

Dawn's Databytes

SECURING YOUR WIRELESS NETWORK

BY DAWN SANDERS

Aloha all! Last month we had our "Wireless Alphabet Soup." Now we'll see how to secure that network, but first some questions from our readers:

Dear Dawn,

I bought a new wireless system and it works fine except whenever my boyfriend calls I lose my connection. Do you think my new wireless system is jealous?

Signed,
Marcy in Makakilo

Dear Marcy,

No dear, your system is not jealous. Your wireless router is too close to the base station for your cordless phone. They both use radio waves and the phone signal is confusing the router. In fact, any device that uses radio waves can interfere with a wireless network. If possible, then move your base station to another room. If that is not possible, then you may just have to resign yourself to using a corded phone if you need to be on the phone and the Internet at the same time.

Databytes Dawn

Dear Dawn,

Just after I set up my wireless network I noticed my neighbor often sitting on his front porch with his laptop. He never used to do that.

Signed,
Suspicious in St. Louis Heights

Dear Suspicious,

Nothing suspicious about that! Your neighbor is blatantly using your wireless network to connect to the Internet. Remember wireless networks work on radio waves and they don't stop at your house walls. However, fear not! In next month's article, we will go over how to secure your wireless network. In the meantime, whenever you notice them out there, grab your cordless phone and stand between him and your router and make a call.

Databytes Dawn

With the growing populari-

ty of wireless networks and the inability to secure access within a room, where do we start with security? We need to add a few more ingredients to our Wireless Alphabet Soup. Here is the short list of steps to take to secure your network:

1. Change the default Service Set Identifier (SSID).
2. Disable SSID broadcasts.
3. Change the SSID periodically.
4. Enable MAC address filtering.
5. Enable Wired Equivalent Privacy (WEP) 128-bit encryption.
6. Change the WEP encryption keys periodically.

SSID is a 32-character unique identifier attached to the header of packets sent over a wide local area network (WLAN) that acts as a password when a mobile device tries to connect to the BSS. In other words, SSIDs are sometimes known as "network names." The SSID essentially is the name of the wireless network. It differentiates your wireless network from your neighbors. All access points and all devices attempting to connect to a specific network must use the same SSID.

If you are wondering how your neighbor can use your network without giving him

the SSID, it's because most wireless networking devices give you the option of broadcasting the SSID. They broadcast the beacon so that wireless-networking products, such as the wireless network interface card (NIC) in your PC, can easily find the access point. Unfortunately, these messages are unencrypted and contain much of the information needed for someone to surreptitiously connect and use your Wireless Network. While this option may be more convenient, it allows anyone to log into your wireless network, including your neighbor.

Another problem with wireless networking products is that they often come with a default SSID set by the factory. It does not take very much to discover the default SSIDs. For example, it is not uncommon for the default SSID to be the company name. Change your SSID to something unique. Look up "How to change the SSID" in the user's manual and carefully follow the directions.

Next, enable MAC address filtering. This allows you to provide access to only those wireless nodes with certain MAC addresses. This makes it harder for a hacker to access your network with a random MAC address.



Now, we come to WEP Encryption. WEP is a security protocol for wireless local area networks and aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. Use the highest level of encryption possible, a "Shared" Key, multiple WEP keys, and regularly change your WEP key.

All these steps help ensure that your wireless network is more secure. Unfortunately, in computers and networking, there are no 100% guarantees. As usual, the Internet is a great place to find information. One more step in securing a home network is to add a firewall device rather than a router.

Submit your questions to dawn@cdis-now.com and please visit us at www.cdis-now.com.

Happy Computing!
Dawn

Avoid "Scary" Investment Moves

SUBMITTED BY KEVIN O'KEEFE

It's Halloween. And, in all likelihood, you probably don't mind seeing some of the "terrifying" costumes worn by children. However, outside the realm of trick-or-treat, you'll want to avoid something that is truly frightening: bad investment moves.

Here are a few ideas for doing just that:

* Don't chase "hot" investments. In the past few years, investing in real estate has been "hot." Low interest rates have led an enormous number of people to purchase property not as a place to live, but as an investment vehicle. Their eagerness to become tempo-

rary landlords has been fueled by the belief that "housing prices always go up." But this just isn't true: housing prices have stagnated and fallen in the past, and they may well do so again in the near future. If that happens, many people will be paying mortgages on investment property with uncertain prospects - all-too-certain property taxes, leaky roofs and furnaces that need repair. So, whether it's investing in real estate or any other so-called "hot" market, don't rush to join the crowd - it may soon be full of people with regrets.

* Don't always accept "conventional wisdom." When there's turmoil in the world, inflation is heating up and the financial markets are strug-

gling, what should you invest in? Some would say gold. But on an inflation-adjusted basis, gold trades at roughly the same price as it did in 1833. By contrast, from 1926 through 2004, large-company stocks recorded an average annual return of more than 10 percent, compared with the average annual inflation rate of around 3 percent for that same period, according to Ibbotson Associates, an investment research firm. In other words, it doesn't always pay to "go for the gold" - or for any other "nugget" of conventional investment wisdom, either.

* Don't fall in love with your investments. Generally, it's a good idea to buy high-quality investments and hold

them for the long term - but "long term" doesn't necessarily mean "forever." For example, if you have developed significant concerns about a stock's future, or if the stock just no longer meets your needs, get rid of it. You can almost certainly find better uses for your investment dollars.

* Don't take a "time out" from investing. You can always find plenty of reasons for not investing: High oil prices, war, corporate scandals and more. But these problems, or ones even worse, have always been around - and the most successful investors have been the ones who kept on investing, through good times and bad.

* Don't forget your "emergency fund." If you haven't set

aside six months' to a year's worth of living expenses in a liquid account, such as a cash account or cash alternative, you risk jeopardizing your progress toward your long-term financial goals. Without this emergency fund, you may be forced to cash out some of your investments when you have to pay for a new furnace, a major car repair or some other large, unexpected cost. Over time, all these "raids" into your investments can really work against you.

By following these suggestions, you can go a long way toward eliminating those scary investment moves that can haunt your future financial security.