

dan1

From - Tue Nov 04 09:43:02 1997
>From deckd Tue Nov 4 09:33:03 1997
Received: (from root@localhost)
by orion.sk.sympatico.ca (8.8.6/8.8.6) id
JAA03467;
Tue, 4 Nov 1997 09:33:01 -0600 (CST)
From: Sympatico Admin <deckd>
Message-Id:
<199711041533.JAA03467@orion.sk.sympatico.ca>
Subject: Forging your return address.
To: carljohn@sk.sympatico.ca
Date: Tue, 04 Nov 1997 9:33:01 CST
X-Mailer: Elm [revision: 212.4]
X-UIDL: 65b46dc2d72f7c813951638c648fb5f5
X-Mozilla-Status: 0005
Content-Length: 814

Hi Larry,

We have determined that you have be trying set your email program to be anonymous;ie forging your return address. If you wish to be anonymous then get a free email account with hotmail.com or rocketmail.

Your forged reply-to addresses 'fred@dev.null' get rejected by our email system and sit in our mail queue. Also please do not set your email program to relay through someone else's server in another domain as there have been complaints. We do not allow this to be done from anyone outside our domain.

Please note: this note is being sent to our security dept. as we deem this type of activity to be mis-use of the mail system and as such you could loose your access privileges.

If you have any question or concerns then please reply to this note!

Thanks
Dan Deck
Sys Admin

Page 1

dan2

From - Tue Nov 04 17:37:54 1997
Received: from phantom.sasknet.sk.ca
(deckd@phantom.sasknet.sk.ca [142.165.5.14])
by orion.sk.sympatico.ca (8.8.6/8.8.6) with
ESMTP id QAA13046
for <toto@sk.sympatico.ca>; Tue, 4 Nov 1997
16:34:16 -0600 (CST)
Received: (from deckd@localhost)
by phantom.sasknet.sk.ca (8.8.6/8.8.6) id
QAA16514;
Tue, 4 Nov 1997 16:44:07 -0600 (CST)
Date: Tue, 4 Nov 1997 16:44:07 -0600 (CST)
From: Dan Deck <deckd@phantom.sasknet.sk.ca>
Message-Id:
<199711042244.QAA16514@phantom.sasknet.sk.ca>
To: toto@sk.sympatico.ca
Subject: Re: Forging your return address.
Mime-Version: 1.0
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: quoted-printable
Content-MD5: 1fjG1EMLpr+IR6osktMk7Q==
X-UIDL: fb39bccff7c329489ed0df904aa33a27
X-Mozilla-Status: 0011
Content-Length: 4725

> From toto@sk.sympatico.ca Tue Nov 4 11:22:23 CST 1997
> Date: Tue, 04 Nov 1997 11:10:59 -0600
> From: Toto <toto@sk.sympatico.ca>
> Reply-To: toto@sk.sympatico.ca
> Organization: "When anonymity is outlawed, only
outlaw children will =
be able=20
to protect themselves from sexual predators on the
InterNet."
> X-Mailer: Mozilla 3.01C-SYMPA (Win95; U)
> To: Sympatico Admin <deckd@harrier.sasknet.sk.ca>
> CC: cypherpunks@toad.com, toto@sk.sympatico.ca
> Subject: Re: Forging your return address.
> References:
<199711041533.JAA03467@orion.sk.sympatico.ca>
> Status: RO
>=20
> Sympatico Admin wrote:
> > Hi Larry,
> >=20
> > We have determined that you have be trying set your
email program to
> > be anonymous; ie forging your return address. If you

Page 1

dan2

wish to be
> > anonymous then get a free email account with
hotmail.com or =
rocketmail.
>=20
> Dan,
>=20
> The Sympatico Netscape software you provide has
features that allow
> the user to choose not to give out their email address
to those that
> they wish to keep it from, such as spammers, criminals
and sex-shop
> operators.
> I have not been made aware of any Sympatico policy
which requires your
> users to make themselves vulnerable to anyone and
everyone who has
> connections to the InterNet.
Under normal conditions and because of the large amount
of spamming that
goes on it is not unacceptable to forge your userid as i
include in my
reply-to address deckd#\$\$@sk.sympatico.ca and this
defeats most auto
harvesters. But I don't hide it completely.
Your attempts to forge your domain shows that yes you
are an experienced
user and it does hide your identity, but it shows up on
other mail =
servers
as suspicious activity.
>=20
> > Your forged reply-to addresses 'fred@dev.null' get
rejected by our
> > email system and sit in our mail queue.
>=20
> My chosen reply-to addresses at 'dev.null' are a
traditional UNIX
> method of directing files and email to /dev/null,
which is the
> equivalent of the Trash Bin on a Mac. You seem to have
set up your
> UNIX system to emulate a Win95 Recycle Bin, in that it
assumes that=20
> the user doesn't know what he or she is doing, so
saves deleted items.
> Dev.null addresses are designed to get rejected by the

Page 2

dan2

email system,

> so it seems rather useless to keep them in your mail queue.

Because sendmail requires a valid return address and valid domains the and yours are not they are kept in the mail queue till the timeout =

period

of one day then they are deleted.

And yes I know of /dev/null but because the system has now been setup to

stop spammers from using our mail server for relaying, these messages do =

show

up in the queue.

>=20

> > Also please do not set your

> > email program to relay through someone else's server in another =

domain as

> > there have been complaints. We do not allow this to be done from =

anyone

> > outside our domain.

>=20

> You will have to explain to me what exactly you are talking about

> here, as it is unclear to me what you are referring to.

> Please forward me copies of the complaints.

What this refers to is you setting your outgoing or smtp server entry to

any server which will accept outgoing mail. And it was brought to our=20

attention by a mail admin at another location, as he saw the rejected

messages in his maillog as well.

> =20

> > Please note: this note is being sent to our security dept. as we =

deem this=20

type

> > of activity to be mis-use of the mail system and as such you could =

loose

> > your access privileges.

>=20

> Since this seems to be of such serious concern to you,

Page 3

dan2

I would =
certainly
> appreciate it if you could explain to me in greater
detail exactly =
what
> it is about my use of my account that Sympatico has a
policy problem
> with, and why.
At this point it is the forged domain name and user name
that is the =
problem as=20
it=20
makes it harder for other system admins to figure out
who is causing
them problems. Also the messages are sitting in the mail
queue and being
retried for a day which uses up system cycles. And it
causes us to have =
to spend=20
time trying to figure who is doing this and why.
We have in the communications tariff a statement to the
effect that if
any of your actions adversely affect our systems we have
the right to =
suspend
or remove your access from our system. This isn't the
exact wording but
covers this situation.

> =20
> > If you have any question or concerns then please
reply to this note!
>=20
> I notice that your reply to address, 'Sympatico Admin
<deckd>', is not
> a valid InterNet email address. Is this an internal
system address?
Yes
> =20
> Toto
>=20
>=20
Dan