

Re: [Full-Disclosure] Email marketing company gives out questionable security advice

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-07/0066.html>

From: Nick FitzGerald (nick_at_virus-l.demon.co.uk)

Date: 07/03/03

To: full-disclosure@lists.netsys.com

Date: Thu, 03 Jul 2003 14:37:49 +1200

"Richard M. Smith" <rms@computerbytesman.com> wrote:

> *Last week, I received an unsolicited email message from Mobil Travel
> Guide about their new online service. In the message, I was encouraged
> to turn back on ActiveX and scripting in Outlook in order to view a
> Flash movie embedded in the message. Needless to say, I thought this
> was a terrible idea. ...*

Indeed...

> *... Instead, I wrote the company who created the ad,
> Digital Produce (<http://www.digitalproduce.com>), saying they were giving
> out bad security advice and they should stop doing this sort of thing
> in future mailings.
>
> I got a reply from the company this week basically saying that they
> agree with my concern, but not my solution. Instead they decided to put
> a little security warning on their "real media fix" page. This fixer
> page can be found here on their Web site:
>
> http://www.digitalproduce.com/site_resources/pdfs/outlookfix/
>
> I think the warning message is pretty lame and misleading. Microsoft
> released the Outlook Security Update a few years back because anti-virus
> software wasn't stopping email worms. Turning back on ActiveX and
> scripting only encourages the virus writers.*

Yep.

The "correct" solution to this "problem" --- if you accept the general notions that IE is a reasonable choice of web browser and that it's security zone mechanism provides adequate protection --- is that the active content should be indirectly linked. That is, the message should link to a web page containing the active material. Then, if the message's recipient chooses to brose the page and thus take the

attendant (although generally entirely obscured) security risks, they can. This greatly reduces the exposure surface, assuming that a small proportion of message recipients actually click through the link (and should greatly reduce the mail sender's network bandwidth usage). It also greatly reduces the "active mail" peddlers' need to become "security advisors" — a role they clearly are very ill-prepared to accept and when they do whose "advice" is likely to be of dubious value if mass-mailing active-content advertisements is the modus operandi. Even if all recipients of their messages click through, only a small-ish proportion will have been sufficiently wary to have customized their "Internet" security zone to prevent such active content "playing", and most of those who have will probably be quite able to make the determination whether the site hosting the material is "trustworthy enough" to add the site to their "Trusted Sites" security zone so the content can be played.

Of course, the huge proliferation of active-content Email and the continuing promotion of "active-content Email focussed" products (such as IncrediMail and others) means that there is a large userbase with an expectation that such mail should be available.

Unfortunately, this expectation is usually layered atop a general, but unstated, assumption that "of course it's safe — they would not [or even _could not_] have made it available previously if it were not". Thus, the age old problem of removing some functionality from a product because it turned out to be a complete security disaster (or for whatever other reason) at the risk of alienating a large chunk of your userbase arises.

I think it was brave of Microsoft to have changed the default security zone settings of IE, OE and Outlook from their initial dire settings and I do give MS credit for that. However, I also wish they had gone further and simply removed the ability to re-enable the "please shoot me in the foot" options from the products. This would have sent a much stronger, and greatly needed, message to the userbase and to those whose business model is essentially based on an assumption of corruption of human decency.

> *(As an aside, the Xbox division of Microsoft is also a customer of Digital Produce. I wonder if any Xbox ads gave out this same bad security advice?)*

Presumably, at least if those ads were relatively recent, for as you say, the recent-ish changes in security settings in MS's dominant Email clients must be starting to bite the "Digital Produce"s of the world.

> *OTOH, it's not too hard too understand where Digital Produce is coming from. According to a recent article in Internet News, only about 30% of email users can view rich media email. ...*
<<snip>>

Full-Disclosure: Re: [Full-Disclosure] Email marketing company gives out questionable security advice

Is that article available online? Could you post a URL to it?

- > *Along these same lines, images in HTML email messages will be the next*
- > *thing to go. The upcoming versions of Outlook and the AOL 9.0 email*
- > *reader will no longer show images in HTML email messages by default.*

Cool.

Another sign that someone at MS is concerned its products should catch up with the feature sets of the truly security aware web browsers and Email clients...

<<snip>>

- > *It will be interesting to see how email marketing companies and*
- > *spammers adapt to these technical changes in HTML email.*

Well, based on past trends (and assuming that usage of something like IncredIMail doesn't explode to "fill the gap") they have several years of "installed base" that seems highly resistant to upgrading, or even installing any post-Gold security hotfixes or service packs, to feed off. This means that IE 5.x Gold and associated OE users will keep them in business for at least another three or four years...

Regards,

Nick FitzGerald

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>