

*from MacWorld*

## ***HomePlug Network Adapters***

***Power-Line Technology Broadens Home Networking Options, but Security Issues Arise for Mac-Only Networks***

***By Christopher Breen***

Anyone who's wriggled through spider-infested crawl spaces and drilled into beams and walls in order to run Ethernet cable through a home or office has undoubtedly thought, "There's got to be a better way." Recently, that better way has been an IEEE 802.11b wireless network, a la Apple's wireless AirPort technology. But AirPort isn't an option if the distance you want your network to cover exceeds AirPort's range or if you have an older Mac -- such as a Power Mac G3 or a PowerBook without a PC Card slot.

But don't don the spider-suit yet, for there's another option: HomePlug networking. With two or more HomePlug 1.0-compliant adapters, you can network computers and printers -- as well as share a broadband connection -- via the power outlets in a home or office. We put five of these adapters through their paces -- the Asoka Plug-Link Ethernet Bridge, GigaFast HomePlug Ethernet Bridge, Linksys Instant PowerLine EtherFast 10/100 Bridge, Netgear Powerline Ethernet Adapter, and Phonex Broadband NeverWire 14 QX-201 -- and found that they all performed adequately. But only the NeverWire

adapter makes it easy for Mac users to implement security measures in a HomePlug network, and it's this feature that puts the NeverWire ahead of its competition.

### **Plugging Into HomePlug**

Each adapter has a power and an Ethernet port, and each has status lights that indicate an active power connection. (The Linksys adapter provides an additional light that turns on once you've established a 100BaseT connection.) To connect a device to your network, you'll have to plug it directly into a powered wall socket, and then connect one end of an Ethernet cable to the adapter and one end to your Mac's Ethernet port or a free Ethernet port on a router or hub.

Nearly all of these HomePlug adapters work in sets of two or more, with a 16-adapter limit on any given network. The HomePlug Ethernet Bridge adapter is the exception: it's currently limited to two adapters. (A new HomePlug Ethernet Bridge with

***Con't on page 2, HomePlug***



***United We  
Stand***

### **KMUG MEETINGS**

#### **Evenings**

First Wednesday of each month at 6:30 P.M.  
Bremerton Fire Station, 5001 Kitsap Way  
(across from Dairy Queen & Denny's)  
(park along Arsenal Way or in the parking

#### **Luncheons**

Third Thursday of each month at 10:30 A.M.  
Solarium Room, All Star Lanes,  
Myhre Road, Silverdale  
(one block East of Silverdale Way)

***KMUG's Newsletter Archive is now at:  
<http://homepage.mac.com/kmug1>***

## ***Con't from Page 1, HomePlug***

support for as many as 16 adapters should be available by the time you read this.) In a typical two-computer network, you'll have one adapter per machine. If you want to share a broadband connection, all you need is a HomePlug adapter connection for your router.

A HomePlug network can be affected by interference from household appliances such as stereos, computers, microwave ovens, and hair dryers. More-severe interference -- an intervening circuit-breaker box, for instance -- can disrupt the link between HomePlug adapters. Thankfully, these devices are rate-adaptive: they can lower their data rates to compensate for power-line interference. However, because such interference is common in most homes and offices, you may have to try different power outlets to find the best connection.

### **Power Networking**

Although all of the adapters can be used either in a computer-to-computer configuration or with a router or hub, certain adapters make it easier to set up these configurations. For example, the PlugLink Ethernet Bridge, HomePlug Ethernet Bridge, and NeverWire have switches that let you choose between a direct-to-computer connection and an uplink connection to a router or hub (the kind of connection you'd

choose if you were sharing a broadband connection, for example). The Powerline Ethernet Adapter lacks such a switch, but Netgear graciously includes a straight-through and a crossover cable, as well as instructions on when it's appropriate to use each. In what looks like a case of unfortunate economizing, the Instant PowerLine Etherfast 10/100 Bridge provides no Ethernet cables at all.

### **The Need for Speed**

Although HomePlug networks boast a maximum data-throughput rate of 14 Mbps, this is the theoretical limit. In practical use, you should see speeds about 30 to 50 percent faster than a typical 802.11b wireless network, which also operates well below its theoretical maximum of 11 Mbps. While this is sprightly enough for Web surfing, you'll really notice the slowness when you copy files across a network.

To test speeds, we attached the adapters to a 400MHz PowerBook G4 and a 700MHz flat-panel iMac G4. Both Macs were equipped with 10/100BaseT Ethernet ports. We copied a 50.2MB file between the two Macs over a wired Ethernet connection, over an AirPort connection (using an graphite AirPort Base Station), and via each of the five HomePlug adapters. We weren't surprised that

***Con't on page 3, HomePlug***

### **HomePlug Network Adapters Compared**

COMPANY	PRODUCT	MOUSE RATING	PRICE	CONTACT	SECURITY	INCLUDED UPLINK CAPABILITIES	PROS	CONS
Asoka	PlugLink Ethernet Bridge	3.5 mice.	\$99	650/591-3236, www.asokausa.com	Windows-based application	switch	Uplink switch.	No Mac encryption software.
GigaFast	HomePlug Ethernet Bridge	3.0 mice.	\$99	626/964-2960, www.gigafast.com	Windows-based application	switch	Uplink switch.	Supports only two units; no Mac encryption software.
Linksys	Instant PowerLine EtherFast 10/100 Bridge	3.0 mice.	\$99	800/546-5797, www.linksys.com	Windows-based application	none	Additional status light indicates 100BaseT connection.	No Mac encryption no included cables; software.
Netgear	Powerline Ethernet Adapter	3.5 mice.	\$99	888/638-4327, www.netgear.com	Windows-based application	crossover cable	Uplink switch.	No Mac encryption software.
Phonex Broadband	NeverWire 14 QX-201	4.0 mice.	\$129	800/257-0601, www.phonex.com	built-in hardware	switch	56-bit DES encryption via button on adapter.	More expensive than other adapters.

### Con't from page 2, HomePlug

the wired Ethernet connection was far faster than either the AirPort or the HomePlug connection -- it took just 6 seconds to copy the file.

Transferring the file over the AirPort connection took 3 minutes and 55 seconds. While not nearly as zippy as the direct Ethernet connection, the HomePlug adapters outperformed AirPort, with speeds ranging from as fast as 1 minute and 20 seconds to as slow as 2 minutes and 55 seconds.

These numbers reflect tests in a real-world environment, one in which electrical interference ebbs and flows. For example, when the adapters shared a plug with a power strip connected to a host of peripherals, including a computer, a scanner, a printer, and powered speakers, it took each adapter nearly a minute longer to copy our test file. Because of the many variables involved, we were unable to ascertain exact speeds for each of the HomePlug devices.

#### **(In)security**

Our speed tests shouldn't unduly influence your buying decision, but your ability to secure your HomePlug network certainly should. You can successfully link these adapters throughout apartment buildings and office spaces that share wiring; if you live or work in such an environment and would prefer that others not access your network or pilfer your bandwidth, you'll choose the NeverWire, hands down, for its security features.

Turning on encryption is a simple matter of pressing a Secure button on each NeverWire unit within the network. This initiates 56-bit DES encryption, which, although it's a less secure level than most current encryption schemes, is solid enough to deter all but the most determined hackers. However, the NeverWire's method is desirable only when you control the space in which the adapters reside.

To secure the other HomePlug adapters you must run the included Windows-compatible encryption application from a PC (all the adapters use the same Security Configuration Utility software). This software generates and stores a password in the unit's hardware, so you can configure the adapters with a PC and have the encryption still work with your Mac. If you don't have access to a PC and want a secure network, we don't recommend anything but the NeverWire.

#### **Macworld's Buying Advice**

At a cost of \$200 to \$250 for a two-computer network, these adapters aren't the most economical solutions around -- 1,000 feet of Category-5 (Ethernet) cable costs less than \$80 -- nor are they the speediest. But if you plan to operate a network in a single-family home or small office and don't require peak performance, you'll be content with any of these adapters. If you need a measure of security in your setup, Phonex Broadband's NeverWire 14 QX-201 is your only choice. ●

---

### from TechTV

## *Jaguar's Spam Filters*

*Apple's latest email program can help stop unwanted deliveries to your in box.*

*By Roman Loyola*

*Screensavers Staff, TechTV*

Apple's email program that comes with Mac OS X, called Mail, is often eschewed for mail programs that have more features. Fortunately, the updated Mail program that's available with Jaguar has many new features, including a spam-filtering service that can help ease the load in your in box. On today's show Leo demonstrates

the spam-filtering feature and shows you how to use it effectively.

#### **Train the spam sieve**

Mail's spam filtering is based on what Apple calls "adaptive latent semantic analysis." In plain English, Mail determines what is and isn't spam based on the content of the email you receive. Mail takes the email that you've designated as spam, identifies patterns of content within that email,

*Con't on page 4, Filters*

### **Con't from page 3, Filters**

and uses this analysis to identify spam in future email. (If you're interested in learning more about adaptive latent semantic analysis, read this University of Colorado paper.)

The key to Mail's filtering success is proper "training." When you first launch the new version of Mail, the spam feature is essentially blank. It has no definition of spam. You need to train the application to be able to correctly identify spam.

#### **How to train Mail's spam filter**

The beauty of Mail's complex spam filter is that it's very easy to train and use. By default, the filter is set to its Training option. Here's how you access the spam-filter option:

1. Launch Mail. Click the Mail menu and point to Junk Mail.
2. A pop-up menu should appear. If you haven't modified it, it will be set to Training .

In Training mode, Mail is learning to define spam. When you get spam in your in box, you tell Mail about the email by selecting it and then pressing the Junk button. Mail then uses that offending email as part of its definition of spam, and identifies it as spam by using a color code. As you select more

email as spam, the definition grows and Mail gets better at identifying spam.

If you get an email that's incorrectly identified as spam, all you have to do is select the email and then click the Not Junk button. Mail will then create a definition in its filter to designate future email like this one as not spam.

#### **Mail's spam filter goes automatic**

Once you've decided that Mail has been a good student and is done training, you can set the spam filter to Automatic. Here's how you switch to Automatic mode:

1. Click the Mail menu and point to Junk Mail.
2. A pop-up menu should appear. Select Automatic.

In Automatic mode, Mail automatically moves email that fits the spam criteria into the Junk box.

Make sure you keep it in Training mode for a while to build a robust definition of spam. That way, when you switch to Automatic you won't lose "real" email to your Junk folder.

You can inspect your Junk folder to see if an important email was erroneously marked as spam. Select the message and then click the Not Junk button. ●

---

## ***PERSONAL SECURITY CHECKS***

*I got this as an email from one of the kids. The suggestions really make since and should be seriously considered. ed.*

A corporate attorney sent the following out to the employees in his company. The next time you order checks have only your initials (instead of first name) and last name put on them. If someone takes your checkbook, they will not know if you sign your checks with just your initials or your first name but your bank will know how you sign your checks.

Put your work phone # on your checks instead of your home phone. If you have a PO Box use that

instead of your home address. If you do not have a PO Box, use your work address. Never have your SS# printed on your checks -you can add it if it is necessary, but if you have it printed, anyone can get it.

Place the contents of your wallet on a photocopy machine; do both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel. Keep the photocopy in a safe place. I also carry a photocopy of my passport when I travel either here or abroad.

We've all heard horror stories about fraud that's committed on us in stealing a name, address, Social Security number, credit cards, etc.

Unfortunately, I, an attorney, have firsthand knowledge

***Con't on page 5, Security***

Con't from Page 5, Security

because my wallet was stolen last month. Within a week, the thief(s) ordered an expensive monthly cell phone package, applied for a VISA credit card, had a credit line approved to buy a Gateway computer, received a PIN number from DMV to change my driving record information online, and more.

However, here's some critical information to limit the damage in case this happens to you or someone you know:

We have been told we should cancel our credit cards immediately. However, the key is having the toll

free numbers and your card numbers handy so you know whom to call. Keep those where you can find them easily.

File a police report immediately in the jurisdiction where it was stolen; this proves to credit providers you were diligent, and is a first step toward an investigation (if there ever is one).

But here's what is perhaps most important: (I never even thought to do this)

Call the three national credit reporting organizations immediately to place a fraud alert on your name and

Con't on page 6, Security

from MacWorld email

# Apple Computer vs Apple Corps

by Lisa Schmeiser, Senior Associate Editor, Macworld

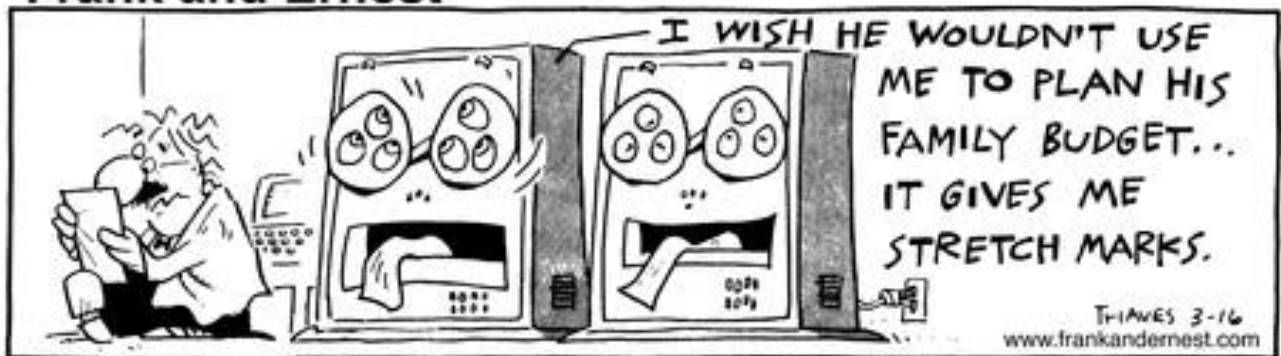
More on Apple Records: Who would have thought that a throwaway joke in a news summary would prompt reader mail, but some of you wrote in last week to ask whether Apple's reported music service would violate the terms of the agreement Apple Computer signed with the Beatles' recording company, Apple Corps. According to the book Apple Confidential by Owen W. Linzmayer, "Essentially, Apple Computer paid the British company an undisclosed sum for the worldwide rights to use the Apple name on computer products, but Apple Corps retained the rights in the music

field."

Not that this ended the matter tidily. In February 1989, Apple Corps filed suit against Apple, charging that Apple violated the terms of the agreement by marketing products with music synthesizing capabilities -- these products being the MacPlus, the Mac SE and the Mac II. Although Apple Computer maintained it had not broken the agreement, the company did pay a \$26.1 million settlement in October 1991. Exactly how the company paid was the subject of another, longer dispute between Apple and its insurers, one that wasn't resolved (not in Apple's favor) until May 1999. Apple had planned to appeal to the California Supreme Court.

There is currently no word in the press as to whether or not Apple Corps will be reviving any trademark disputes with the advent of any Apple Computer-based music subscription service. ●

## Frank and Ernest



Copyright (c) 1985 by Thaves. Distributed from www.thecomics.com.

*from MacWorld*

## *Protecting Your E-mail Address*

If you've ever published your address on a Web page or posted to a Usenet discussion group, odds are your e-mail address has been scooped up by an address trawler, a program that scans Web pages and newsgroups for e-mail addresses. Spammers collect and use these addresses, and they sell them to other spammers.

Protecting your address is largely a matter of staying under the radar of such address-harvesting tools. Here are some things you can do:

- Don't publish your e-mail address on a Web site, in directories, or in other public forums.
- Don't include your e-mail address in any links.
- Don't put your e-mail address in your signature.
- Don't enter your e-mail address into Web forms unless you trust the organization running the site and they have a legitimate need for your address. And even if that's the case, read the site's privacy policy to see whether it shares or rents address lists and stay clear if it doesn't have a privacy policy.
- Don't use opt-out or unsubscribe links in spam. If

they work at all, they only confirm that your e-mail address is valid and ripe for more spam.

**Web-Site Contacts** -- If you don't put your e-mail address on your Web site, how can people contact you? Although there's no single solution for every situation, there are some strategies:

Put a contact form on your Web site. For people who don't know how to create one, most ISPs provide templates. Just be sure to examine the HTML. If it contains your address (even as a hidden item), ask your provider for a form that doesn't spell out your entire address.

Make a small image that displays your e-mail address. Don't add a link. The downside: visitors without graphics capability (old browsers, cell phones, and so on) and visually impaired people may miss the information. Write out your e-mail address using full words. This may confuse some trawlers though spammers are beginning to catch on to this technique.

Use JavaScript tricks to obscure your address by encoding it or breaking it into unrecognizable chunks. (Check out Matterform Media's SpamVaccine [[www.matterform.com](http://www.matterform.com)] or simpler scripts that are widely available [see [www.joemaller.com/js-mailer.shtml](http://www.joemaller.com/js-mailer.shtml)].) However, these work only if your visitors' browsers support JavaScript, and address trawlers are starting to figure out this trick, too. ●

---

### *Con't from page 5, Security*

Social Security number. I had never heard of doing that until advised by a bank that called to tell me an application for credit was made over the Internet in my name. The alert means any company that checks your credit knows your information was stolen and they have to contact you by phone to authorize new credit.

By the time I was advised to do this, almost two weeks after the theft, all the damage had been done. There are records of all the credit checks initiated by the thieves' purchases, none of which I knew about before placing the alert. Since then, no

additional damage has been done, and the thieves threw my wallet away this weekend (someone turned it in). It seems to have stopped them in their tracks.

The numbers are:

Equifax: 1-800-525-6285

Experian (formerly TRW): 1-888-397-3742

Trans Union: 1-800-680-7289

Social Security Administration (fraud line): 1-800-269-0271

We pass along jokes; we pass along just about everything. Do think about passing this information along. It could really help someone you care about. ●

# *KMUG Meeting Minutes*

## *April 17, 2003*

Frank Hartung, President, opened the April 17 meeting at the Star Lanes in Silverdale by discussing a new service to dial-up members which consists of a CD furnished by Frank containing the latest software updates. One or two of them will be available to members to pass around in lieu of downloading huge files through dial-up. The subject of starting a new web page at for the Club at .mac was also discussed.

Don Diehl reported that membership is remaining constant and distribution of the Newsletter is going well.

John Pizzo has a new toll free number (1-877-577-5996). His email address is pizziconsulting@earthlink.net. He stated he charges \$75/hr for a prepaid program for 6 hours a year for

\$395. Quick phone calls from his clients are free.

Gwen Kauffroath mentioned that the last meeting of Mac Lab which is held on Tuesdays at 2:45-4:30 at the Jr. High School on Hostmark Street when school is in session, had an interesting session about Fonts. At a later date Lewis Coleman will give a demonstration of Apple Scripts.

Other subjects discussed covered which new printers and scanners members suggested, where to download updated drivers, changing passwords in Keychain, sources to get waterproof paper for printing labels for outdoor use (searching with Google works) and customizing music in iMovie or iPhoto for slide shows.

Submitted by:  
Phyllis Robie

---

### *Technology - MacCentral*

## *Spammer Sues User Who Fought Back*

*By Art Jahnke, CIO.com*

Like just about everyone else, Francis Uy has no use for spam. In fact, Uy hates spam. He hates it because it fills up his inbox with a lot of offensive junk, and he hates it because of the hassle that it brings to one of the most helpful technologies that has appeared in his lifetime, the Internet.

"Anyone who uses the Internet for business knows how much time and bandwidth it takes to deal with all of that junk," said Uy.

But unlike just about everyone else, Francis Uy decided to do something about spam. After receiving an unwanted offer to buy anti-virus software, Uy, a tech specialist at Johns Hopkins University, visited

the seller's website and found the name -- Allen Moore -- and address of the spammer. He then posted that information on another site, where he encouraged site visitors to use Maryland's anti-spam legislation to sue spammers.

As it turned out, site visitors took a more direct action, calling Moore on the phone and signing him up as a subscriber to magazines that he never subscribed to.

When the issue finally did make it to court, it was Moore who brought it there, claiming that he had received eight harassing telephone calls, more than 200 unwanted magazines and dozens of products that he never ordered. Moore sued Uy for harassment.

On Monday, a Maryland district court judge ruled that Moore was wrong: Uy had not harassed him. At least, Uy hadn't harassed him any more than a newspaper harasses people whose names are published along with descriptions of their misdeeds. The website could stay, the judge said, and Moore could either take a hike or appeal. ●

***KMUG's Newsletter Archive is now at:  
<http://homepage.mac.com/kmug1>***

----- **ABOUT MEMBERSHIP** -----

To join Kitsap Macintosh User's Group, send name, address (e-mail and snail mail) and dues (see renewal below for membership fee to:

**KMUG**

**P.O. Box 1271, Silverdale, WA 98383**

or come to one of our meetings and sign up!

----- **ABOUT KMUG** -----

**Officers/Board of Directors**

President pro tem .....	Frank Hartung (fhartung@charter.net)	Web Page Developer .....	Richard B. Nerf
Vice President .....	Vacant	Event Coordinator .....	John Dunlop
Treasurer .....	Don Diehl (diehldon@attbi.com)	Secretary .....	Phyllis Robie
Newsletter Coordinator ...	Joe Williams (jwilly6173@yahoo.com)	Member-at-Large .....	Wally Dowd

----- **RENEWING MEMBERSHIP** -----

If you received a paper newsletter please check the membership expiration date on the address label.

To renew with the newsletter e-mailed to your computer, dues are \$20.

To renew with a paper newsletter, dues are \$30.

----- **ABOUT MEETINGS** -----

**Evenings:**

First Wednesday of each month at 6:30 P.M.  
Bremerton Fire Station, 5001 Kitsap Way  
(across from Dairy Queen & Denny's)  
(park along Arsenal Way or in the parking lot)

**Luncheons:**

Third Thursday of each month at 10:30 A.M.  
Solarium Room, All Star Lanes,  
Myhre Road, Silverdale  
(one block East of Silverdale Way)

**This month's newsletter editor was Joe Williams**



**KITSAP MACINTOSH USER'S GROUP  
POST OFFICE BOX 1271  
SILVERDALE, WA 98383**

