

Re: VMPC isn't free

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-08/2132.html>

From: Mok-Kong Shen (mok-kong.shen_at_t-online.de)

Date: 08/27/03

Date: Wed, 27 Aug 2003 16:00:23 +0200

Tom St Denis wrote:

>

- > *I've thrown in my share of research topics with mixed results. For*
- > *instance, I did get some nice replies to my study of the branch*
- > *properties of FFT-like networks [for instance].*
- >
- > *The problem is when people like Barzotak [or whatever] discover "new and*
- > *great" ciphers they waste weeks of time where legitimate questions*
- > *almost always get ignored. In the end their contributions are zero*
- > *since they brought nothing to the table.*

There are clever and less clever or stupid people, good and bad researchers. Maybe you are lucky to belong to the genius class, but still one has to have certain tolerance towards the less gifted ones. Note also that everyone starts as a beginner who can't yet do things that a profi could do.

- > *Problem is Moz [for whatever reason] doesn't have a Killfille. It has*
- > *filters which don't really work that well. So unless I move to another*
- > *reader [which isn't an entirely bad idea] all there stupid posts come*
- > *through loud and clear.*

I use Netscape and it's trivial to kill mails/posts according to various criteria. (I even kill mails from one country.) The only problem is that the spammers employ ever different new sender address etc. Maybe you have to find out whether it isn't worthwhile for you to switch to Netscape or another browser. Even if you couldn't change that, one simple way is to never click on posts bearing the names of those who, from your past experience, only write stuff that you dislike. (In my mailbox, I click on only about 5% of what comes in.)

- > *The problem is he [like the others] don't take the science seriously.*
- > *They trivialize everything and insult the regulars. This is what drives*

- > *the real pros away. Even if Barzatsols didn't "insult people" his*
- > *constant barrage of mootness is enough to drive the S/N ratio straight*
- > *to zero.*
- >
- > *Believe it or not but there are actually real people who study crypto*
- > *for a living. Having their work trivialized at every step is just*
- > *insulting and they'd rather do without. This is where us amateurs lose out.*

I am not sure that you could correctly decide whether others are taking the science seriously in many cases. (Yes, there are on the other hand politicians who think to be able to always correctly decide who have the right or wrong 'thought'.) First class researchers don't spend much of their time in our group in my view. That's bad, but I don't think you, as individual, could ever change that. On the other hand, I am personally of the opinion that this group should provide the opportunity to amateurs and beginners to express their (eventually very wrong) ideas so that they could have a certain chance to mature to become profis oneday. If you are a profi and have the goodwill to help others, you should have a certain amount of patience and tolerance to the amateurs and beginners in my opinion. (Note, though, that you are never 'required' to help others or even to follow-up at all.)

- >
- > *For example, I've been recently having a conversation with Alice*
- > *Silverberg about tori-based crypto. The conversation brought out*
- > *several interesting facts that most newbies probably wouldn't realize*
- > *[and I'm still asking a few questions yet].*
- >
- > *I'm rather certain there are other newbies in this group would like to*
- > *learn what the XTR and CEILIDH algorithms are and how they work. [for*
- > *example].*
- >
- > *Of course unless one of the few regular pros posts about it you'll never*
- > *learn about it. And why won't you? Because the other pros don't*
- > *discuss matters in this group. And why don't they? The prevalent*
- > *reason [from what I gathered by actually talking to them] is that*
- > *"sci.crypt is a huge waste of effort".*

As said previously, you couldn't hope to 'improve' the world in any big sense. It is a fact in this (and of course other) group that, if one expresses negative opinions on others' posts, there will often be a long sequence of very inutile discussions, unless one expresses one's opinions in very objective/precise/pertinent/logical ways such that there isn't anything left that the partner could counter. So, I would say that one should in general refrain from giving more or less vague negative opinions, just for the purpose of reducing bandwidth and (indirectly)

not further worsening the image of the group in the eyes of the profis (who we desire to attract to our group).

- > *So you're damn right I'm pissed off at the troll-of-the-week when they*
- > *post their useless design of the week. People have to ignore them*
- > *completely and eventually they'll just leave.*

For the general people, I like to re-iterate my hint of the possibility of employing kill-file and (in case a suitable browser is not available for that) of refraining from clicking on posts of certain selected persons.

M. K. Shen