Practical Information for Residents of Manufactured Home Communities

Resident Reporter

Western Manufactured Housing Communities Association

PUBLISHED BY WMA
455 CAPITOL MALL, SUITE 800
SACRAMENTO, CA 95814

Hang up on phone fraud

Consumers are beginning to see the effects of a new form of fraud on their telephone bills. This new fraud, in which hackers compromise voicemail systems in order to make fraudulent collect, third-party or direct-dial calls, has surfaced industry-wide. It isn't until consumers receive notification from their telephone company's security group, notices something different about their voicemail greeting, or receives a large bill that they realize they've become a victim.

Major phone companies have begun implementing new advanced security measures to protect consumers and businesses against this fraud by introducing technological solutions to thwart unauthorized calling from some areas of the world that generate the highest incidences of fraudulent calling.

Now for example, some consumers or business people who receive AT&T international collect calls may notice that instead of saying "yes" to accept an international collect call, they may be asked to follow instructions as to random codes they will need to speak or dial when prompted by an automated operator. Such technological deterrents have proven very effective to date.

Defense:

- Always change the default password provided by the voicemail vendor.
- Choose a complex voicemail password, of at least six digits, so it would be difficult for a hacker to guess.
- Don't use obvious passwords such as an address, birth date or phone number.
- Change your voicemail password often.
- Check your announcement regularly to ensure the greeting is indeed yours.
- Owners of small businesses should consider disabling the auto-attendant, call-forwarding and out-paging capabilities of voicemail if these features are not used because those features also can be hacked.

The Facts About The 809 Area Code Scam

Fraudsters have been distributing bogus e-mails through the Internet that are purported to come from AT&T. The topic, a phone scam involving the 809 area code. The scam itself is real, however, the e-mail and warning contain erroneous information.

The 809 area code scam first surfaced five years ago and continues to victimize consumers on occasion, although much less frequently than in the past. And there have been far more inquiries recently than consumers actually being victimized.

How the Scam Works

In most cases a message is left on an answering machine or pager requesting the recipient call a number immediately for one of several reasons. The most common involves calling for information about a relative who has died, been arrested or injured. When consumers fall prey and call the number, the scam artist attempts to keep the caller on the line for as long as possible to increase the caller's long distance calling charges. The bogus e-mail claims the 809 area code sends calls to the British Virgin Islands, when in fact 809 is the country code for the Dominican Republic.

The e-mail also warns consumers that dialing the 809 area code will result in charges of $2,400 per minute. That simply isn't true. The basic rate for a call to the Dominican Republic is less than $3 a minute although some 809 numbers terminate with pay-per-call services that permit the levy of additional fees. Since numbers located offshore are not subject to U.S. laws, there are no legal requirements that consumers be informed in advance of the extra charge. And lastly, the e-mail purports to originate within AT&T's corporate offices and includes the name and partial telephone number of an imaginary employee.

Defense:

- To avoid falling prey to the scam, consumers should know where they're calling before they dial. When consumers receive such a message from someone they don't know they should simply disregard it.
- Consumers should also be aware that it is usually necessary to dial 011 to reach an international location. However, there are some locations outside the United States, such as the Caribbean and Canada, whose telephone numbers resemble domestic long-distance calls, but carry a higher international rate.
- If a consumer isn't familiar with a certain area code, they can visit www.consumer.att.com to look up any area code or country code in the world.

Revealing your calling-card number

Your calling-card-number is like money in the bank to scam artists who can use it to sell long-distance calls to locations around the world. Here are some potential scams that may con you out of your calling-card-number:

Someone calls you at home posing as a telephone representative and asks for your calling-card-number to check on unauthorized charges billed to your account. Or, the caller may tell you that your calling-card-number has been deactivated in error and that he needs you to "verify" your number so it can be re-instated in the system.

Defense:

- Never give your calling-card-number to anyone over the phone no matter how convincing they sound.
- Most major phone companies have systems in place that will provide an early warning that fraud may be occurring. For example, a high incidence of international calls on a customer's calling card that previously showed no international calls will trigger an alert to AT&T for investigation.
- Reputable phone companies' representatives would never ask customers to identify their calling card number, unless you initiate an operator-handled call.

Cramming and Slamming

"Cramming" occurs when telephone customers are charged for services they've never ordered or received. Close behind came "Slamming," which occurs when customers have their telephone service switched without their permission. Here are some common ways you could be crammed or slammed!

You may receive a sweepstakes promotion in the mail telling you to call an 800 number to win a prize. When the call is made, an automated system is activated and you are unknowingly enrolled in a club or program, and the charge is placed on your phone bill. Or, you may fill out a contest entry form, only to discover later than the promoter used your phone number to sign you up for a calling card, voice mail or some other service. In many instances, the fine print on the form said that by entering the contest, you have signed up for the service.

You may receive a call from a telemarketer asking you to switch your long-distance service. Although you say you are not interested in switching, your long-distance service is changed anyway. Or, you may fill out a contest entry form, which also changes your long-distance service without your knowledge. In many instances, the fine print on the form said that by entering the contest, you have agreed to switch your service.

Defense:

- You can guard against both cramming and slamming by reading your phone bill carefully each month. Watch for unfamiliar company names, logos or charges that you don't understand or don't remember ordering. Call your carrier or the number associated with the charge and ask for an explanation.
- Ask that all offers from communications providers be sent to you in writing so that you may review them before making a decision. Read the offers carefully before signing any form, contest entry, check or survey.
- Make a note of the name and telephone number of the marketing representative in case you need to reach the company in the future.
- Check your telephone bill periodically to make sure you still have the long-distance company you selected. You can call (toll free) 1-700-555-4141 to verify your long-distance company.

Placing International Calls Without Realizing It

It's not always easy to tell if you're dialing an international telephone number. In most cases, you have to dial "011" to begin a call to a foreign country. But there are locations outside the U.S. whose telephone numbers may look like domestic long-distance calls, but they are actually international calls and international rates apply. For example, 809, 284 and 876 are area codes in the Caribbean.

There are many scams that deceive consumers into calling international numbers. You may see an ad for a service that directs you to call a specific number, or you may receive a page, an e-mail message or an "urgent" message on your answering machine. All messages direct you to call a number for more information - almost always an international number.

Defense:

- Be cautious about area codes you don't recognize. Check your telephone directory or call the operator to determine where the area code is before making your call.
- Control access to your telephone so unauthorized callers do not use your phone to call these services. A block on calls to "900" services will not stop calls to "011" or "809" numbers. If you're sure you won't need to make international calls, call your long-distance carrier and ask them to put an international block on your telephone line.

Call Forwarding Scam

You may receive an automated message on your telephone that says you have won a prize or money. The message directs you to dial a 2-digit code preceded or followed by the * or # key (such as *79 or 72#), and then an 800 number to claim your prize. When you dial the number, you are not connected to anyone. What this procedure has done, though, is program your telephone to forward your calls to a long distance operator. Con artists can then call your number, be forwarded to the long-distance operator and place calls that are billed to your home telephone number.

Defense:

- If you receive this type of call, simply hang up. If you receive this message on your answering machine, do not place this call. No legitimate sweepstakes or contest would likely contact you in this manner.
- Know the numbers used for Call Forwarding from your local telephone company.

For more information and other valuable tips, please visit www.att.com/fraud/home.html