Keep criminals off your Wi-Fi

4/30/2011

The worst thing you can find online is child pornography. Even the thought of it makes me sick. It is disgusting that someone would want to look at this filth. I'm sure you feel the same way.

So imagine if you were falsely accused of downloading child porn. A whole team of federal agents busts through your door in the middle of the night without warning. You're interrogated for hours before being hauled off to jail. All your computers and gadgets are confiscated.

That's just the beginning. You have a lot of explaining to do to your spouse and children. And don't forget about your neighbors who saw the whole thing.

This situation could permanently destroy your reputation. Even if you get the matter cleared up, it will always lurk in the back of peoples' minds. It will affect your kids, too. Who'd let their children play at a suspected pedophile's house? And image the schoolyard taunts.

I know what you're thinking. I'm being alarmist by creating a hypothetical situation that would never happen.

Tell that to the man from Sarasota, FL, who experienced a visit from the FBI. He was accused of downloading over 10 million images of child pornography. Fortunately, the real culprit was eventually caught. He had been sitting in a boat outside the victim's building. A simple aluminum can antenna let him access the victim's wireless network.

Or talk to the man in Buffalo, NY, who was rudely awoken one early morning. He heard someone breaking in to his house. When he went downstairs, he was confronted by a team of government agents. They were from Immigration and Customs Enforcement. The man was roughly subdued, and his electronic equipment searched.

The FBI had traced child pornography traffic to the man's IP address. Someone was using his router to distribute the images. The accused man wasn't responsible, but it looked like he was. He was eventually cleared after his computer was checked. One of his neighbors was eventually arrested instead.

Both men could have easily avoided their predicaments. Had they spent a few minutes securing their wireless routers, they would have been in the clear. The child pornographers would have used someone else's unsecured network instead.

Don't let a careless oversight disrupt your life. Take a few moments to secure your wireless network. Do it now; you never know when a pervert will try to steal your Wi-Fi.

Securing your router isn't terribly difficult. I'll walk you through the process. Just note that every router is somewhat different. I highly recommend having the manual on hand. It will help you find the right settings. If you don't have it, you can download it from the manufacturer's Website.

Additionally, you may lose your wireless connection during this process. So, print these instructions before you start and keep them handy.

Start by opening your computer's Web browser. Most routers have a Web-based administration system. You need to know your router's IP address to log in. This is normally either 192.168.0.1 or 192.168.1.1. Some routers use other IP addresses. Check the router's manual to find out which one your system uses. There is also a way you can find out manually.

PC users need to open a Command window. For Windows 7 and Vista, click Start and type in "CMD" (minus quotes). In XP, go to Start>>Run and type in "CMD" (minus quotes). Hit Enter.

In the resulting Command window, type "ipconfig" (minutes quotes) and hit Enter. You'll see a list of text and numbers on the screen. Find the phrase Default Gateway. The number next to that is your router's IP address.

Things are a bit easier on a Mac. Click the Apple logo in the top left and choose System Preferences. Then click on Network and find where it says Router. That will list the router's IP address.

Now, go back to your Web browser. Type the router's IP address into the address bar. Hit Enter to connect.

The router will ask for your username and password. If you don't know it, check your router's manual. Every router has a default username and password.

Of course, every hacker knows these defaults. They could waltz right into your network. So you should change the password. You can find the password section under Basic Settings or a similar heading.

Next, find the Wireless Settings page or similar. It will have an option for setting the network name (SSID). This is how routers identify themselves. Give your router a unique name so you can find it later.

There should also be a section for enabling encryption. This is what will keep the bad guys off your network. You want to make sure you have the right settings.

There should be several encryption options. The one you want is WPA-PSK (Wi-Fi Protected Access—Pre-shared Key). You can also find it listed as WPA2.

Avoid the WEP and older WPA options at all costs. These are outdated standards and can be broken. For good security, it's WPA-PSK/WPA2 or nothing.

If your router doesn't have WPA2, you may need a firmware upgrade. There should be an option for this in the router settings. Upgrading the firmware may enable WPA2 support.

If it doesn't, it's time to get a new router. They don't cost that much in the grand scheme of things. It's a small price to pay to keep away pedophiles and other criminal lowlifes.

Once you select the appropriate encryption, you'll need to enter a password. This can be 8 to 63 characters long. You want to make sure this password is strong. That means using at least 20 characters. Avoid common words and phrases. Be sure to use upper-case characters, lower-case characters, numbers and symbols.

This password is going to be hard to remember. You also won't be using it regularly. Go ahead and write it down. Just be sure to store it in a secure, yet handy place.

Once you're ready, click Save or Apply. This will enable the changes to your router. It will also kick you off the network if you're on a wireless connection. You'll need to reconfigure your computer to get back on.

In Windows 7, there is a wireless icon in the notification area. This is in the lower-right corner of the screen. Right-click the icon and select Connect to a Network. You'll see a list of available networks. Select your network from the list. It will be named with the SSID you set previously. Click Connect, enter your encryption password and click OK. That should be it.

In Vista, go to Start>>Connect To. Select your network name and click Connect. Enter the encryption password and click OK.

XP is a bit more complicated to configure. Go to Start>>Control Panel and double-click Network Connections. Right-click the Wireless Network Connection icon and select Properties. Then go to the Wireless Networks tab.

Find your network in the Preferred networks list. Select it and click Properties. Find the Network Authentication setting and select WPA-PSK. Under Data Encryption, select AES. Then for Network Key, enter the encryption password. Make sure the option This Key Is Provided For Me Automatically is not checked. Then click OK.

Your computer should reconnect to the network. This process will have to be repeated for every wireless computer and gadget. Fortunately, it should only have to be done once per gadget.

Advances in technology can lead to many benefits. However, there are usually some downsides as well. Learn how to avoid the dark sides of technology:

- You already know identity thieves want your information. Now, they're increasingly targeting children, with devastating effects. Find out how to protect your child's identity.
- Facebook is a great place to connect with friends and family. However, scammers would love to steal your profile. Enable Facebook's new security features to keep them out.
- The Internet is a great way to find useful information. However, your personal information is also floating around out there. Learn how to opt-out of people search sites.