

WiFi Security Guy - Great IT Questions!

Q: Is this for designed to protect home PCs to WiFi router?

A: It protects from PC/laptop across wireless network (not "to" router).

Q: Is this designed to protect mail?

A: It protects more than just mail. It protects *everything* sent and received. That includes the pages you visit, unsecured login (a lot of memberships sites don't encrypt your login), forms you fill in, etc.

Q: Is the assumption that the only concern is for a hacker located near the home PC and can track all the data since WiFi is not protected?

A: The more likely scenario is that the hacker is located near the café, hotel, etc. where you are. There is much more traffic and therefore more data to collect.

Q: Do we still need a solution if there is WiFi WPA or WPA2 encryption deployed on the WiFi?

A: Yes. WEP, WPA, and WPA2 can all be broken. There are hundreds of videos on YouTube demonstrating it, as well as if you Google terms like "hacking wpa" you'll come across all the free tools to do it yourself.

If you're ready to get started with the: [WiFi Security Guy Team](#)

Q: What happens if the hacker sits between the WiFi Security Guy's server and the mail server... as the traffic between those two are not encrypted?

A: That's the backbone Internet provider like AT&T.

1. They are strictly regulated and you won't find interlopers just hanging out in AT&T's server room just collecting data.
2. If they have someone on staff breaking the federal regulations it won't matter if you are using my security or not, your data is going through that backbone today without my security. That's like asking, "Does your security stop the admin on the mail server from reading my mail?" Of course there's no way for me to that, and if they don't trust the admin on the mail server or that works for AT&T, they shouldn't be using the internet at all.
3. If you won't trust AT&T *with* my product, you won't trust AT&T without it either... get off the Internet because Ma Bell can see everything you're doing online.

Q: Is there a problem if the PC to mail server uses IMAP/SMTP over SSL?

A: Your mail would be secured, but nothing else.

Most email servers today don't even provide SSL connections, and those that do, the users don't know to set it up.

Like I said, I can go to Panera Bread on any given day of the week and record 2 hours during lunch break and always get 20+ logins.

If you're ready to get started with the: [WiFi Security Guy Team](#)

Q: Because the Home PC is dependent on the secure server and network speed it has, it may incur performance issues?

A: True. I ask all my clients if they notice any latency (slow performance). I have yet to meet one that it says it runs slower. Some even indicated that it seemed to run faster, and there's a good reason for that. The transport protocol is UDP (connectionless) which has much less handshaking packets going on and much faster recovery for missing packets than TCP, and the encryption algorithms not only encrypt but they also compress so more data is transmitted using less bandwidth.

That being said, I wouldn't download a movie.

Q: Many people do not configure WPA, WPA2 even if it exists and they do not configure mail over SSL, sometimes the mail servers themselves do not allow mail over SSL.

A: That's right. The last time I drove from downtown to my house (a 20 minute drive); I found that 94% of all the networks were not secured.

And being a hosting provider with secured email servers I can tell you most of my clients just don't configure their email to use the security.

Read more about [The six \(6\) WiFi Myths of a Wireless Network!](#)

Thanks, The WiFi Security Guy Team

If you're ready to get started with the: [WiFi Security Guy Team](#)