

Re: Spamnet add-in to Outlook

Source:

http://www.tech-archive.net/Archive/Outlook/microsoft.public.outlook.program_addins/2004-10/0199.html

From: Sue Mosher [MVP-Outlook] (suemvp_at_outlookcode.com)

Date: 10/29/04

Date: Fri, 29 Oct 2004 09:37:32 -0400

If you're modifying the security settings item (you should never be modifying the template itself), open the item, and then choose Edit | Revise Contents. If you make a change to the members of the item, be sure to make some other change in the item – perhaps toggling a setting on and off. Otherwise, Outlook may not save the change to the member list. To save the changes to the item, choose File | Post. Any other method of modifying the item may cause problems.

As for the password issue, if you are running Outlook with a profile that points to a mailbox other than the mailbox for the Windows account that you are logged in under, you will be prompted for your network credentials the first time you create a security settings item during a given Outlook session, you will be prompted for your network credentials. Use the credentials for the mailbox whose Outlook profile you are using.

--

Sue Mosher, Outlook MVP

Author of

Microsoft Outlook Programming - Jumpstart for
Administrators, Power Users, and Developers

<http://www.outlookcode.com/jumpstart.aspx>

"tdog" <tdog@discussions.microsoft.com> wrote in message
news:2E64F170-9CB7-4FA0-81B9-5ADBC65C3E92@microsoft.com...

> Sue,

>

> Thanks. I agree that setting up the Outlook Security Template and not
> utilizing the default security may cause SpamNet to trigger the pop-ups.

>

> The spamnet.dll file is the correct add-in to trust (I've been working
> with

> Cloudmark on the issue); however, the Template itself seems to
> periodically

> fail and must be re-created (it gives an error about permissions/passwords
> sometimes when we modify the template, and this appears to destroy its
> functionality). I think it's odd that when changes are made, we are never
> prompted for a password as the MS documentation suggests we should be. Do
> you

> know why that may be?

>

> I agree also that the PDFMOutlook.dll file does not seem to be coded to
> take

> advantage of the built-in Outlook 2003 trusts.

microsoft.public.outlook.program_addins: Re: Spamnet add-in to Outlook

>
> The best scenario, then, is probably to use NO Security Template but allow
> the default security model to rule to alleviate the SpamNet pop-ups, and
> then
> disable the PDFMOutlook.dll add-in from loading with Outlook (in the
> Registry). I'm still curious about why the Security Template is behaving
> in
> the manner it does - any ideas or suggestions on that would be greatly
> appreciated.
>
> As always, thanks so much for your help, Sue.
>
> cheers /td
>
> "Sue Mosher [MVP-Outlook]" wrote:
>
>> Anything is possible, but given that SpamNet works fine without prompts
>> under the default trust mechanism built into Outlook 2003, their code
>> doesn't seem to be the problem.
>>
>> Are you sure you trusted the correct .dll? If I were you, I'd be
>> discussing
>> this issue with CloudMark.
>>
>> My guess about PDFMOutlook.dll is that it is not properly constructed to
>> take advantage of the trust mechanism.
>>
>> "tdog" <tdog@discussions.microsoft.com> wrote in message
>> news:B143F1E1-BA65-4ABD-B794-62DF2DE8EF98@microsoft.com...
>> > Sue,
>> > Thanks for the response. The Outlook Security Settings folder is in the
>> > Public folder structure in Exchange, the affected clients have the
>> > proper
>> > CheckAdminSettings value in the Registry (it was also set up to address
>> > the
>> > PDFMOutlook.dll issue which produces similar pop-ups, and it does fix
>> > that
>> > issue if you have certain Programmatic Settings approved - trusting the
>> > DLL
>> > in Trusted Code does nothing), yet we still have many users getting the
>> > security model pop-ups in OL2003 when SpamNet 3.0 is installed.
>> >
>> > I have read in several places that OL2003 allegedly trusts COM add-ins;
>> > however, we are not the only users experiencing the problem (and we
>> > don't
>> > have ActiveSync installed, which according to Cloudmark can cause the
>> > SpamNet
>> > add-in to trigger the pop-ups).
>> >
>> > Could there be an issue with the SpamNet DLL coding such that Outlook
>> > does
>> > not recognize it (and thus not trust it) correctly?
>> >
>> > Thanks.
>> >
>> > "Sue Mosher [MVP-Outlook]" wrote:
>> >
>> >> Sounds like the trust mechanism isn't working, either because the
>> >> folder
>> >> is
>> >> in the wrong place, the required client registry entry isn't set, etc.
>> >> In

microsoft.public.outlook.program_addins: Re: Spamnet add-in to Outlook

```
>> >> any case, Outlook 2003 trusts COM add-ins by default. In other words,
>> >> if
>> >> SpamNet is the only reason you fired up that folder, you don't need
>> >> it.
>>
>> >>
>> >> "tdog" <tdog@discussions.microsoft.com> wrote in message
>> >> news:545F4D6C-1D5C-4252-AF42-A5BFBB04EFD1@microsoft.com...
>> >> > Hello,
>> >> >
>> >> > I and other enterprise users are running Outlook 2003 with SpamNet
>> >> > 3.0
>> >> > and
>> >> > we get the "A program is trying to access e-mail addresses..."
>> >> > pop-up.
>> >> > This
>> >> > occurs even though we have trusted spamnet.dll in our Outlook
>> >> > Security
>> >> > Template per the reference in the Cloudmark Knowledge Base which
>> >> > points
>> >> > to
>> >> > the Microsoft ORK article. ActiveSync is not installed on my system
>> >> > and
>> >> > never
>> >> > has been (brand-new system).
>> >> >
>> >> > Has anyone else had any luck getting the trust to work for the
>> >> > SpamNet
>> >> > plug-in? Thanks!
>> >> >
>> >> > cheers /td
>> >>
>> >>
>> >>
>>
>>
```