

Re: Access Workgroup File

Source:

<http://www.tech-archive.net/Archive/Access/microsoft.public.access.modulesdaovba/2004-07/1515.html>

From: Tim Ferguson (*FergusonTG_at_softhome.net*)

Date: 07/26/04

Date: Mon, 26 Jul 2004 10:28:06 -0700

"Larry Linson" <bouncer@localhost.not> wrote in
news:uyGhTyqcEHA.212@TK2MSFTNGP12.phx.gbl:

> *"Tim Ferguson" wrote*
>
> > *There is no legitimate use for such a*
> > *utility:*
>
> *it may well be used by people who legitimately have lost*
> *the password, had a developer leave under a cloud, etc..*

Okay: it may be a counsel of perfection about documenting UserIDs, PINs and
so on, but it is repeated all over all the documentation and instructions
for setting up Access security. I would guess that the care taken is pretty
much in proportion to the value of the encrypted data.

>
> *There aren't any*
> *applications done in Access so secure that US\$150 will not get you the*
> *data*

Last time I asked whether anyone had *_first hand_* experience of a properly
secured Access database being cracked, Rebecca R was the only one who
replied, saying she knew of someone who has seen it happen. Has time moved
on so that this is now reliably confirmed?

Not that I disbelieve it, I am just trying to get a grip on the reality of
the situation. Should we be advising friends/ colleagues/ clients to move
away from Access for sensitive data? Ok — that is far too vague a question
to get a sensible answer, but you can see what I am getting at.

> *Your data can be made much more secure by putting it on a server,*
> *using a good server database, and using the server OS and server DB*
> *security.*

Agreed absolutely.

microsoft.public.access.modulesdaovba: Re: Access Workgroup File

B Wishes

Tim F