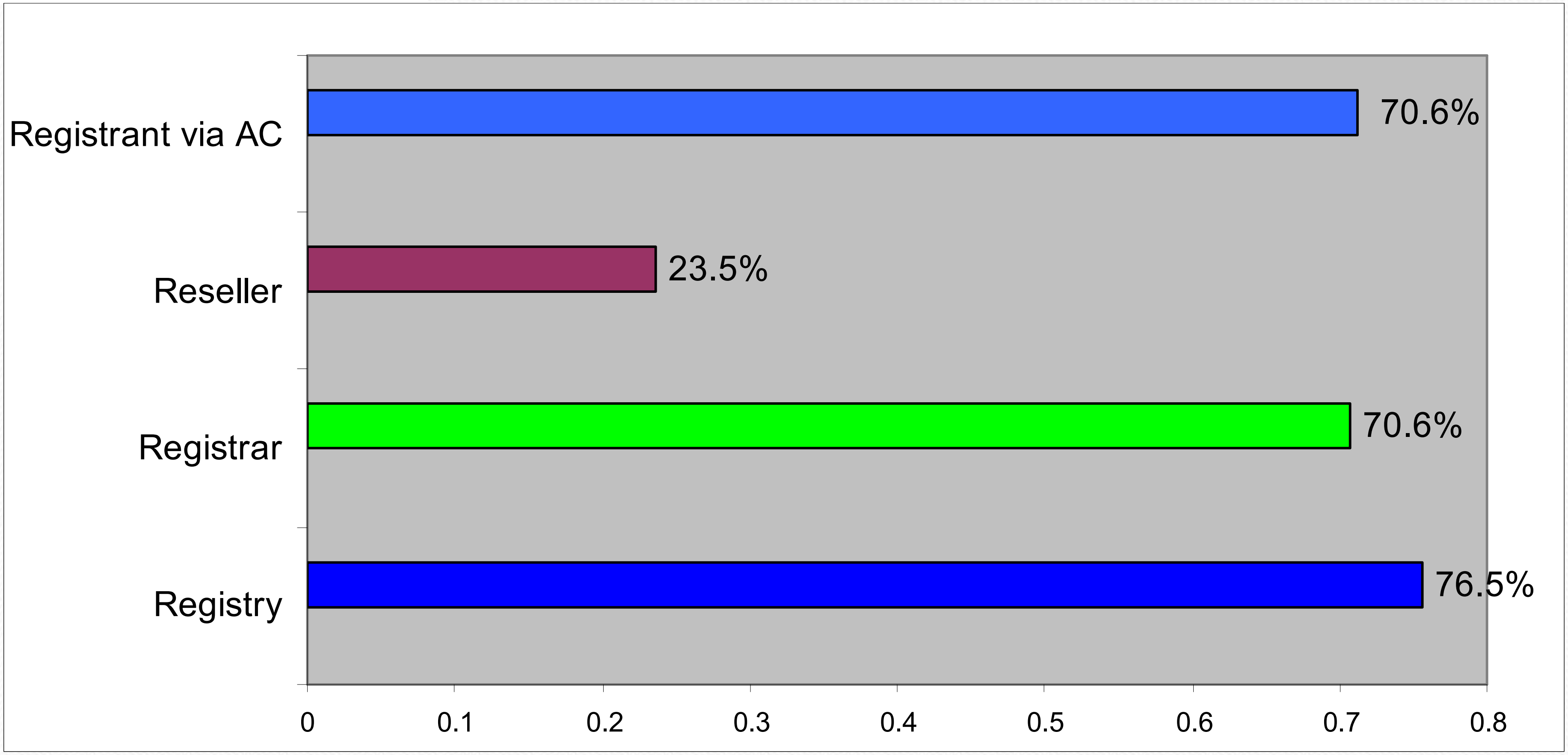
APTLD & MYNIC JOINT SURVEY



Q19

Who is/are involved in the transfer of domain name from existing Registrant to new Registrant?

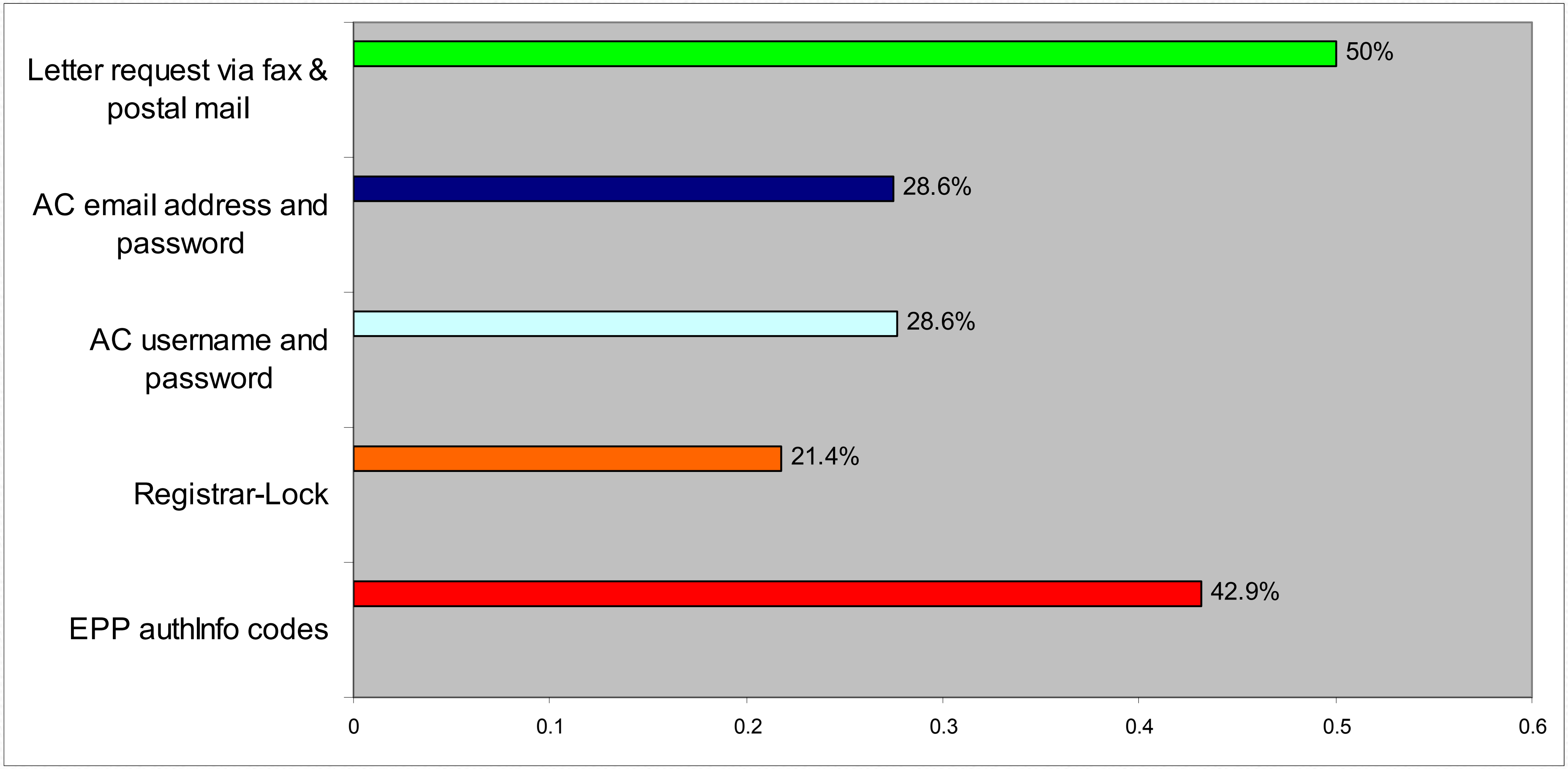
APTLD & MYNIC JOINT SURVEY



Q20

What security measures are involved in the transfer process?

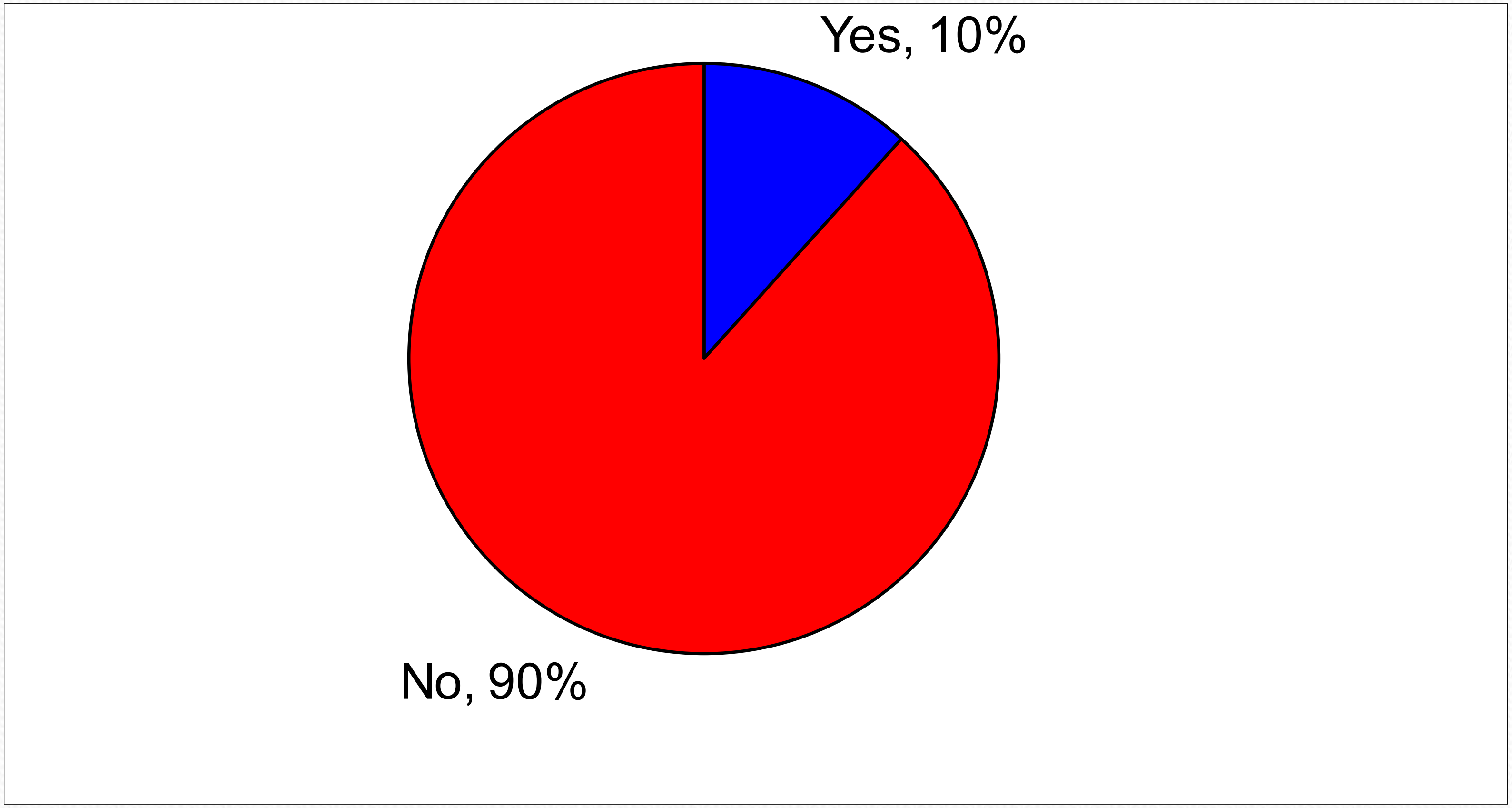
APTLD & MYNIC JOINT SURVEY



Q21

Has your ccTLD received any complaints from registrants that their DNS rrecords were used for fast flux activity?

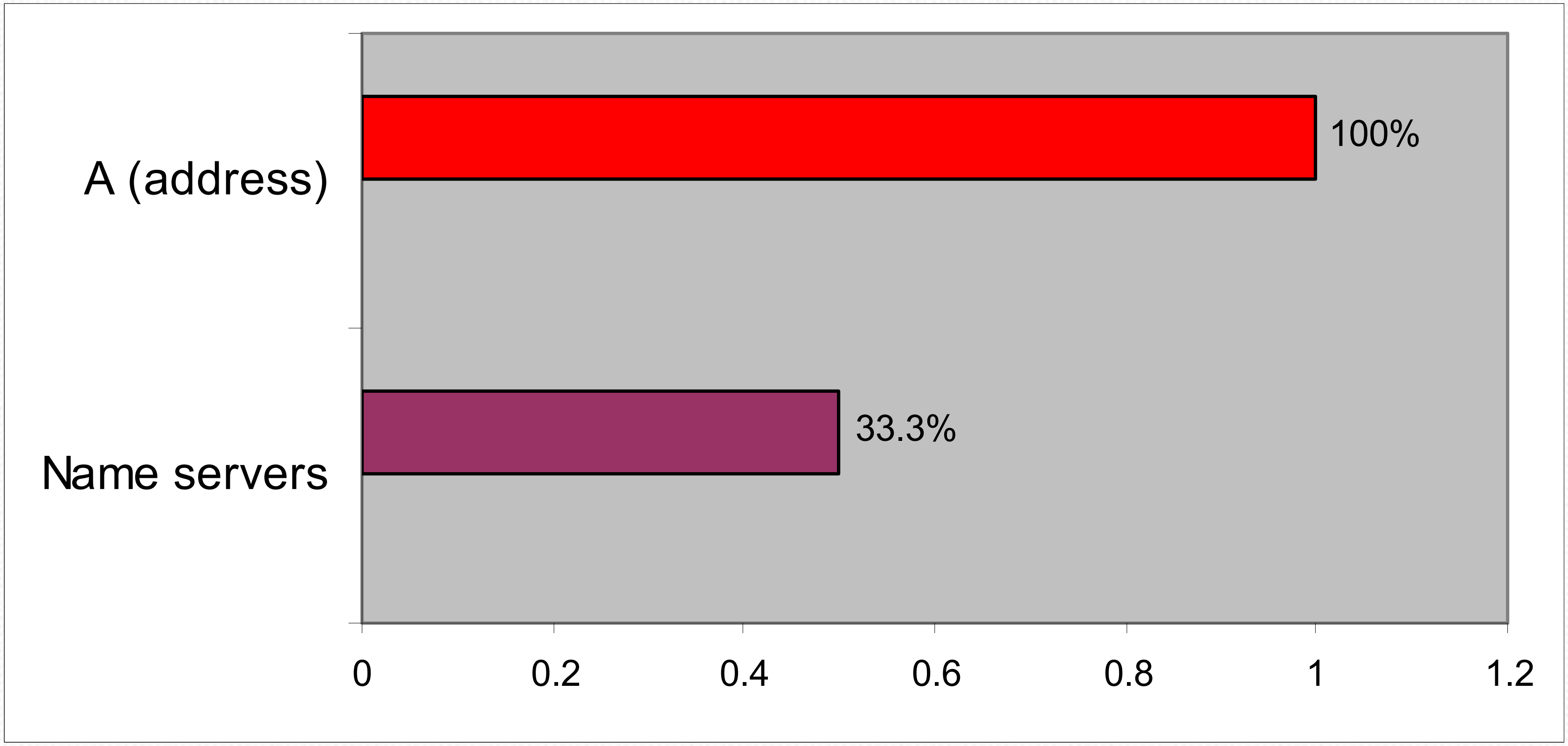
APTLD & MYNIC JOINT SURVEY



Q22

Which DNS resource Records were used for fast flux activity?

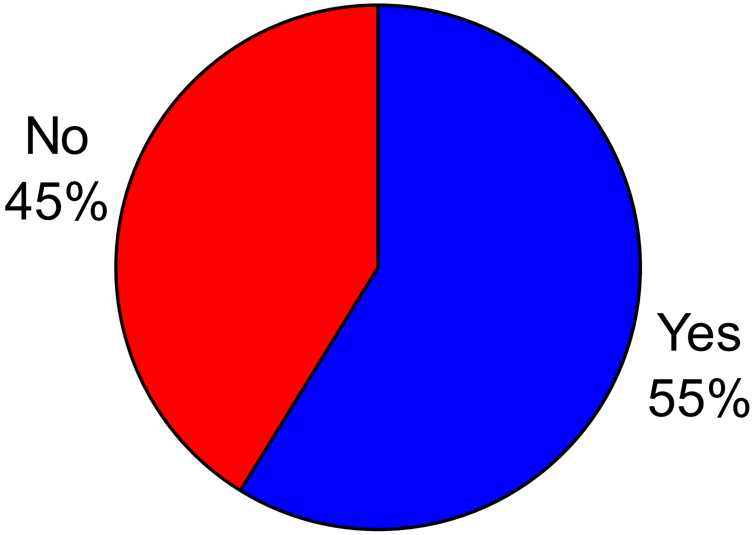
APTLD & MYNIC JOINT SURVEY



Q23

Has your ccTLD Domain names been used for phishing activity?

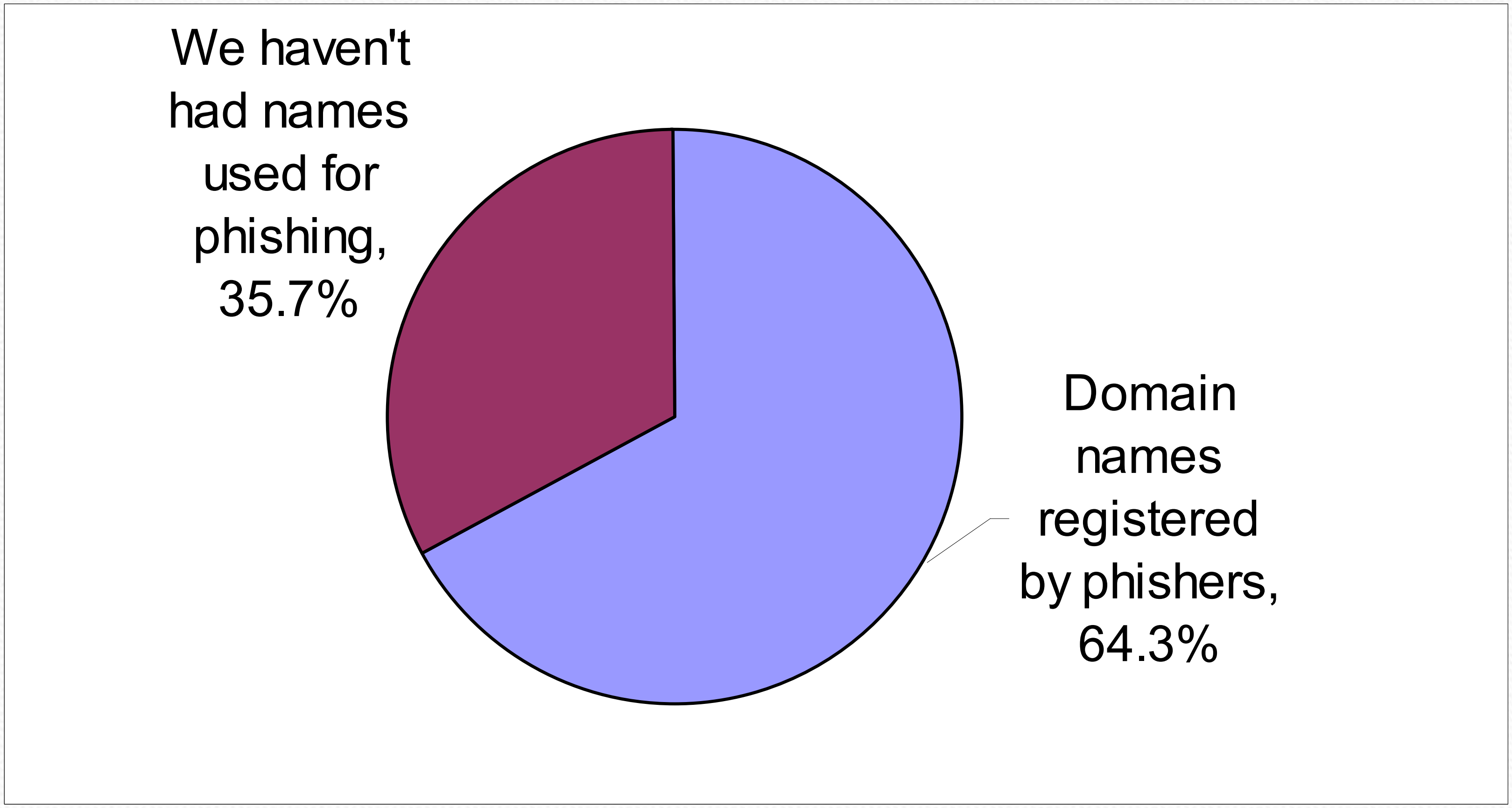
APTLD & MYNIC JOINT SURVEY



Q24

How is this phishing activity carried out?

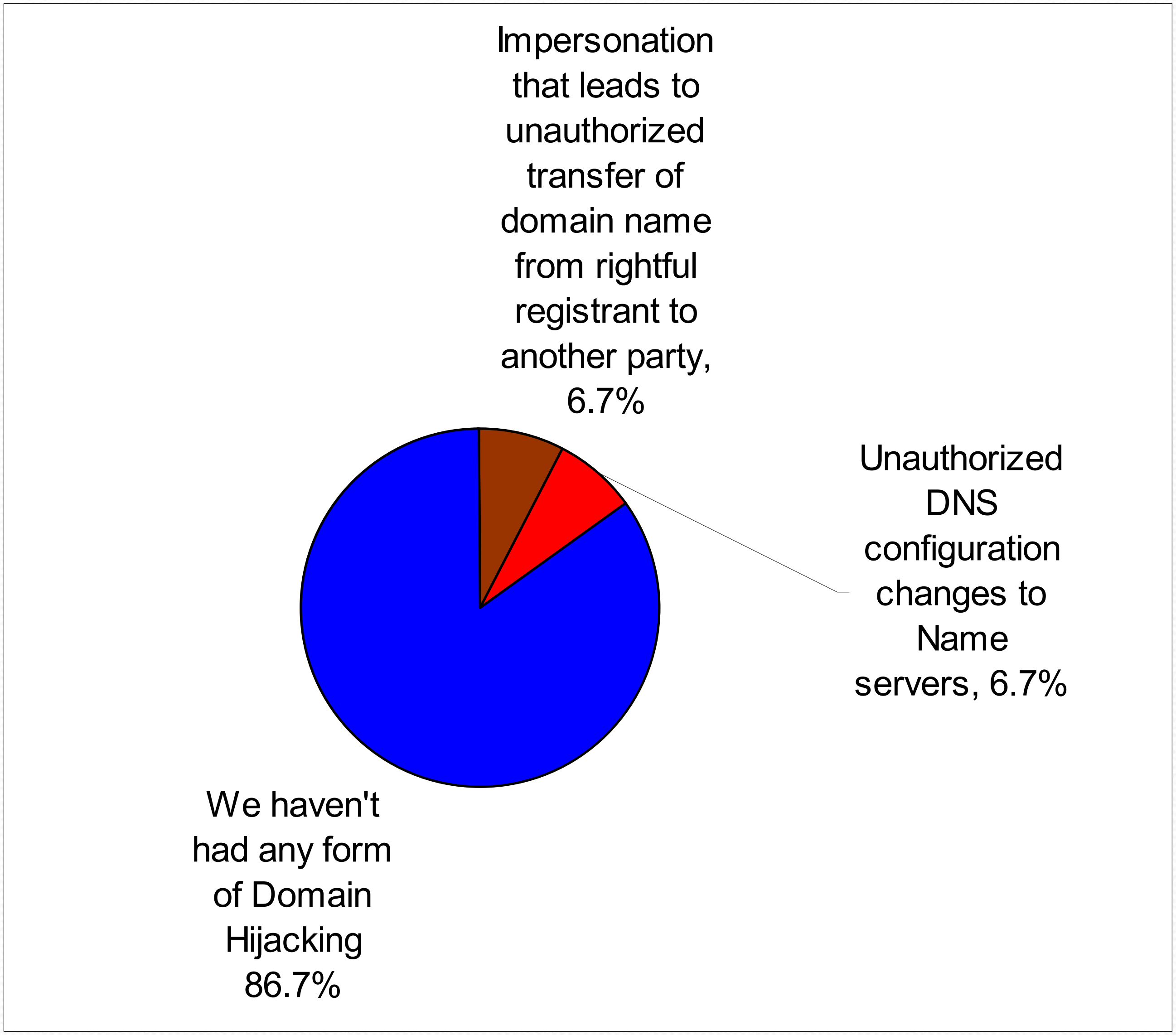
APTLD & MYNIC JOINT SURVEY



Q25

What forms of Domain Hijacking does your ccTLD registrants experience?

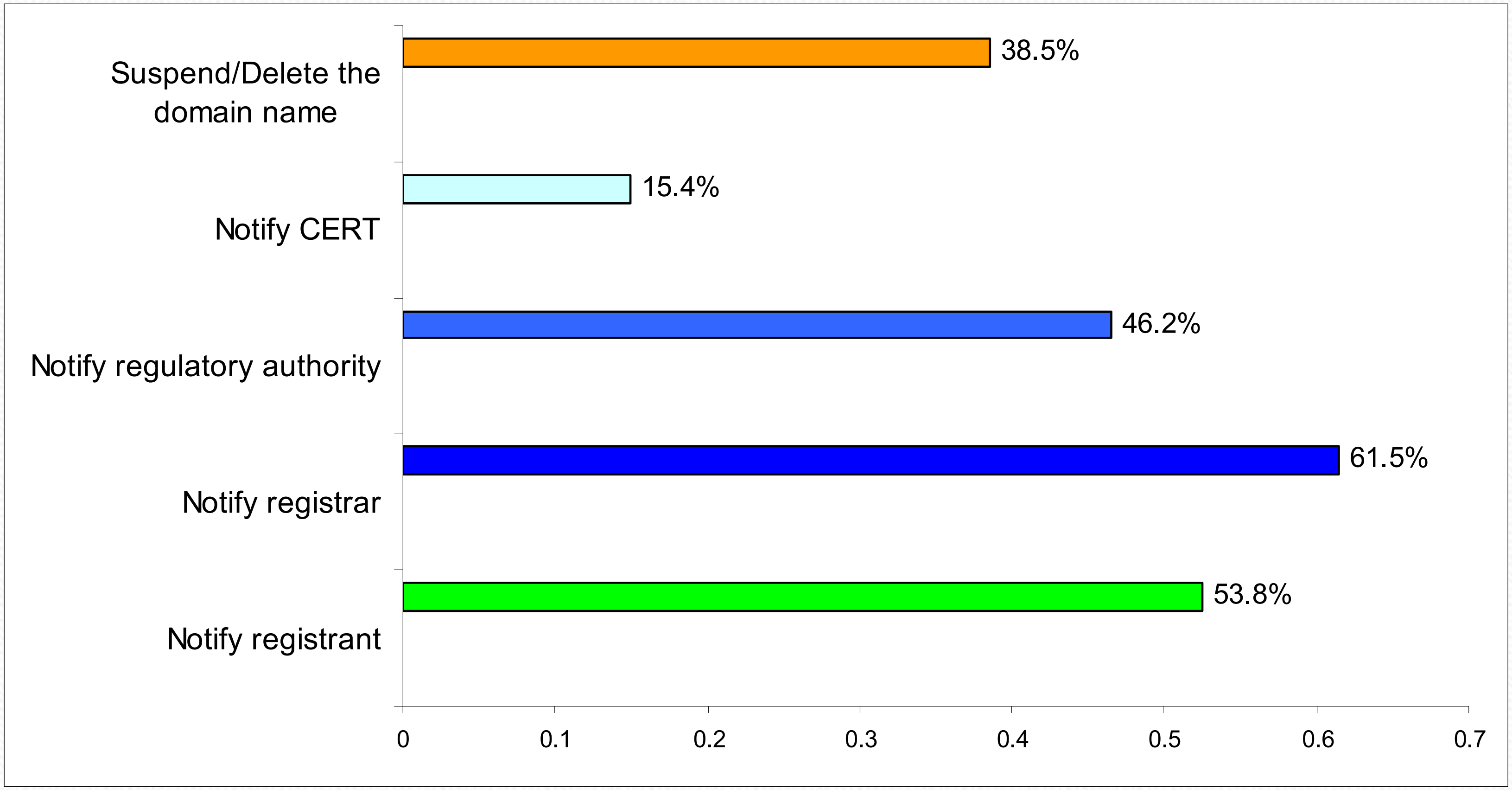
APTLD & MYNIC JOINT SURVEY



Q26

What action does your ccTLD take when complaint is directed to you?

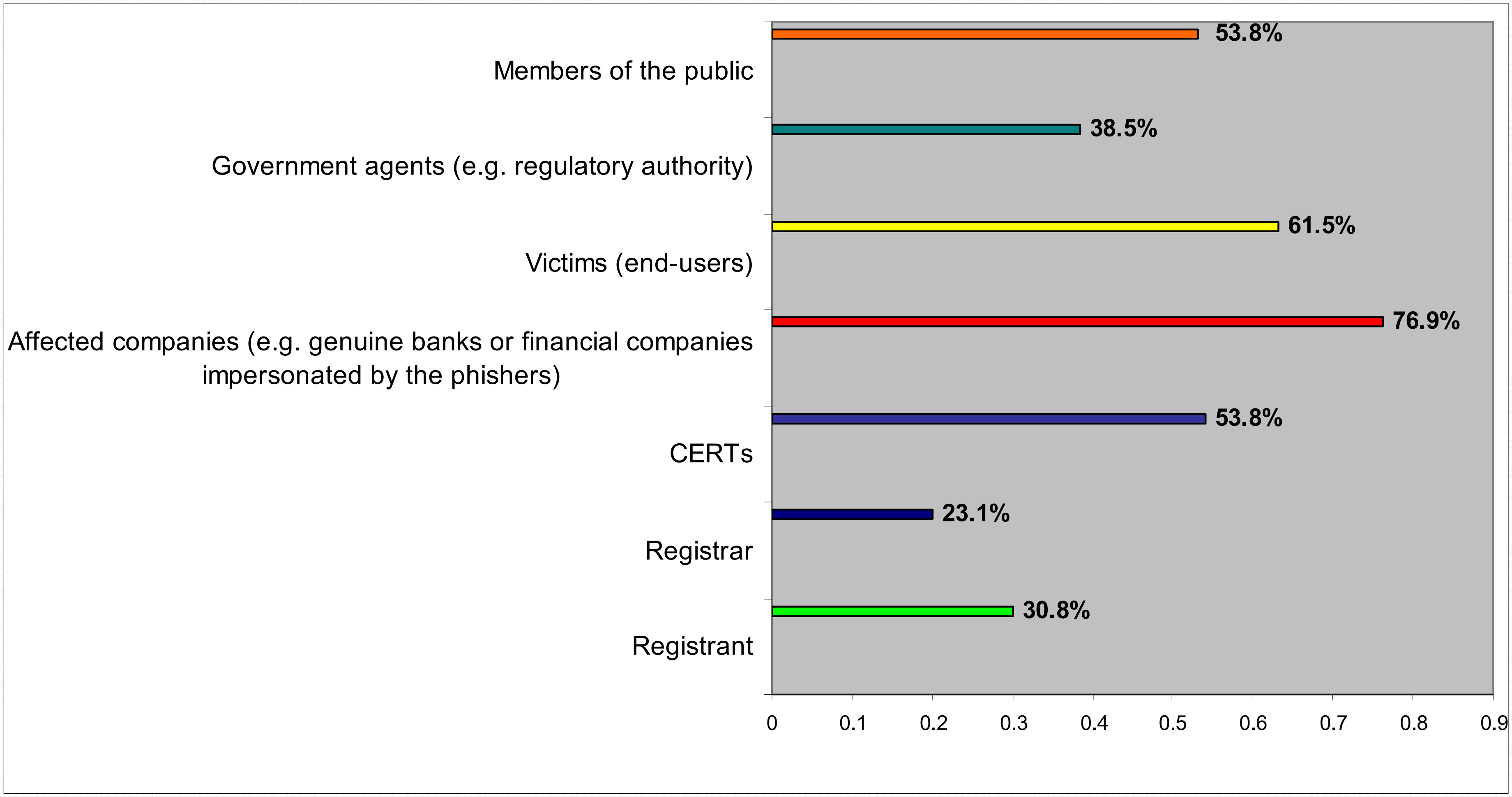
APTLD & MYNIC JOINT SURVEY



Q27

Who complains on the phishing activity to your ccTLD?

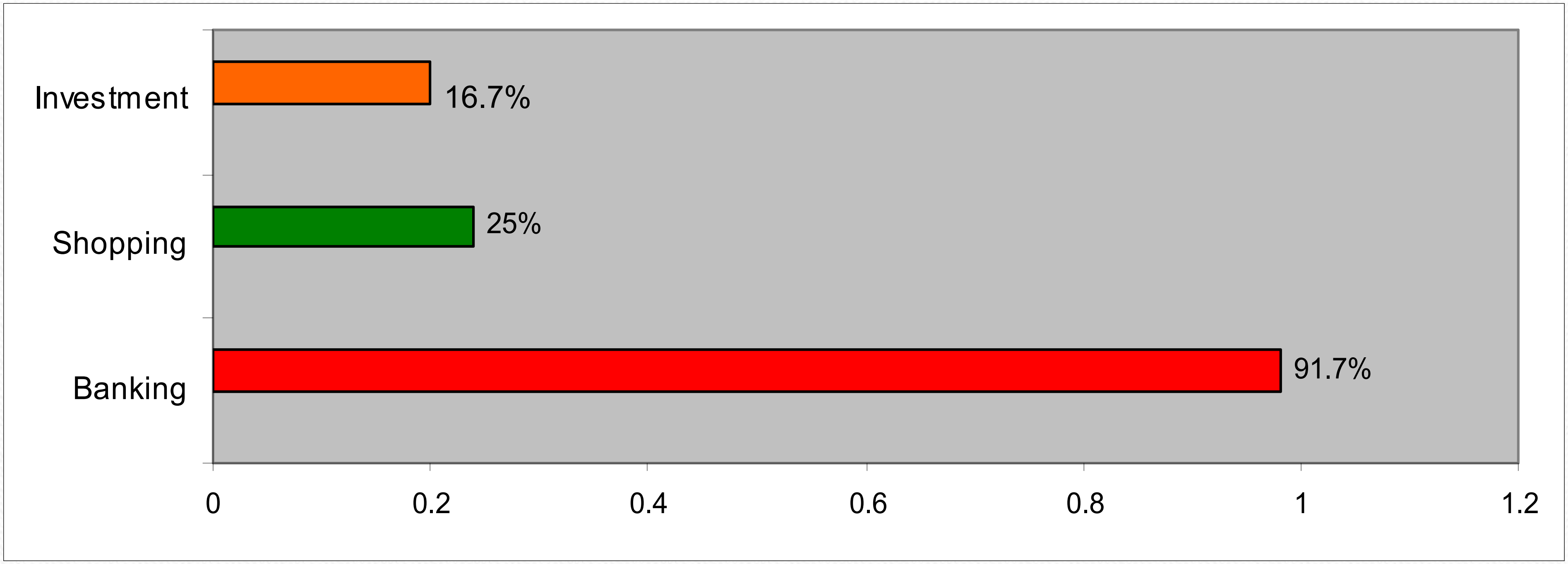
APTLD & MYNIC JOINT SURVEY



Q28

What is the type of phishing activity that your ccTLD domain names experience?

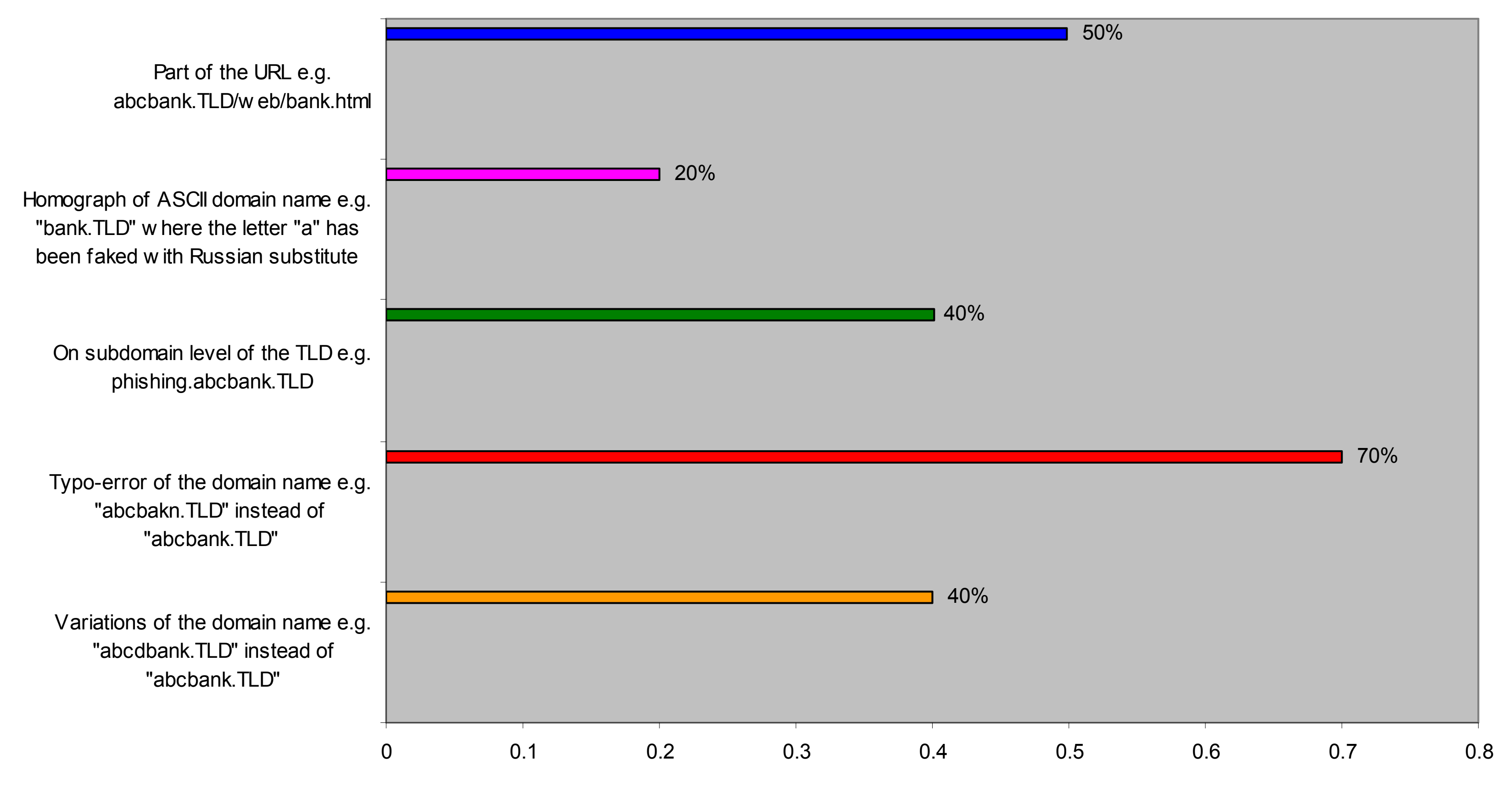
APTLD & MYNIC JOINT SURVEY



Q29

What are the patterns of domain name registrations used by phishers?

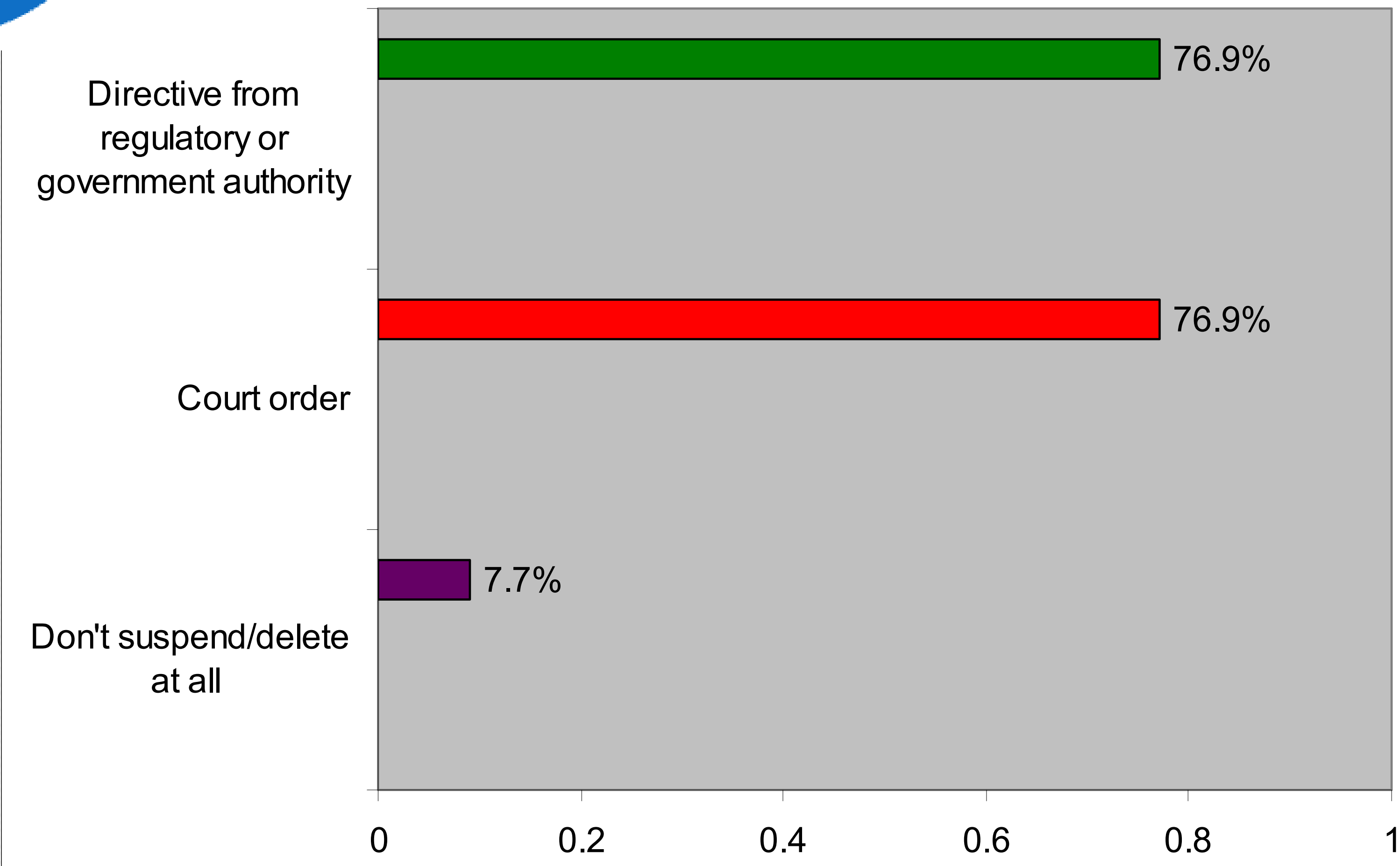
APTLD & MYNIC JOINT SURVEY



APTLD & MYNIC JOINT SURVEY

Q30

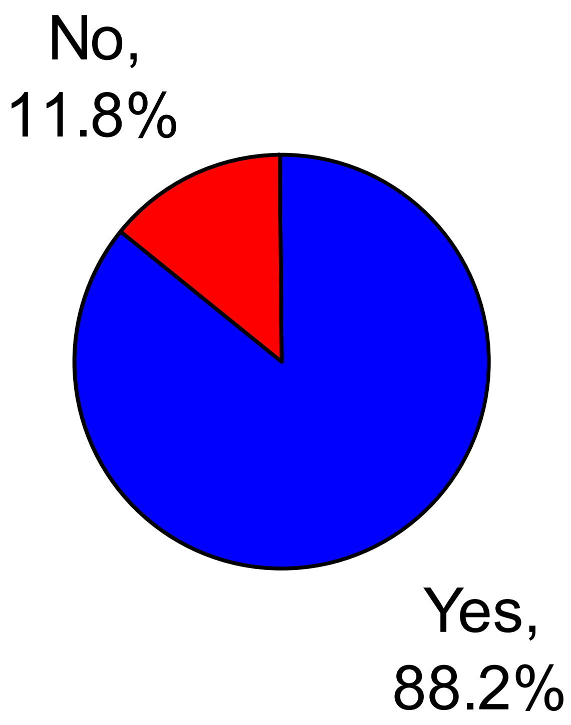
If you don't suspend/delete the domain name, on what basis would your ccTLD suspend or delete a domain name that's subject of a complaint on Phishing activity?



Q31

Do you feel that your ccTLD has a role in reducing phishing activity?

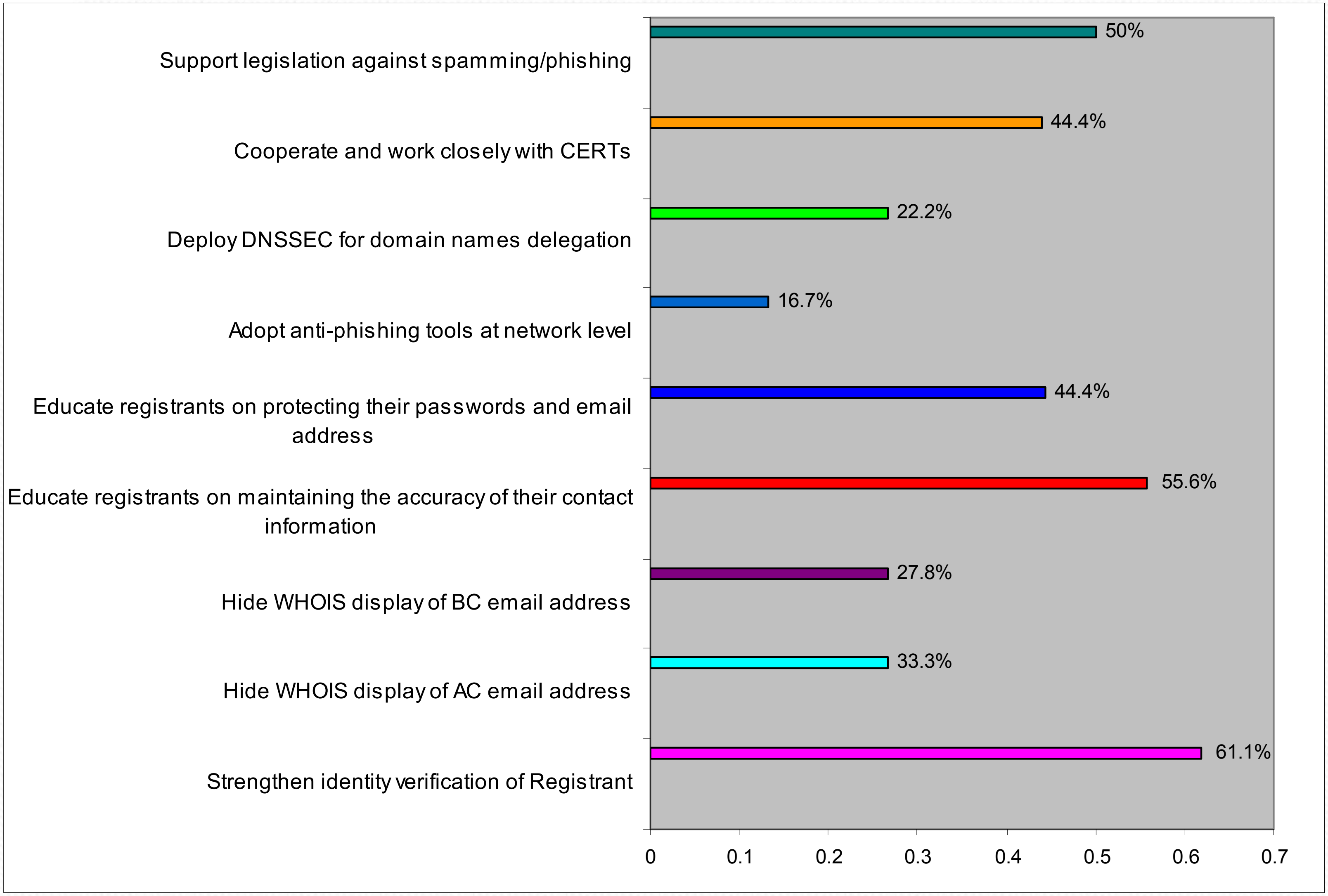
APTLD & MYNIC JOINT SURVEY



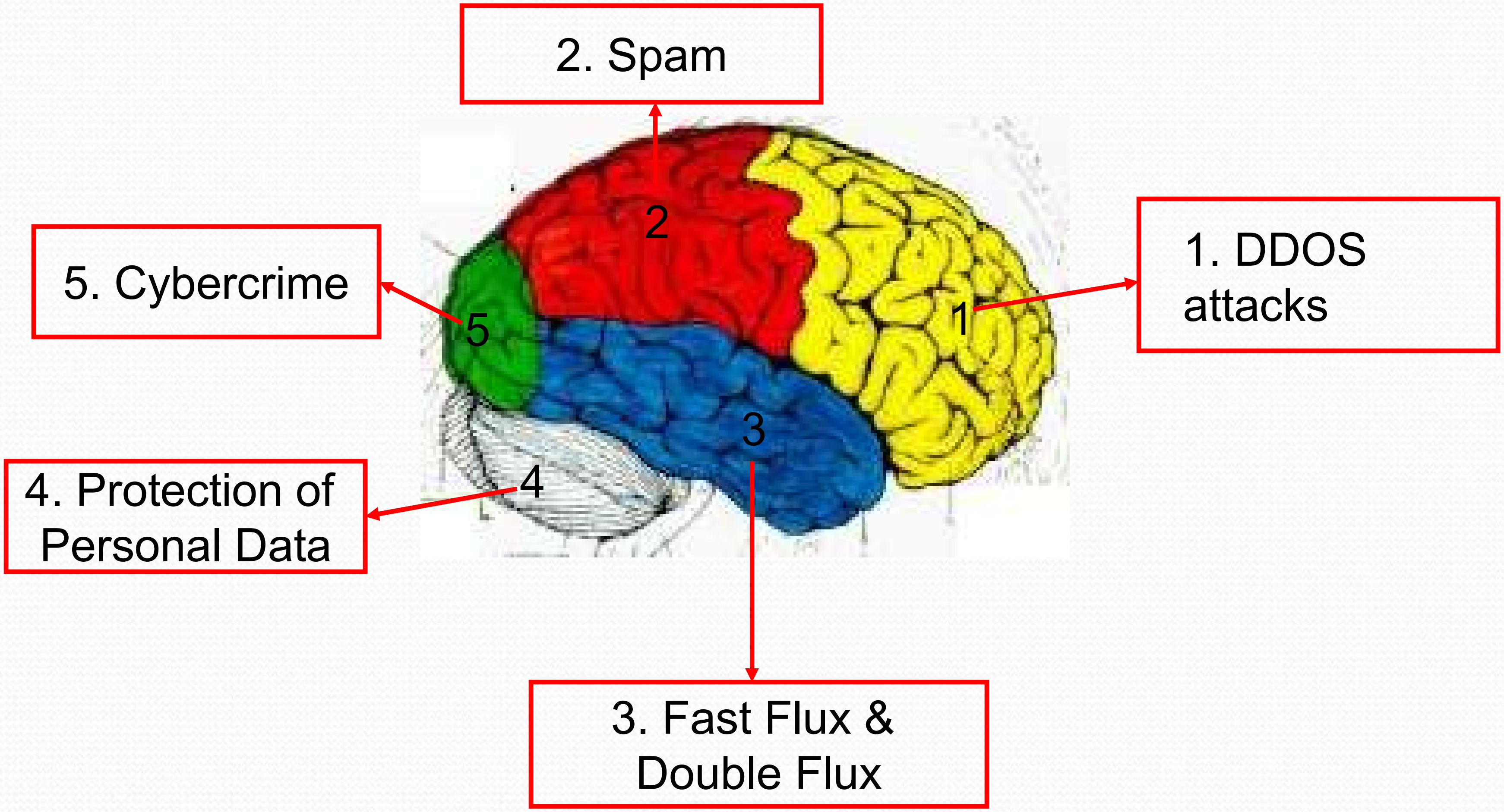
Q32

What can your ccTLD do to reduce phishing activity?

APTLD & MYNIC JOINT SURVEY



Conclusion:
Top 5 critical security issues in ccTLDs mind



2. Spam

5. Cybercrime

1. DDOS attacks

4. Protection of Personal Data

3. Fast Flux & Double Flux

22 RESPONDENTS FROM
19 APTLD MEMBERS
&
ccNSO for
Phishing survey

Presentation by MYNIC
Berhad