UKOPA

United Kingdom Onshore Pipeline Operators' Association

Website Report January 2003

1   Summary

The open access section of the UKOPA website has been available online since 09/09/02. Upon completion Visual (Sales & Service) Ltd. will submit the site to all major search engines. This section includes a wide range of current information regarding UKOPA membership, activities, Working Groups, Committee membership as well as technical information, including UKOPA position statements and papers. In addition, an email service to UKOPA members is operated via this section. Construction of the secure access section or Member's Centre has been completed, and this section will be activated by 01/02/03. The Management of the UKOPA website is authorised by the Management Council, and is undertaken on their behalf by the UKOPA Secretary Phill Jones. A website maintenance contract covering registration, access, email receipt/delivery, standard updating, members centre access, search engine interface is currently under consideration.

2   Current Status

2.1   Open Access Section

The open access section of the website allows access to i) general available information, ii) details of information/documents approved as available for public issue and iii) approved publications.

Technical management and administration of the above is carried out on an ongoing basis by the UKOPA Secretary with approval from the Management Council, although formal editorial controls has yet to be approved.

A Members' email service is provided through the open access section. Issues relating the availability and use of this service have been experienced and raised.

2.2   Secure Access Section

Construction of the secure access section or Members' centre is complete and access usernames and details have been confirmed by the UKOPA Secretary. On implementation (scheduled for (01/02/03)), current members will receive email notification of their password via their registered contact.

NOTE: passwords will be randomly generated case sensitive alpha-numeric codes.

In the first instance any queries relating to membership registration should be directed to the UKOPA Secretary.

As agreed by UKOPA, the members centre will be managed by the UKOPA Secretary. Initial use will involve providing members with access to downloadable information and documents restricted to UKOPA (i.e. Association meeting notes, Working Group meeting notes, restricted circulation papers etc). Notification of changes to the content of the member's centre will provided by the UKOPA Secretary.

2.3   Software Maintenance

Website software maintenance will be carried out under contract (yet to be awarded) under direction from the UKOPA Secretary.

Maintenance activities include:

- Domain registration
- Provision of secure access
- Updating of content (additions/deletion to open and secure access sections)
- Format revisions
- Maintenance of search engine interface

3   Issues for Discussion

3.1   Unsolicited Email Correspondence

A number of members have reported receiving unwanted and inappropriate email messages (predominantly from 3rd world sources containing fraudulent financial information/invitations for involvement).

This is known as "Spamming" and is the practice of flooding the Internet with many copies of the same message, in an attempt to force that message on to people who would not otherwise choose to receive it. Email spam targets individual users with direct mail messages.

Lists of emails are often created by scanning:
- Usenet postings (when using news groups, joining discussion forums, etc)
- Stealing Internet mailing lists (subscribing to public news letters or public information services)
- Searching the Web for addresses. (This can happen at any time, you are connected to the Web)

Every effort has been made to secure the information held by UKOPA on its members. UKOPA does not disclose any information to third parties and as such is less likely to attract spam using the UKOPA website than many others, particularly those websites which are frequented by the general public.

Members should consider the following points in order to minimise the inconvenience of receiving spam:

i) Removal lists rarely work, they verify to the spammer that an e-mail address is good and get put onto a premium CD which can in turn be sold for even more money. It's best not to respond in any way to an unwanted e-mail.
ii) Local unwanted email filtering (see attached details)
   Use your message filter in your email application
   Outlook Express -> Tools -> Message Rules -> Blocked Senders List
   MS Outlook -> Actions -> Junk E-Mail -> Add to Junk Senders List

For more on preventing spam see Appendix A. below.

3.2 Editorial Control

The website now provides a recognised route for fast and efficient publication of material. Formalisation of transparent and effective control and authorisation of the content and format of information and documents published on the website is required.

4 Opportunities for Website Development

The following have been identified as possible opportunities for development:

- Database Access
  Existing database – the pipeline fault database could be made available for simple queries.
  New databases – eg collation of data on 3rd party infringements.

- Notice Board Service – eg information notices and consultation responses.

5 Costs

The quoted charge for the software maintenance contract is £1975.00 per annum. Award of a contract for 2003/2004 to Visual (Sales and Service Ltd) is to be considered by the Management Council on 15/01/03.

<u>Appendix A</u>

Once an email address is on a spammer's list, it can be very hard to get off, especially if he's selling it. Here are some tips on how to stop spam before it starts.

Reduce your exposure to "harvesting"
Don't display your email address(es) in public more than necessary, at least not in a form that's easy prey for scavenger bots (programs that spammers run to "harvest" email addresses).

If you post to Usenet or chat, consider disguising your address. There are dozens of ways of doing this so that humans who really want to contact you can figure out how to do so: look at a few postings and choose one you like. We have heard reports that some harvesters are already wise to addresses such as me@nospam.myisp.com so try a variation on the nospam. There are plenty of adjectives that could be added. Of course almost any method can be thwarted by sufficiently intelligent scavenger bots, but most of them aren't very smart.

Your choice of email address can affect the amount of spam you get. A common user name such as jsmith will typically get more spam than a weird unique name such as jsm93x98, particularly at a large ISPs, due to a technique called dictionary spamming. Choosing an email address that begins with a letter late in the alphabet also gets less spam, because many lists are sold sorted in alphabetical order, and spamming sessions are often terminated before they complete.

Check your browsing isn't giving you away
In a very small number of cases, your email address may be discovered by a web site you visit. This has occurred through bugs in places such as Web-based email services. Early versions of some browsers gave away email addresses routinely.

Reporting spammers to ISPs and email providers
A free service that does the sleuthing and complaining for you is http://spamcop.net/.
If the spam asks invites responses to an address at one of the major online providers or at a "disposable" address such as the free accounts provided by http://www.hotmail.com/ or http://www.juno.com/, your course is clear: simply forward the spam to the postmaster at the company named. All these companies have strict policies against spam and should terminate the account promptly, if it is really being used by a spammer. If not, they may decide to track down and cut off or sue the spammer.

Reporting spammers to law enforcement agencies in the US
There are various law enforcement agencies where you can report spam.
1. If the spam involves fraudulent or deception practices, you can forward it to uce@ftc.gov for the US Federal Trade Commission to add to their database.
2. If a Nigerian says they have millions of dollars waiting for you to collect, forward the email with the subject "419 sample - no financial loss" to 419.fcd@usss.treas.gov for the US Secret Service to investigate. Nigerian Advance Fee Fraud (also called 419 Fraud) has been going on since the 80's with faxes, and has recently become common with email.

Finally - What about removal services?
Be cautious about sites where you can register to have your email address removed from spammer's lists.
Some are ineffective; some actually *add* your address to other spammers' lists.
Some services say they will not give addresses to spammers: they have to submit their lists for "cleansing."

Anyone can start a removal service site; the difficult part is getting spammers to pay any notice. Due to the strange economics of the Internet, it's easier for spammers to spam everyone. They already know that almost nobody wants to hear from them, so why should they go to the trouble of removing those names?

The only motivation we can think of is the fear of being sued. Some large online providers do sue spammers to protect their customers, and the US Federal Trade Commission has said that they will go after spammers who use fraudulent tactics such as fake removal addresses. But what can the average person do to stop a persistent spammer? Not a lot!

    (Ref : Scott Hazen Mueller, Contact:- http://spam.abuse.net/)