

Re: Draft I: Why You Don't Want to Install Software

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-11/6679.html>

From: Kevin Weilbacher [SBS-MVP] (kweilbacMVP_at_gte.net)

Date: 11/27/04

Date: Sat, 27 Nov 2004 06:17:22 -0500

Tears of joy?
Tears of wishful thinking?
Tears from too many Mountain Dews?

```
--
Kevin Weilbacher [SBS-MVP]
"The days pass by so quickly now, the nights are seldom long"
"Susan Bradley, CPA aka Ebitz SBS Rocks [MVP] " <sbradcpa@pacbell.net> wrote
in message news:OLSy0gE1EHA.2788@TK2MSFTNGP15.phx.gbl...
> sniff sniff ...wiping a tear from my eye :-)
>
> Andrew M. Saucchi, Jr. wrote:
>>         I've prepared the first draft of a document I hope to convince
>> my
>> boss to distribute to our clients in hopes of drastically reducing the
>> number of local administrators we have lurking around our networks. I
>> figured others might benefit from this, so I'm posting it here. Anyone
>> who
>> cares to contribute is more than welcome to do so. It may well need to be
>> fleshed out a bit, but I'm hoping that by the time I'm finished, my SBS
>> clients in particular will come to me and plead, "Please don't let me
>> install software-- you do it."
>>
>>         "Why You Don't Want to Install Software"
>>
>>         Many of you may believe that installing software is part of having a
>> computer, much like placing bread into a toaster is part of owning a
>> toaster, or filling the gasoline tank is part of owning an automobile.
>> The
>> idea of contacting your network consultant to install software probably
>> sounds as necessary as having a pet consultant to put food in your pet's
>> bowl. In this document we will endeavor to demonstrate why software
>> installation must be left to professionals.
>>
>>         In earlier versions of Windows-- namely, those descended from DOS,
>> the
>> 3.x/9x/ME line-- there was only one type of user, the "super user." Any
>> user
>> could install software. Any user could access any file on the hard drive.
>> Any user could modify or delete any file on the hard drive. Any user
>> could
>> trash the entire operating system, just by deleting or modifying one
>> file.
>> And trash they did. Windows 9x was notoriously unstable and fragile.
>> Installing one program could cause other programs to stop working.
```

microsoft.public.windows.server.sbs: Re: Draft I: Why You Don't Want to Install Software

>> Moreover,
>> this was long before adware, spyware, malware, e-mail scams, and
>> Internet!
>>
>> Microsoft knew that this model would be woefully inadequate for an
>> operating system on which businesses would depend to conduct their
>> affairs.
>> If a home user trashed his computer, he could curse a bit, reformat,
>> reinstall, and get over it. Businesses would not tolerate that sort of
>> instability. They would need some security. The idea of an operating
>> system
>> that allowed anyone to do anything-- like an ATM that consisted of
>> nothing
>> more than a stack of \$100 bills in an open drawer on a street corner with
>> a
>> pencil and a sheet of paper for people to record what they had
>> withdrawn--
>> simply would not suffice.
>>
>> Enter Windows NT. This was Microsoft's operating system for
>> businesses.
>> It was redesigned from the bottom to the top, and one improvement that
>> was
>> built-in security. Users fell into one of two main groups--
>> administrators
>> and users. Administrators would install programs, while users would run
>> them. Programs would be installed into a "Program Files" folder, and this
>> folder as well as the Windows system folders were off-limits to users.
>> Key
>> parts of the system registry were also off-limits. That would prevent
>> accidental (or intentional) deletions and modifications. If a user
>> attempted
>> to execute a virus-laden program, the operating system would prevent it
>> from
>> doing any serious damage, simply because the key folders were protected.
>> The
>> days of system instability were numbered-- or so everyone thought.
>>
>> Let's jump to today. Windows XP, a descendent of Windows NT (and,
>> later,
>> Windows 2000) is now the dominant desktop operating system. We all know
>> that system instability and fragility are with us as much as ever.
>> Systems
>> are routinely reformatted and reimaged. Cleanup of adware and spyware is
>> a
>> commonplace task for the network consultant. What on earth happened?
>>
>> Somewhere along the way, the application vendors got lazy and
>> careless.
>> They started writing software that would run only if the user was made an
>> administrator. They never tested their software under ordinary user
>> accounts. In short, they just didn't give a hoot. Consultants were stuck
>> making everyone administrators because otherwise the applications
>> wouldn't
>> run, and the application vendors either didn't even know the difference
>> between an administrator and a user or they simply wouldn't support
>> running
>> their programs as a user. Users didn't help, either-- they insisted that
>> they needed to be able to install software.
>>
>> The situation today is critical. Because users are generally allowed
>> to

microsoft.public.windows.server.sbs: Re: Draft I: Why You Don't Want to Install Software

>> be administrators, not only can they consciously install software, but
>> they
>> can inadvertently install trojans, adware, and spyware, sometimes without
>> even clicking "Yes" to anything. Antivirus and anti-spyware software can
>> stop some of these pests from gaining a foothold in a system, but
>> basically
>> the workstation is wide-open for serious damage to be done. We've
>> returned
>> to the bad, old days of Windows 3.1.
>>
>> The single most effective defense against adware, spyware, trojans,
>> and
>> viruses is simply not to allow users to be administrators. When these
>> attempt to install, Windows will stop them dead in their tracks if the
>> user
>> is not an administrator. For this to be effective, however, users must
>> agree
>> not to be administrators and to leave software installation to
>> professionals. Professional network consultants, or network managers,
>> have
>> the experience to deal with glitches that may arise during installation.
>> Furthermore, tools now exist to help the network manager to determine
>> exactly what has to be done to make an application run with ordinary user
>> privileges-- but this process is not trivial and does require the
>> experience
>> of a professional.
>>
>> In summary, then, you don't want to be an administrator of your
>> workstation because the power to install software also gives anything
>> running with your name and password the power to install software-- and
>> the
>> power to destroy your system beyond simple repair. Even experienced
>> network
>> consultants don't run their own office workstations with administrator
>> accounts for everyday tasks. So stay behind the white line and leave the
>> driving to us!
>>