

microsoft.public.access.security: Perhaps the most OBVIOUS question you will ever see.

## Perhaps the most OBVIOUS question you will ever see.

*Source:* <http://www.tech-archive.net/Archive/Access/microsoft.public.access.security/2005-02/0043.html>

---

*From:* Curious George (*curious\_at\_spampoop.com*)

*Date:* 01/28/05

Date: Thu, 27 Jan 2005 21:03:14 -0500

Dear Colleagues:

For the life of me I don't know why I have to ask this question since the answer is so obvious, however, I need to have others tell me that I am not completely insane.

I work at a place where we have a myriad of wireless access points and NO, I am not writing from there at present.

NONE of the wireless access points has any form of security on them whatsoever. No WEP, no CHAP. . . no nothing. Everything is open so you could walk into our joint, grab an IP address and surf the web to your heart's content.

Here is the problem. My boss insists that its "no big deal" and that since the servers are on the inside and protected, we really don't have a thing to worry about. Furthermore, my boss is under the impression that since we are situated in a wide area, that nobody would be able to get into our network because of this distance. Needless to say, my boss does not consider somebody sneaking into a parking lot with a laptop, a good network card and a directional bazooka antenna a possibility.

So here is what I have to explain to my boss' boss and, perhaps, the board of directors. . . and here is where I can't help but laugh. I hope that I will be able to keep a straight face come Monday when I have to explain myself to people why its important.

Okay, so I know the analogies. For example, I understand that not having a secure wireless network with many Waps and high gain transmission antennas is the same as putting cables out to anybody within 'x' amount of yards with a sign that says "free internet access", but since I am going to be asked these obvious questions, just what type of damage could somebody do?

Yeah, I know about denial of service attacks, yeah I also know about enumeration and password guessing, but considering that we have an SQL server on the inside of our network (no, the sa account password is not

Perhaps the most OBVIOUS question you will ever see.

microsoft.public.access.security: Perhaps the most OBVIOUS question you will ever see.

null) what are we talking about.

I can envision so many things. Like somebody just sitting there capturing packets to get things like usernames, passwords and the like, but come on. . . what else could they do.

I have read my boss the riot act many times, but this is now going to go in front of somebody over my boss' head, so, aside from giving them worst case scenarios, end of the world analogies, etc., how else could people break in.

Creative responses are appreciated and will be rewarded with much praise.

I can't believe that I have to actually explain this to people, and this entire thing would last about two seconds when it comes to talking with a computer professional, but you see, my boss is under the impression that they are a computer professional because they received a Master's degree in Comp Sci back in the 80's. I know that this line of thinking is dangerous, but I really want some creative answers to put my point across strongly, and yet professionally.

Although I realize that this post will likely be the butt of many jokes (which I will appreciate immensely) I never the less would appreciate a bit of useful information in your responses.

I am going to have a serious drink now, and then bang my head against the wall.

Thanks in advance,

CC