

# Top 4 TIPS of WiFi Security Guy

**1. How does wireless networking work?** Wireless networking is just like walkie-talkies. Whatever one walkie-talkie transmits, all the walkie-talkies in the area can pick up. Wireless networking is exactly the same. Whatever your computer is transmitting on a wireless network, every computer in the area can pick that up and see it. This includes your login names, passwords, emails, sites you visit, and account information. You may remember going to the mall about 10 years ago when it was the fad to have walkie-talkies when you split up into several groups. You'd use the walkie-talkies to coordinate eating together and meeting at different places. You may remember times when you would suddenly hear some other group of people on your walkie-talkie. They were doing the same thing as you, they brought walkie-talkies to keep in touch, and whatever they say, you can hear. And you also know whatever you say they can hear. Wireless networks are exactly the same.

## 2. The six (6) WiFi Myths of a Wireless Network

I've ran into a series of misconceptions over the years about wireless security and I compiled them together into one complete list.

**Myth:** It takes expensive computer equipment to get my personal information off of a wireless network.

**Truth:** I still have the first laptop I used to break into wireless networks. Today this laptop is 10 years old. It would actually cost you more in shipping to buy this laptop than the cost of the laptop itself. And it's still more than powerful enough to break into any network and collect all the personal and private information on that wireless network.

**Myth:** It takes expensive software to break into a wireless network and get my personal information.

**Truth:** The software is freely downloaded from the Internet. Using a search engine to search for wireless hacking tools will give anyone all the free software they'd ever need to collect your personal information off of a wireless network.

**Myth:** It must take a super genius to use that cheap laptop and free software, so I'm safe.

**Truth:** It took an expert in security and wireless networking to write those free tools, but they write the tools with the intention of them being easy to use so anyone can download them and break into wireless networks and collect all your personal information. And if someone is having problems getting those tools to work they just go back to the site where they downloaded the tool and ask for help. There are literally whole online communities dedicated to helping with the tools and advising on how to break into wireless networks and collect private information.

**Myth:** I have a password on my wireless network so I'm safe, when my friends come over they have to type in my password or they can't get on my network.

**Truth:** Those free tools from the Internet can easily break all versions of wireless encryption and passwords that come on wireless routers today. For proof just go to YouTube and search the following phrases: "hacking wifi", "hacking wep", "hacking wpa", "hacking wpa2". You'll see thousands of videos not only demonstrating how they broke into wireless networks but also videos that show step-by-step how you (or a hacker) can break into wireless networks (often within minutes).

**Myth:** The hotel/cafe I'm at gave me a password and they only give it to their guests, so I'm safe.

**Truth:** First, as we discussed in the previous myth that password is easily broken. Second, they give that password to everyone else so a hacker doesn't have to even break the password, they either become a guest or pretend to be one in order to get the password. And everything you do on that wireless network in the hotel or cafe can be seen by everyone else in the building.

**Myth:** I have Norton, McAfee, Windows Firewall, etc, so I'm safe.

**Truth:** That's simply not true. Norton, McAfee, other antivirus and firewalls are all good products and you need them. They protect your computer from receiving viruses or having other malicious things done to your computer. But they don't protect any of your information when it is being transmitted on the wireless network or while your computer is receiving it from a wireless network. If you have Norton, McAfee, or some other similar product I recommend you keep it, you need that protection, just keep in mind it doesn't keep your identity safe from theft on a wireless network.

As we found out on the call, Deb thought she was safe because a tool she uses to keep all her passwords uses "triple DES", but that just means it stores her passwords encrypted, but it can't encrypt them when it sends them to your email server (or your other online accounts), the email server is expecting the exact same password you used when you setup the account, sending an encrypted version would be different than what the email server expects so it wouldn't let you login.

**Get your Questions Answered here:** [WiFi Security Guy - Great IT Questions!](#)

**Bonus Myth:** I have Lifelock or some similar product so I'm safe.

**Truth:** Lifelock only protects you against someone opening a new account in your name or under your social security number. It doesn't protect against someone using your existing accounts to steal from you. Join our WiFi team and you'll learn how to get this service FREE! [WiFi Security Guy Team](#)

### 3. How would a hacker commit Identity Theft against me?

***All they need to do is watch you read your email one time!!***

Here's how they do it:

1. The hacker runs a tool called dsniff that captures every login name and password on a wireless network. When you go to read your email your login name and password are sent in "clear case" (which just means not encrypted, where anyone can read them) across the wireless network out to your email server. Once the hacker sees your login name and password he'll be able to read your email from that point forward. On any day of the week I can go to the local sandwich shop here in town and use dsniff to collect 20+ logins during a two-hour lunch period. People just don't realize what kind of information they are giving away.

2. That's bad, but it gets worse, a lot worse. Every online store you have an account with sends you fliers once a week at least. This hacker watches your email and makes a list of all of those online stores that send you fliers. Why? - Because that's where you have online accounts. After a couple weeks he's ready to strike, he has a complete list of all your online accounts. ***This includes your bank and credit card accounts - you get emails from them too!!!***

3. Now that he has a complete list of your online accounts he goes to each of the online stores in his list (he can do other things with your bank and credit cards, but I'm just covering your online stores here). He tries to login to each of those stores with the same password you use on your email account - 95% of all people only have one password on all their online accounts!!! The hacker knows this and tries this method first.

4. Let's say you're smart, you use a completely different email address for every one of your online accounts. Good for you, but that doesn't present a problem for our hacker. He goes to each of the stores and has your password reset. Where does the new password go? It goes in an email to your email account which he is reading. He writes down your new password and deletes the email so you never see it. Now he goes to each of your online stores, logs in to your account, and places an order with your credit card on file - a large order, \$2,000 - \$5,000 worth. And he has it overnighted, and not sent to him, but to a local apartment complex or maybe an apartment complex in another city where he has someone he works with who will pick it up.

5. The reason he has it sent to an apartment complex is because there are a lot of people going in and out and the chances of him being noticed are really small. Also, Fedex/UPS just knock on the door and leave the boxes sitting there. The hacker uses the tracking number from the order to know exactly when the package was delivered and he picks it up within 5 minutes. If necessary he can even be there to sign for the packages, "pretending" to be going into that apartment right when the delivery man shows up.

6. The reason the hacker has the package overnighted is two-fold: (1) Why not? It's not his money, (2) Your card isn't charged until "fulfillment". In other words if it takes 3 days for the company to put that large order together your card isn't charged until the 3rd day. Since it's overnighted, your card is charged one afternoon and the hacker is picking up the shipment in less than 24 hours. That gives you a 24-hour alert period from the time you would first know there was an order placed on one of your cards until the time he actually receives the goods. In that 24 hours you would have to (1) realize there is a charge on your card you don't recognize, (2) contact the company the charge came from and "argue" with them over the fact that you didn't place the order (and they'll say "oh no, Mr. Smith, we see here it was placed with your credit card using your online account you've had with us for years now..."), (3) realize it's fraud, (4) have the packages intercepted and arresting the hacker. You have a small 24 hour window to do that. Most people don't see the charges on their cards for weeks, usually not until after they receive their statement.

In the end you're out thousands of dollars, the online company thinks maybe you placed this order yourself and are trying to make it look like fraud, it takes a long time to clear up (even if they cooperate), ***and you never knew it was because you used a wireless network, as matter of fact you never really figure out how you got hacked.*** You change all your passwords, you don't know that it doesn't really matter, as long as you use wireless without any protection your Identity is always subject to Theft.

#### **4. OK, so how does Wifi Security Guy secure me?**

Wifi Security Guy creates an encrypted tunnel from your computer, out across the Internet, to a secured server. Everything you do is encrypted and put in this tunnel. Using the example of reading your emails, your login name and password are encrypted and put in the tunnel where they travel across the wireless network, across the Internet to our secured server. Our secured server is the only server in the whole world that has the correct encryption keys to decrypt your information and pull it out of the tunnel. It decrypts your login name and password, and sends them on to your email server. It's ok for your password to be un-encrypted at this point, because there's no hacker that can see it while it travels across the big back-bone networks of the Internet. If you have any mail the email server will send the emails to the secured server, the secured server then encrypts your email and sends it down the tunnel to your laptop. Your email travels across the wireless network inside the encrypted tunnel.

This encryption is the same grade that banks and the military use. A hacker may be able to break into your wireless network, or you may be on a "open" wireless network that doesn't have a password or encryption, but he can't see what's inside the encrypted tunnel. He can tell there's a tunnel there, but he can't figure out what's inside the tunnel. Join our [WiFi Security Guy Team](#)

Thanks, The WiFi Security Guy Team