Blacklisted! 411

The official hackers magazine

INSPIRING MINDS TO THINK OUTSIDE THE BOX...

The Origins of Phreaking

A new class of hackers arose in the last half of the 1900s

Also inside this issue:

The World of Vintage Computers
The Macintosh Underground
Tempest Monitoring

VOLUME 6 ISSUE 2 SPRING 2004

Blacklisted! 411 v6i2
$5.95 U.S. $7.75 CAN

The Origins of Phreaking

By Gary D. Robson for Blacklisted! 411

Hackers are people fascinated by technology and its applications. How could anyone who fits that description not be drawn by the allure of something as ubiquitous as the telephone? The phone on your wall is an amazingly simple device, yet the phone system on the other end of those wires is one of the most complex switching systems ever created.

A whole class of hackers arose in the last half of the 1900s that focused their attention and fascination on the telephone system, and they called themselves phone phreaks. Phreakers are a class unto themselves. They might mess with trunk lines just to see how things work (like when Steve Wozniak and John "Captain Crunch" Draper tried to call the Pope in Rome), or break into the telephone switches themselves, as Kevin Poulsen did when he rerouted lines to manipulate a radio station contest and win a Porsche.

No other type of hacking has generated the wealth of hardware gadgets ("boxes") and massive underground community that phreaking has. Sometimes it is clearly illegal. A little later in this article, you'll read about someone who went to jail just for possessing a device that could make free long-distance telephone calls. Sometimes it's very useful. Long before they were available commercially, phreakers were building controls that flashed lights when the phone rang.

Have you ever dealt with a poorly-wired building with multiple telephone lines? Figuring out which number you're using can be quite a pain. Telephone linemen use a telephone number called the ANAC (Automatic Number Announcement Circuit). When you dial it, an automated voice reads back the number you're calling from. This number is not given out to customers, and is often changed every quarter, or even more frequently. When I was wiring a phone board in a building with 20+ phone lines, the ANAC number saved me a huge amount of time and trouble, and it saved a lot of calls to the operator, too. Unfortunately, the only way to find it is through a friendly phone company employee or your neighborhood phone phreak.

Where It All Began

I can't say for certain the exact moment when phone phreaking was created, but I can tell you that Joe Engressia's experience was one of the first, if not the first. It was around 1957, and Joe was eight years old. Joe was fascinated by telephones. When talking on the phone, it didn't matter that he was blind.

He discovered that he could dial recorded messages, and listen to all kinds of fascinating things. Often, he would happily whistle to himself as he listened to the recordings, and one day, the recording stopped abruptly as he was whistling. Ever curious, he experimented. Because he was blessed with perfect pitch, he discovered that whistling the E above middle C (a frequency of 2600 Hz) would stop the recording every time.

What the eight-year-old Engressia didn't realize was that the 2600 Hz frequency was an internal telephone company signal to take control of a trunk line, which opened up almost limitless possibilities for routing calls with no long-distance charges. Since he didn't know what was going on, Engressia actually called the phone company and asked why the recordings stopped. That was just the beginning of his love of exploring the telephone systems.

When you placed a long-distance call in those days, the system was quite simple. You would connect first to your local telephone exchange. When it detected that you were dialing long-distance, it would scan the outgoing trunk lines for an "idle" tone—the 2600 Hz frequency that Engressia discovered. A phone phreak would dial an 800 number, which would trigger the local exchange to connect an idle trunk line and tag the call as free. Then the phreaker sent the 2600 Hz tone down the line. The long-distance exchange would interpret that as an indication that the call was complete, but the local exchange would still consider the trunk to be in-use for a free call.

At that point, the phreaker could dial anything and connect to anywhere, with the call still identified as free.

In the years that followed, Engressia learned how to manipulate the trunks after he connected, and got to know more phone phreaks like himself. He could place long-distance calls anywhere without getting billed for them, but that wasn't what motivated him. He just wanted knowledge.

Others without Engressia's perfect pitch had to come up with different ways to produce the 2600 Hz tone. Some used an electronic organ or synthesizer, playing into a normal tape recorder. Others decided to create devices to produce the tones that they needed. Those devices, called boxes, were fairly simple at first, just producing the 2600 Hz tone, and other frequencies needed to routing calls on the trunks. Those original boxes were called blue boxes. Later, a whole rainbow of boxes would emerge, doing everything from simulating the signal generated by a coin dropping in a payphone slot (a red box) to letting other people call you without getting billed for it (a black box).

Some discovered the simplest of all methods. The toy whistle enclosed in a box of Cap'n Crunch cereal, if one of the holes was covered, produced a 2600 Hz tone. This little whistle gave John Draper, who later became famous for his blue-boxing exploits, the nickname of Captain Crunch.

Engressia became obsessed with learning about phone systems. His dream was to get a job with the telephone company. He traveled around the country by bus, taking guided tours of telephone company offices wherever he could.

When Engressia was caught, articles about him ran in many Southern newspapers and magazines, and his fame grew. Soon, he was in touch with phone phreaks all over the continent. He even got a mention in Cecil Adams' column, The Straight Dope (later reprinted on page 238 of Adams' book, The Straight Dope Tells All).

In 1971, *Esquire* magazine ran an article about phone phreaking, featuring Engressia's and Draper's exploits, and those of some people

who manufactured blue boxes, including one man who sold them to the Mafia. The *Esquire* article quoted Engressia as saying,

> *"I want to work for Ma Bell. I don't hate Ma Bell the way some phone phreaks do. I don't want to screw Ma Bell. With me it's the pleasure of pure knowledge. There's something beautiful about the system when you know it intimately the way I do."*

To many people, there's a big difference between exploring the phone systems (as Draper and Engressia did), selling devices that can provide free, untraceable calls (as Steve Wozniak and the fellow in the article did), and out-and-out criminal activity like stealing and selling credit card numbers. To the telephone companies, and to prosecutors, they are all criminals.

Because of the Esquire article, Draper was investigated, and it led to the first of several jail terms for him. Engressia, too, went to trial. He was given a suspended sentence on the condition that he give up phone phreaking for good. An unexpected side effect of his trial was that the phone company refused him service, leaving him unable to get a telephone in his own name.

Despite these busts (or perhaps in part because of these busts and the publicity they generated), phone phreaking was at its heyday. The network of phreakers was growing, they were developing more and more ways to share information, and the phone companies hadn't developed good technologies to prevent phreaking.

Hardcore phreaks often learned more about the telephone systems than the technicians that maintained the equipment. Eventually, Engressia did achieve his goal and become a troubleshooter for Mountain Bell in Denver. Others went the same route. "Control C," a member of the infamous hacking group "Legion of Doom," became an employee of Michigan Bell.

Phone phreaks communicated, of course, using the phone. They might use simple loops, or set up huge conferences like the famous 2111 conference that took place in early 1971. The 2111 conference, which took advantage of an unused test system in Vancouver, BC (Canada), went on 24 hours a day, 7 days a week, for months. It was a never-ending stream of information sharing.

Later, the communication moved more to bulletin board systems, which started popping up all over the country in the 1980s. This led to actual written guides to phreaking, and later to police "sting" boards like the Phreaker's Phortress.

At the core of phreaking were those blue boxes and their multicolored brethren.

Blue Boxes

In a television special produced by WGBH in Boston, Steve Jobs talked about how he and Steve Wozniak, the famous founders of Apple Computer, got their start. "Woz and I had known each other since I was about 12 or 13 years old," Jobs said. "And our first project together was, we built these little blue boxes to make free telephone calls, and we had the best blue box in the world. It was this all-digital little blue box."

In fact, the two Steves sold these boxes door-to-door in the dormitories. Then, as Jobs said, "We had a lot of fun doing that." Now, of course, that could lead to jail time. According to John "Captain Crunch" Draper, Woz actually made enough money from selling these boxes to build the original prototype Apple I computer.

Building a blue box is trivial. Even a non-geek can pick up a musical instrument that generates a fairly pure tone (such as a synthesizer), and play E above middle C into a tape recorder. Presto! Your handheld tape recorder is now a blue box.

For decades, the phone company could do little about blue boxes. They monitored phones with suspicious calling patterns, but that did nothing to hinder phreakers that used public pay phones. Gradually, though, as the system changed over from analog to digital, the 2600 Hz signal was phased out or blocked from consumer equipment, and blue boxes worked in fewer and fewer places. Today, a blue box is nearly worthless.

Red Boxes

With the rampant curiosity of phreakers, it was only a matter of time before somebody wondered how the phone company knew when coins had been dropped into a pay phone. Eventually, it was discovered that all you had to do was replace the 3.579545 MHz crystal in your dialer with a 6.5536 MHz crystal, and you could reproduce the sound of coins dropping in the payphone slot! Thus was born the "red box."

By the way, it doesn't really work the way it was portrayed by Razor and Blade in the movie *Hackers*. Remember the scene where they describe using a tape recorder to record the sound of $5.00 in quarters dropping into a payphone? Just hit "play" and you'll never pay for a call again? The tones generated by the phone when quarters are dropped in the slot don't actually get sent back to the earpiece of the receiver, so you can't record them..

Instructions appeared all over the underground BBSs, showing how to modify a Radio Shack tone dialer to create a "red box." Changing the crystal made the * key generate 1700 Hz and 2200 Hz instead of the original 941 Hz and 1209 Hz. Repeating it five times with the proper timing produced the tones that the payphone transmitted when a quarter was dropped in the slot. A black market was generated in 6.5536 MHz crystals.

Does this still work? There are probably places where it does. Federal laws have tightened up so much, though, that you can get jail time simply for possessing a red box. Even if you never use it. Even, in fact, if you don't know what it is.

Ed Cummings, who writes under the pen name of Bernie S, found this out the hard way. In March 1995, he was arrested for possession of a red box, and ended up spending almost a year and a half in jail.

Of course, there is always more than one side to a story, and the Bernie S story is a long and complex one. The prosecutors pointed out that he was convicted earlier of tampering with evidence for removing batteries from a dialer, which made this a parole violation. They also noted that he was found to possess computer hardware and software that could potentially be used to obtain "unauthorized access to telecommunications service," and "subversive" materials, including a copy of the Anarchist's Cookbook and bomb-making instructions. The defense pointed out that he has never been accused of actually using the red box, or any of the other devices. In fact, the core of the prosecutor's case in this regard centers around the premise that a red box's only use is theft of service, and that there is no legitimate purpose for owning one. With the passing of the USA PATRIOT Act in 2001, the Federal government has made it clear that the pursuit of knowledge is not always a safe one.

All in all, take this as a warning. Messing with red boxes can have extremely negative consequences. Neither *Blacklisted! 411* nor this author encourage building, using, or owning them.

Caller ID

Caller ID is offered by just about every telephone company these days. They advertise that people equipped with caller ID boxes can see the telephone numbers of everyone that calls them. Of course, you can easily block caller ID by either calling the telephone company and telling them that you would like caller ID disabled on your telephone line, or dialing a special prefix before your calls (typically *67).

Don't let these lull you into a sense of false security, thinking you're making untraceable calls. Remember the following:

1. Caller ID can not be blocked when calling 800 numbers (or other toll-free numbers, like 888). Since anyone with a toll-free number is paying for the incoming call, they will know the calling number.

2. Caller ID is not blocked on internal telephone company equipment. They can always look at the ID on the call, even if it is not transmitted to the phone you're calling.

3. Caller ID can not be blocked on "911" emergency lines, and on other special law enforcement lines.

BLACKLISTED 411 WANTS YOUR ARTWORK

Are you an artist? Do you like Blacklisted! 411? Do you hate Blacklisted! 411? Well, if you're looking for work, it doesn't matter if you like us or not, does it? If you'd like to show off some of your talent, why not send us some samples on PAPER or send us a disk with your sample artwork. We'd be happy to show off your work, give you a free subscription or make some other arrangement if you'd like. If you're interested, take a look through the magazine and make note of the existing artwork. Think about it and try to come up with something completely original which coincides with the general theme of the magazine. A few ideas to consider: Pirates, Skull & Crossbones, Einstein, Computers, Electronics, Phones, Cable TV, Satellite TV, Radio, etc.

Here's who you send your artwork to:
Blacklisted! 411 ARTWORK
P.O. Box 2506, Cypress, CA 90630

We WANT to hear from YOU*....don't delay - just send us what you have. We prefer freehand artwork on PAPER, but will accept in high resolution (if at all possible) computer graphics formats: TIF, TGA, JPG, GIF, PSD, PCX and most other popular image formats.*

How Caller ID Works

The caller ID data packet is transmitted during the "silence" between the first and second ring. It consists of a packet of mostly ASCII data sent at 1200 baud, with 8 data bits, 1 start bit, 1 stop bit, and no parity. The basic ("single message") data packet looks like this:

Message Type: Always 04 hex.

Message Length: Total number of data bytes in message. Does not include the length of the header information or checksum.

Four-Byte Date: ASCII representation of date as two-digit month followed by two-digit day (e.g., 0321 for March 21st).

Four-Byte Time: ASCII representation of current time, in receiving party's local time zone, as four-digit military time (e.g., 1430 for 2:30 p.m.).

Telephone Number: The telephone number field will contain one of three things:

1. The telephone number of the calling party (in ASCII)
2. "O" (Uppercase letter O, ASCII 4Fh), if the receiving party's central switching office doesn't have the phone number information. This could happen in a call originating from an area without caller ID capability.
3. "P" (ASCII 50h), if the person initiating the call has caller ID blocked, either because the caller requested that the central office disable it on that number, or because the caller pressed a bypass code (usually *67) before the call.

Checksum: All of the bytes of the date, time, and phone number, added together modulo 256. This means that only the eight lowest-order bits of the sum are kept, so that the checksum will fit in a single byte. This is used to verify that there hasn't been a transmission error in the caller ID packet.

As an example, if I called you at 8:00 a.m. on July 4 from 202/555-1234, the caller ID packet would look like this (in hex):

04 12 30 37 30 34 30 38 30 30 32 30 32 35 35 35 31 32 33 34 90

The first byte says that this is a caller ID packet, and the second says that there are 18 bytes of data (12h). The data, in ASCII, is "07040800202555 1234", which is the date, time, and telephone number. If the 18 data bytes are added together, the result is 390h. Keeping only the rightmost byte gives us the checksum of 90h.

If a caller disabled caller ID before making that call, the packet would look like this:

04 09 30 37 30 34 30 38 30 30 50 90

Again, the first byte says that this is a caller ID packet, and the second gives the length, which is 9 bytes. The date and time are the same as the previous packet, and the 50h, which is an ASCII "P," indicates Privacy Mode, or disabled caller ID.

There is also a "multiple message" data format that transmits a name along with the telephone number.

Caller ID and Computers

Do you think that caller ID's usefulness ends at that little $19.95 caller ID box that you attach to your phone line? Not at all!

Many of today's modems have the ability to read caller ID information. With appropriate software on the computer, you can have a complete log of everyone that calls on your line, even when you're not home.

Obviously, if you can do it, others can, too.

For example, a cracker targets a computer system discovered during a wardialing exercise. He places several calls to the system, trying to guess passwords. Each time he calls, the computer reads the caller ID information from the line and records it. The third (or tenth, or whatever) time that the cracker calls with an incorrect password, the system stops accepting calls from that number and pages the administrator. The administrator takes a look at the system logs, and calls the police.

Could the cracker have gotten through by disabling caller ID? That depends on how secure the target system is. It may be set to reject all calls with caller ID blocked, or to stop accepting such calls after the n^{th} unsuccessful attempt.

To Sum Up...

There's a lot going on inside our telephone systems. At the phone company's end, all of the switching is being handled by computers, which means the system is both complex and vulnerable.

Despite the early history of phreaking as a lighthearted exercise for inquisitive youngsters, it blossomed into an expensive theft-of-service problem for telephone companies, and they responded with a very hard line in enforcement.

A do-it-yourselfer with a soldering iron and a handful of off-the-shelf parts can build a lot of useful and interesting projects that work over the telephone lines. As our privacy erodes in modern society, building illegal projects becomes harder to conceal. The phone company will neither know nor care if you build home remote-control devices using DTMF, or if you build phone ring amplifiers and line splitters. If, however, you manage to construct a box that gets you free phone calls or taps your neighbor's phone, it's only a matter of time before someone comes knocking at your door.

Enjoy phreaking. Enjoy playing with the phone system. But if you cross the line, you'd better watch your back.

Types of Boxes

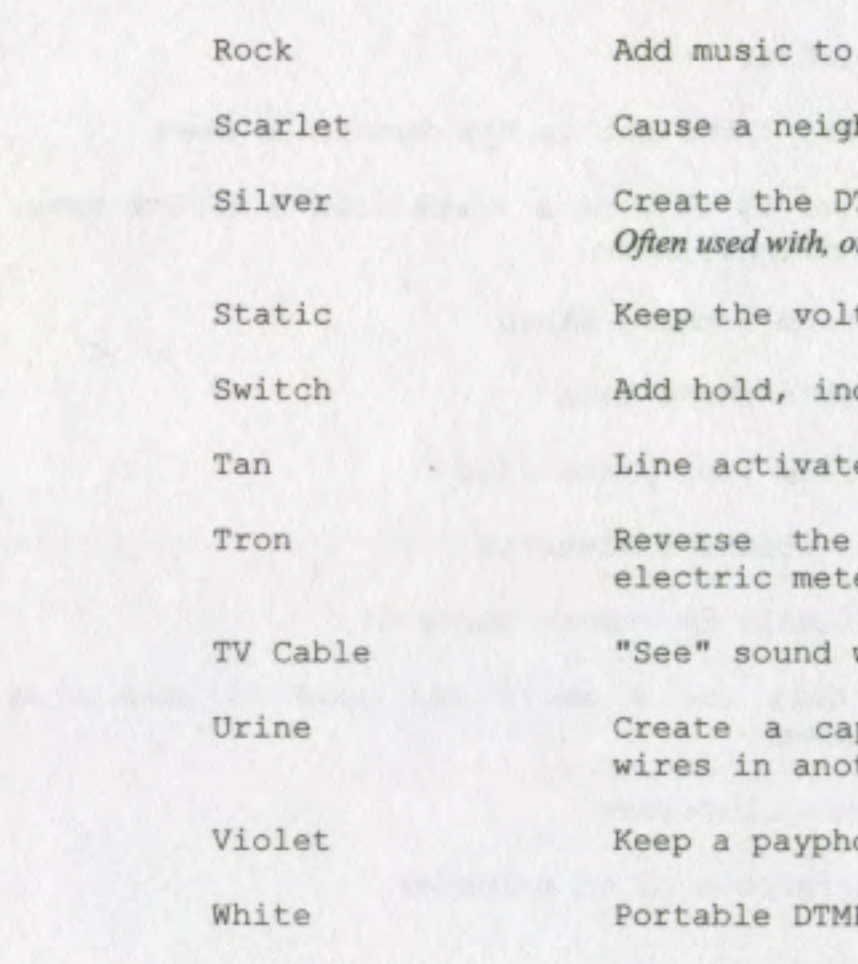
There are many different types of boxes available for phone phreaks. Most are illegal. Some are apocryphal (to the best of my knowledge, for example, nobody has ever built a blotto box). If you are really interested in phreaking, I'd suggest you get on the Web and start searching. There are schematics available for many of the boxes. Make sure you know how to use a soldering iron, and that you have a good attorney.

If you actually choose to use one, prepare for disappointment. Many of these boxes, if they ever did work, no longer do. If you build one, and it does work, you may have just set yourself up for some jail time (were you paying attention during the Bernie S story earlier in this article?).

Just to satiate your curiosity, though, here's a list of various boxes from the alt.2600/#hack FAQ, Beta 0.200. My commentary is added in *italics*.

Acrylic	Steal Three-Way-Calling, Call Waiting and programmable Call Forwarding on old 4-wire phone systems
Aqua	Drain the voltage of the FBI lock-in-trace/trap-trace.
Beige	Lineman's hand set. *Essentially, this is just a telephone with alligator clips on the end of the cord instead of a modular plug. Typically, they are all one unit (not a separate phone and handset), and the keypad often has the additional ABCD keys in addition to the numbers.*
Black	Allows the calling party to not be billed for the call placed. *The concept behind a black box is simple. It holds the voltage on the line just enough to establish a connection so that you can talk to your caller, but not enough to activate the billing circuits at the phone company.*
Blast	Phone microphone amplifier
Blotto	Supposedly shorts every phone out in the immediate area
Blue	Emulate a true operator by seizing a trunk with a 2600hz tone. *This is the box that made Captain Crunch famous.*
Brown	Create a party line from 2 phone lines
Bud	Tap into your neighbor's phone line
Chartreuse	Use the electricity from your phone line
Cheese	Connect two phones to create a diverter
Chrome	Manipulate traffic signals by remote control
Clear	A telephone pickup coil and a small amp used to make free calls on Fortress Phones
Color	Line activated telephone recorder
Copper	Cause crosstalk interference on an extender
Crimson	Hold button. *Typically, this will be rigged to mute your microphone, but not your speaker, so that you'll still be able to hear the other party, but they won't be able to hear you.*
Dark	Re-route outgoing or incoming calls to another phone
Dayglo	Connect to your neighbor's phone line
Diverter	Re-route outgoing or incoming calls to another phone
DLOC	Create a party line from 2 phone lines
Gold	Dial-out router
Green	Emulate the Coin Collect, Coin Return, and Ringback tones
Infinity	Remotely activated phone tap
Jack	Touch-Tone key pad
Light	In-use light. *These can actually be purchased at just about any home electronics store that sells phone equipment.*
Lunch	AM transmitter. *These are used for monitoring, or tapping, telephones. Any conversation taking place on the phone that the lunch box is attached to will be transmitted, and can be picked up on a normal AM radio from a remote location.*

Magenta	Connect a remote phone line to another remote phone line
Mauve	Phone tap without cutting into a line
Neon	External microphone
Noise	Create line noise
Olive	External ringer
Party	Create a party line from 2 phone lines
Pearl	Tone generator
Pink	Create a party line from 2 phone lines
Purple	Telephone hold button. *See "crimson box."*
Rainbow	Kill a trace by putting 120v into the phone line (joke)
Razz	Tap into your neighbor's phone
Red	Make free phone calls from pay phones by generating quarter tones. *This is what put Bernie S in jail.*
Rock	Add music to your phone line
Scarlet	Cause a neighbor's phone line to have poor reception
Silver	Create the DTMF tones for A, B, C and D. *Often used with, or built into, a beige box.*
Static	Keep the voltage on a phone line high
Switch	Add hold, indicator lights, conferencing, etc..
Tan	Line activated telephone recorder
Tron	Reverse the phase of power to your house, causing your electric meter to run slower
TV Cable	"See" sound waves on your TV
Urine	Create a capacitative disturbance between the ring and tip wires in another's telephone headset
Violet	Keep a payphone from hanging up
White	Portable DTMF keypad
Yellow	Add an extension phone



Blacklisted! 411 is written for the hands-on hobbyist, design engineer, technician, network admin. and experimenter. Hackers and professionals alike read it and love it.

Join the team and give us your support. We're accepting articles, photographs, design work for swag and our website, artwork and creative ideas.

A Brief Overview of DTMF

Anyone with enough interest in technology to read *Blacklisted 411!* has almost certainly become curious about the tones you hear when you press buttons on a telephone keypad. If you've played around with them trying to make music, you probably noticed that each button generates more than one tone, like a harmony.

The system is called DTMF, short for dual-tone multiplexed frequency. Your telephone keypad is wired as a grid with a set of different frequencies (tones), and pressing any key sends out the two frequencies connected to that key—one for its column and one for its row. The frequencies are:

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	*1*	ABC *2*	DEF *3*	*A*
770 Hz	GHI *4*	JKL *5*	MNO *6*	*B*
852 Hz	PRS *7*	TUV *8*	WXY *9*	*C*
941 Hz	*	oper *0*	#	*D*

So if you press the 0 on your telephone keypad, you'll transmit a mix of 941 Hz and 1336 Hz. The A, B, C, and D buttons don't appear on normal telephones, but are available on test sets used by telephone linemen. If you have a use for them, build a "silver box" (see below).

Why send two tones per key instead of one? It prevents the system from accidentally picking up background noise and interpreting it as dialing tones.

The specific frequencies used in DTMF may look like a bizarre mix of random numbers, but there's a method to the madness. All of these frequencies can be generated by dividing down the output from a 3.579545 MHz crystal. Crystals are available in a variety of standard frequencies, and this is one of them. The eight frequencies required for DTMF are actually generated by dividing down the frequency of the crystal.

For example, take a look at the 697 Hz required for the first row (1, 2, 3, A). This isn't really 697 Hz, it's 1/5135th of the crystal frequency (3,579,545 Hz ÷ 5,135 = 697.0876339 Hz). That's not exactly 697, but it doesn't matter. What matters is that the DTMF generator and decoder use the same pattern to generate and read the tones.

It's easy to build a set of dividers and make your own DTMF generator, but there are so many devices available these days that generate DTMF that it just isn't worth the trouble. Telephone auto-dialers, PDAs, and modems all generate DTMF, not to mention the lowly touch-tone phone itself.

Decoding (interpreting) the DTMF tones is more complex. There are many DTMF decoder chips available, which are used in all kinds of devices, from telephone-controlled thermostats to home security systems.

You can also purchase standalone DTMF devices with computer interfaces. As an example, the DTMFLCD-2 from DSchmidt Technologies can be connected to a telephone line, and its 2-line LCD will show any numbers dialed on that line. A pushbutton on the board will transmit its entire memory over an RS-232 port to a computer.

MoTron's XC-2 bidirectional ASCII to DTMF converter also uses an RS-232 (serial) connection, and it operates in realtime, allowing you to receive and send DTMF signals from a computer program.

You can find many more of these with a careful Google or AltaVista search.

Gary Robson has been programming computers since the early '70s. He has worked on everything from the Altair to the Cray I in dozens of programming languages, and written a multi-user operating system for a 70's minicomputer. He has also designed seven semi-custom chips, and written eight books and a stack of computer manuals. Many of his 150+ magazine and newspaper articles are available on his Web site at www.robson.org/gary