

Re: Phishing mails on the increase? [OT]

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.misc/2005-11/1332.html>

From: Michael Heiming (*michael+USENET_at_www.heiming.de*)

Date: 11/13/05

Date: Sun, 13 Nov 2005 22:31:59 +0100

In comp.os.linux.misc Moe Trin <ibuprofin@painkiller.example.tld>:

> *In the Usenet newsgroup comp.os.linux.misc, in article*

> <4ofj43-tb7.ln1@news.heiming.de>, Michael Heiming wrote:

>> *Wasn't aware getting one at all, so checked my spam filer which
>> is cleared nightly from cron. And really a bunch of those
>> pretending to come from one or another bank have been received,
>> but luckily automatically sorted out from SA. (Bayes catches the
>> crap reliable)*

> *One of the ISPs I use allows me to have multiple mail accounts. I mainly
> use it for mail – and all of the accounts have nonsensical usernames
> generated by piping /dev/random through uuencode and taking the last
> 15 characters of the first line of output. This makes 'dictionary' or
> 'phonebook' name harvesting a thing of the past. These accounts are
> only used for contact with financial institutions, and I don't use
> other accounts for that purpose. Thus, any mail from a plisher sticks
> out like a mountain and is auto-deleted at the POP server. At most, I
> see the headers, and that only when I enable logging.*

Only have a very few mail addresses, mostly use the one supplied here (a little munged), iirc I'm using this mail address since a decade or more. Likely because it's easy to remember. Spam wasn't a problem as I begun to explore usenet with it, so it wasn't munged and is certainly contained on any spammer DVD starting kit.

At one point disabled a default catch all account for my domain, which was a nice thing, but spammer started hammering me with thousands of messages daily and it began to be mentionable even with ADSL.

In the last 10 month not a single spam mail was able to pass SA, which defeated about 50000 x spam during this time, with not a single false positive I'm aware of.

[..]

comp.os.linux.misc: Re: Phishing mails on the increase? [OT]

>> *Without looking at the header it's more than obvious after
>> reading the first sentence that those aren't genuine.*

> *It doesn't even get that far here – typically, if it's not rejected
> by the SMTP server using basic blocklists, it's rejected based on
> the From: or Subject: headers. Despite what the phishers may think,*

It doesn't get beyond SA here, had to check a cron zeroed spam file to mention them. There was some rather stupid article about the matter, which made me curious and yep there are about 5 of them from the last 22h.

> *not all of us have CitiBank or PayPal accounts in the mail names that
> they found on those Millions CDs.*

>> *What are your experience about the matter?*

> *The single bank that I do use for Internet transactions and mail has sent
> out snail-mail on average quarterly, reminding me that any mail from them
> will include certain keys – one of which is personalized – to identify
> it as being from them. They also don't ask to "verify" any account
> details over the Internet, _AND_ state that if they do send an email
> indicating a problem with an account, it will have me contact them in
> return using their published toll free telephone number. That is why
> I chose that bank.*

My bank gives a hint on the entrance URL to online banking, they'd never ever send a mail asking for passwords/etc and provides a free call number for questions. Their mails are signed in addition.

The real stupidity beyond the matter, why on earth should they ask me for my password on their server?

--

Michael Heiming (X-PGP-Sig > GPG-Key ID: EDD27B94)
mail: echo zvpunry@urvzvat.qr | perl -pe 'y/a-z/n-za-m/'
#bofh excuse 176: vapors from evaporating sticky-note adhesives