children's charities' coalition on internet safety

.uk Policy Process Secretariat
Nominet
Minerva House
Edmund Halley Road
Oxford
OX4 4DQ

4th December, 2012

Dear Nominet,

Re: Consultation on a new .uk domain name service

CHIS applauds the suggestion that the .uk domain should be linked to a series of new, mandatory security measures which will help minimise the risk of infection, hijacking, fraud and other undesirable or improper uses. We especially welcome the notion that you will authenticate all the contact details of any person or entity applying for a new .uk domain name or renewing one.

Law enforcement has repeatedly stated that the ability to register or renew a domain name without the owner's contact details being properly verified allows criminals and scammers of various sorts a degree of freedom to operate which ought to be and could easily be denied them. Under that umbrella of criminals and scammers are persons who engage in activities harmful to children and young people. Hence our interest in this matter.

If we have understood your background paper correctly, the new arrangements for the .uk domain and all of its associated security will only be open to persons or entities with some sort of provable claim to a UK base. In principle we have no problem with that. If someone with absolutely no links to the UK nonetheless wants to utilise a uk domain name it does make you wonder what exactly is going on. At some level or other there is inevitably the potential for a degree of misunderstanding, even misrepresentation. However, from a child protection perspective, we believe what matters most is the identity authentication element. That alone is very likely to act as a brake on impropriety. In that respect, if no other, UK-based or not UK-based for us is not a decisive factor.

The proposal calls into question the validity of the existing arrangements

The very obvious and strongest point we want to make, however, is that the implication of your proposal is quite stark. You are in effect conceding and openly acknowledging that the regime which applies to some or all of the other uk domains – for example .co.uk and .org.uk - is open to the very forms of abuse which the .uk counter measures are designed to prevent.

Thus the existing regime facilitates, or at any rate can do little to prevent, the distribution of malware nor can it hinder other harmful activities which threaten both the integrity of the internet as a whole as well as the interests of many different kinds of individual internet user. In particular the current arrangements also allow for an owner to misrepresent their contact details. That being the case, what possible justification could there be for maintaining the status quo in respect of those domains? Wouldn't it be better, simpler and easier for everyone to understand if every domain ending in uk operated to a guaranteed high minimum standard?

You say on page 9, third paragraph, that you do not intend to change your practice of (not) verifying owners in the other uk domains because this would render them "not suitable for all types of registrants and domain names". We are not sure that that is a good enough reason for refusing to do the right thing. Some of those "types" are crooks and scammers who may well choose your domains precisely because they know they will get an easy passage.

You seem to be labouring under the misapprehension that to do identity authentication would inevitably involve you or the domain name owners in significantly higher costs and delays. We refer to these points again lower down. However, as the several references to the UK Cyber Security Strategy peppered throughout your document remind us, what is at stake here is the integrity of the wider internet, not simply the likes and dislikes or preferences of domain name owners. The public interest should point you in a different direction.

Public perceptions and expectations

We note from your background report, page 9, that over two-thirds (67%) of your survey thought that anyone using the proposed new .uk domain ought to comply with "UK consumer law regarding security and data protection". That number is cited as evidence to support your specific proposal to create the new .uk domain. However, it would be astonishing, would it not, if that same view did not read across to all of the existing domains that already have uk at the end of them?

We can see that you might hope over time that domain name holders in the "old spaces" might choose to migrate to the new domain, particularly if the new domain's virtues and advantages are widely promoted. Yet it is still difficult to avoid the conclusion that Nominet could be setting itself up to run and profit from two entirely separate regimes, operating at two entirely different ethical levels. That cannot be right.

As things stand the new domain could be characterised as “Probably no crooks”. The older ones would be “Probably as many crooks as before.” That position is untenable in a body which is intended to serve the public interest.

The trust mark

On page 7 you speak about creating a “visible trust mark to indicate this enhanced security” (to internet users visiting a new .uk domain).

What would the absence of a trust mark mean in relation to the pre-existing domains? Nothing. At least it would mean nothing if the person coming to it didn’t know that the (superior) “trust mark” existed elsewhere. And then if someone was scammed or cheated on a non-trust marked site, how would you explain your seeming indifference? The fact is once you are seized of the possibility, as you plainly are, that scammers and cheats can abuse any of the other uk domains your duty to all of them is plain. Two tier trust won’t work. Inevitably it would undermine one tier trust in Nominet itself and the whole uk domain.

Our suggestion is that you go ahead with the new .uk domain as set out in your paper and that you announce your intention to bring all of the other domains ending in uk into an improved security regime.

We can see that you might want to maintain the proposed new .uk domain as a premium service in which case it might not be unreasonable to maintain some differentiators between the old and the new. We’re not sure we need to take a view on the detail of that idea. But those differentiators emphatically should not be connected to the authentication of ownership details.

Without a robust identity authentication system working on every domain ending in uk Nominet cannot be sure it will be able to fulfil its obligations to maintain an accurate WHOIS database. The fact that you refuse to publish details of the research you carried out into the accuracy of the uk’s WHOIS entries hardly fills us with an overwhelming sense that all is well in that department.

Confusions about identity authentication

We are not sure on what basis you say

“.....any registrant criteria of UK presence would require significant and costly

monitoring and validation processes.....”

This is simply not true. Everything depends on how high you set the bar.

For the purposes of complying with the UK’s anti-money laundering rules and in order to comply with the terms of the Gambling Act, 2005, very inexpensive, easy to use and fast services have developed to meet the compliance needs of the UK’s online gambling industry. We can see no obvious reason why Nominet would need to insist on standards which noticeably exceed those.

Incidentally, the same verification systems that are used by the UK's online gambling companies are every bit as capable of verifying people who live overseas as they are people who live in the UK. Moreover it can often be just as easy, just as quick and just as cheap to authenticate persons living in many overseas territories as it is to authenticate someone who lives in the UK. However, irrespective of where they live, if an existing or potential new owner cannot be verified online or provide some other reliable authentication of their identity offline then I am afraid they should be told they forfeit the right to own or to continue to own any domain which has a uk ending.

Conclusion

We appreciate that migrating the "old spaces" in the way we have suggested, or improving the security in respect of all of them, cannot be done overnight. The key thing is to declare a reasonable timescale within which the move will be completed.

However, being realistic, because many will see any discussion of this subject as being inextricably bound up with considerations affecting Nominet's future income stream it might be wise to anticipate the need to constitute a project management group with external and independent representation on it. Finally, we were slightly puzzled by the reference on page 4 to the responses to this consultation. The document says you "may" publish the responses. This implies you may not. Is that correct and, if so, why?

Yours sincerely,

Secretary
Children's Charities' Coalition on Internet Safety
10, Great Queen Street
London WC2B 5DD
United Kingdom

ukchis@btinternet.com
www.chis.org.uk