

Re: How safe is a "Limited" XP account?

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-02/24309.html>

From: Todd H. (*comphelp_at_toddh.net*)

Date: 02/23/05

Date: 23 Feb 2005 16:42:00 -0600

jbrock@panix.com (John Brock) writes:

- > *What bad things can happen to me while using a plain vanilla*
- > *"Limited" Windows XP user account?*

Everything including execution of "arbitrary code."

- > *In the most extreme case,*
- > *suppose I am totally reckless, and I visit every questionable web*
- > *site I can find, and click on every questionable attachment that*
- > *comes my way. In theory it would still seem that nothing really*
- > *bad can happen, other than having files owned by that account spied*
- > *on and/or altered. In fact it seems reasonable to expect that any*
- > *malware I ran into would -- on finding itself in an unexpected*
- > *non-Administrator environment -- simply fail, so even that sort of*
- > *compromise wouldn't be too likely. But I am just speculating, and*
- > *I'd rather know the facts. So what are the risks?*

Search the web for Windows security advisories that include the words "local privilege escalation." These indicate "okay i have a local (restricted) user account, and this hole gives me administrator priv's."

- > *One thing I have heard is that IE, being fused to the kernel, always*
- > *runs with full privileges, and is thus always a security risk, even*
- > *in a Limited account. However I always use Mozilla, which I would*
- > *think would take care of that problem. Or does it? Is there maybe*
- > *some way a malicious web page could get to IE through Mozilla?*

IE is comparatively far more dangerous.

Unpatched Mozilla can still be a big problem though too. You have to keep up on all fronts. Mozilla was also vulnerable to the malformed graphic buffer overflow, but its security track record remains far far better than IE.

- > *And what about Outlook? Does it have the same problem as IE?*

microsoft.public.windowsxp.general: Re: How safe is a "Limited" XP account?

It does too many things by default, yes. There are options that need to be disabled there. Try Mozilla Thunderbird for a little more insulation, or investigate all the default options you need to modify to use Outlook relatively safely.

> *issues. In general I am interested in both likely and worst case*
> *scenarios. Any thoughts?*

There are more secure OS's out there.

What are your goals? What need motivates your questions?

Best Regards,

--

Todd H.

<http://www.toddh.net/>