SPECIAL RED BOX ISSUE
2600
THE HACKER QUARTERLY
VOLUME THIRTEEN, NUMBER ONE! SPRING 1996
$4.50 ($5.50 IN CANADA)
ELITE
Our Nation's Youth Run Amok
Corporations Living In Terror
0 74470 83158 7 61
Payphones of the Planet
UKRAINE
A cheerful sight in Kiev.
Ed Fisher
MOLDOVA
An old phone that runs on Getones (16 per US dollar).
Tom Mele
TRANS DNEISTRE
A little-known breakaway republic between the Ukraine and Moldova.
Tom Mele
ROMANIA
The town of Sacsava where, judging by the chairs, there is a vandalism problem. Works on rare 20 lei coins which are worth about a penny.
Tom Mele
COME AND VISIT OUR WEB SITE AND SEE OUR VAST ARRAY OF PAYPHONE PHOTOS THAT WE'VE COMPILED - http://www.2600.com

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout
Scott Skinner

Cover Design
Phriend2, Shawn West, GTE

Office Manager
Tampruf

"It's not a computer crime to break into someone's system and just look around."
- Susan Lloyd, a spokesperson for the FBI's Washington DC field office
as quoted in the March 10, 1996 Boston Herald.

Writers: Billsf, Blue Whale, Commander Crash, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Kingpin, Knight Lightning, NC-23, Peter Rabbit, David Ruderman, Silent Switchman, Thee Joker, Mr. Upsetter, Voyager, Dr. Williams.

Network Operations: Max-q, Phiber Optik.

Voice Mail: Neon Samurai.

Webmasters: Bloot, Corp.

Inspirational Music: Raekwon and the Wu Tang Clan, Trancemode Express 1.01, Negativland (Sex Dirt).

Shout Outs: Veggie, Freqout, Sciri, Mark0, Zeed, Refugium.

SEE HERE

caught in the web	4
tap alert	6
a page of revenge	9
unshredding the evidence	10
confessions of a beige boxer	12
macs at ease	17
sharp cash trix	18
hacking doors	20
hacking caller id boxes	22
the alaskan phone system	24
avoiding suspicion	26
letters	28
motorola cellular guide	38
2600 marketplace	48
hackers '95 review	53

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.,
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1996 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1995 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677**

Caught in the Web

How do mere individuals stand up to modern day injustices? What can we do to get the word out when the system has failed us and the most important thing is to find others in a similar situation who may be able to help out?

Throughout history, this kind of a challenge has been insurmountable to most. But the times are changing very rapidly. And the one thing individuals have over bloated bureaucracies and huge corporations is the ability to adapt–quickly.

We've learned over the past few years that the Internet is probably the most effective means of worldwide communication in the history of humanity. When word of something needs to be gotten out, all that is required is access and the world can know within seconds. Now, with the growing popularity of the World Wide Web, anyone with the necessary access has the ability to become their own information disseminator, where people from around the world actually come to *you* for information of any sort. And with the growing number and abilities of search engines, people anywhere can find you based on the information you provide.

This kind of power is unprecedented in the hands of solitary citizens. It's precisely because of the hacker mentality responsible for creating this medium that the authorities are in such a panic. This explains the rush to control everything from content to accessibility. But the powermongers are far too late this time. The box is open and the rules forever changed. It no longer matters what those who don't realize this choose to do. They are doomed to failure. What *is* important, though, is for the rest of us to maximize the potential of this technology while it is still in relative infancy.

As consumers, we no longer have to wait for someone to speak on our behalf. With the net, we can speak for ourselves and be guaranteed an audience and, ultimately, a reaction of some sort. In our last issue, we mentioned a problem we were having with an Internet Service Provider (PSI) who had promised us the ability to use 56k data over voice over an ISDN line. When it was finally realized that they didn't offer this service, the contracts had already been signed. Since it was a verbal agreement, there was little recourse and more than a few people (including PSI) believed that we would be held to the contract. Several years ago, that's probably what would have happened. However, by posting our account of the story on our web site (as well as Usenet newsgroups and other Internet forums), we were able to make contact with scores of other people who had had similar run-ins. We used these contacts to pool our resources. When we went one step further and posted *sound files* of telephone conversations where PSI reps were clearly heard saying they supported the service we wanted, there was no way the issue could be avoided. PSI reacted, at first by threatening to sue us. That proved to be an even bigger mistake since individuals on the net are particularly averse to legal threats by large corporations. Now newspapers were actually starting to take an interest in the case. PSI really had no choice. Shortly afterwards and without fanfare, they sent us a full refund. We believe they learned a valuable lesson and we have no hard feelings towards them. What happened *was* an honest mistake. It was their reaction that made them look bad and pressure from so many people that ultimately made them give in. We didn't have to sue them or waste an inordinate amount of time. All we had to do was speak up.

The same kind of power in a different kind of way was felt with the Bernie S. case, which we have been involved in for over a year now. In January of this year, the United States Secret Service managed to have Bernie S. locked up yet again for last year's charge of possessing technology which *could be* used to commit fraud.

By being arrested last year, Bernie technically violated probation for an offense committed several years ago in a small Pennsylvania town.

Because it was such a minor incident–equal in seriousness to "insulting the flag"–nobody could ever have been expected to go to prison for it. However, the Secret Service made it their business to portray Bernie S. as a major threat to society. The judge, along with the probation officer and prosecutor who had previously said the case was of little significance, were heavily influenced by having the Secret Service come to their small town. Based on this image, he was put back in prison with murderers, rapists, and death row inmates. He was considered especially dangerous because the judge had set such a high bail–$250,000. This, despite the fact that he was obviously not a flight risk, having shown up for numerous hearings where he could have been imprisoned on the spot. After several weeks, the judge conceded that the bail was too high and had it lowered–to $100,000. In early March, the judge sentenced Bernie S. to 6-24 months, double the sentence of someone convicted of attempted murder in the same district. Under the law, he should be released on May 30, but the Secret Service may attempt to impose even more suffering on him by seeking to have that extended.

Throughout this entire escapade, the Secret Service has said in every court appearance that some of the most disturbing evidence they found in Bernie's possession was information on the Secret Service themselves–frequencies, addresses, codenames, and pictures that had been on a television show. Special Agent Thomas Varney has said under oath that any reasonable person would view this evidence as proof that Bernie S. was a threat to society. And this assumption was accepted–by law enforcement, the legal system, the media, and, ultimately, the public.

We decided to check into this. We found that all of this information was completely legal and available to the public. And, to emphasize the point, *we* made all of it (and more) available on our web page. The reaction was phenomenal–an average of around 1,000 visitors a day. And the irony was delightful–because the Secret Service overreacted at *one* person's possession of this material, *millions* of people around the world now had easy access to it. It may not have been enough to get Bernie S. freed, but it was enough to get his story into newspapers around the world and have the real issues of the case discussed at long last. We hope this new publicity will cause some heads to roll at the Secret Service and prevent this kind of thing from happening again to more of us. Regardless, Bernie S. has gained

Special Agent Thomas Varney

thousands of friends who will be with him in spirit until this ordeal ends.

What we've done with the net is what the net has been designed for freedom of speech and instant access to relevant material. Being an already existing magazine gives us an advantage, but not a tremendous one. Any person could have done what we did with basic connectivity and strength of convictions. Individuals will continue to use the net to outmaneuver bulky corporations, speak out against bureaucratic and repressive regimes, and take over where the mainstream media has failed us. And those who underestimate this power are in for a very rude awakening.

You can write to Bernie S. and help him get through the days. If you include a return address, he will write back. Only letters and reading materials are allowed–be sure to label your letter or package as "Reading Materials" to avoid having them sent back. All letters and packages will be inspected and read by [illegible] officials. The address is: Ed Cummings, [illegible] County Prison, D-13, 1730 South [illegible] Road, Doylestown, PA 18901. You can [illegible] bernies@2600.com and it will be forwarded.

TAP ALERT

by No comment
and Crash Test Idiot

"Who's the operator?", an anonymous conference voice says. "I am," booms Joe Hacker with confidence. Suddenly, Joe notices his phone goes dead and the tap-alert light has gone off! Joe, startled only momentarily, pushes the red override button on his phone, announces, "Gotta go," pulls the phone cord swiftly from the terminal box and is off safely to his next clandestine operation of the night.

Fiction scenario? Yes. Probable? Yes again... with the help of a tap-alert device described in this article.

The tap-alert device is useful in many ways. How about those times when a parent or roommate dropped onto the line and listened while you were having some salatious conversation not meant for their ears. Wouldn't it have been nice to have known the moment they dropped in? Or perhaps you are wary that your phone line is tapped, but how can you tell for sure? The tap-alert device will detect lower grade taps (not the non-parasitic or the electronic taps at the switch).

Assembly

No project board is required for the following assembly and the final product will be small enough to fit on the average thumb-nail.

First, cut the cathode (the short lead) on the LED as short as you can handle soldering to. Next, cut the cathode (the side with the black band) on the zener diode approximately the same length as the lead you just cut on the LED. Now, solder the LED to the zener diode by soldering the cut lead on the zener to the cut lead on the LED. Next, locate the plus and minus side of the bridge rectifier, this is the side that your zener/LED unit will be soldered to. Solder the zener lead to the minus pin on the bridge rectifier, and the remaining lead of the LED to the plus pin. On the opposite side of the bridge rectifier that you just soldered to are the two pins that you must solder the push-button switch to. Pick one switch lead and solder it to one of the two remaining rectifier pins, then solder the other switch lead to the other remaining rectifier pin. You have now completed assembly of the tap-blocking device... we recommend that you now go drink some Hacker Pschorr Oktoberfest or, if you're real manly, a bottle of Cisco.

Installing the Device into a Phone

If you don't already have a phone to work with, it is strongly suggested that you purchase the Model 2-9220 GE telephone from K-Mart. It goes for $18.99 and comes in many colors (we prefer black). Unlike many phones on the market, the 2-9220 contains all of its electronics in the handset (with two alligator clips, it makes a very nice beige box). Internally a lithium battery keeps stored numbers active in memory and there is plenty of space to add switches, boxes, devices, etc.

Open your phone and locate the red (ring) and green (tip) wires. (If you are opening the 2-9220, the trick is to pull out the Hi-Low-Off and Pulse-Tone slide switches first... they'll pull straight out. Then remove the small plastic plate which was underneath the two buttons by prying it up. Underneath this plate is the well hidden Japanese screw, which, if you haven't read this yet, you are extremely pissed off at. The ring and tip wires will be going into the jack on the mouthpiece end.) Cut the ring wire in two. Solder one ring wire to one of the pins on the push-button side of the tap-alert and the other ring wire to the other pin on the push-button side. If you have a special location in mind inside the phone, jumper wires may be necessary. Plug the phone in and see if the LED lights. If it doesn't light, one of two things has happened:

1. Your phone line is already tapped.
2. You fucked up!

Case 2: GOTO liquor store, get more beer, start over.

Case 1: Disconnect all of your phones, and connect your phone line to an electric power cord (from an old blender or something) and plug it into the 120v outlet... this should do the trick. If (NO_DIALTONE) laugh (EXTREMELY_HARD).

To test the circuit, pick up your new phone, make sure the LED is lit, then pick up a second phone on the same line. If the LED goes out, it is working properly, and you will hear nothing on your special phone. Override the tap-alert by pressing the push-button; your phone will now work as a normal phone allowing you to once again hear and speak on the line.

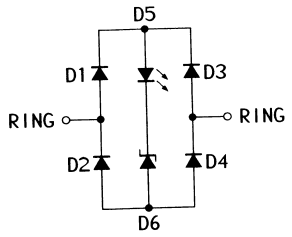
If everything is working OK at this point, you should find a way to mount the tap-alert device inside the phone. Our people have found that drilling two small holes in the bottom of the 2-9220 allows the switch and LED to be pushed through and then screwed down in place with the locking nut from the switch. This method is not only simple, but looks good, and the placement of the LED works out great for an illumination source in those dark alleys (writing is often important in weird places).

Final Notes

If tap-alert devices are in parallel they will not work on each other. In other words, they will not detect when another phone with the device is present on the line. If two or more devices are in series, you will not be able to use your phone at all.

You may find that you can sell these special phones to your friends at school for a nice price. Your friends will appreciate it and so will you, because any calls to your friends will be safe from prying ears!

Many thanks to the little purple guys with yellow spots for their help with the tuning forks. We wouldn't have hit 2600 hertz without them.

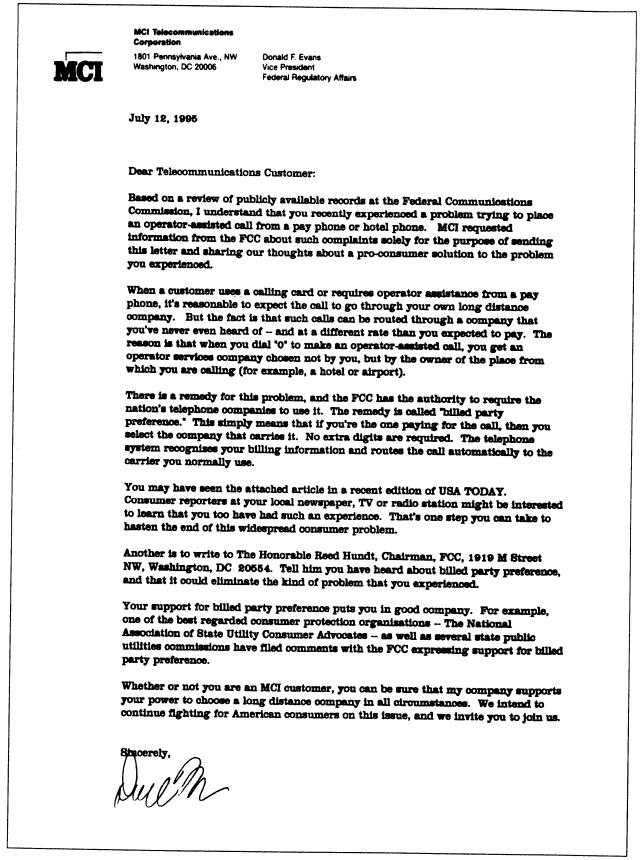


Parts List: (Radio Shack of course)

SYMBOL	CAT. #	PRICE	DESCRIPTION
D6	276-564	0.99	15v Zener Diode
	275-1571	2.39	SPST Momentary Pushbutton Switch
D5	276-041A	0.99	Light Emitting Diode
D1-D4	276-1161A	0.99	Bridge Rectifier

Optional:
Model 2-9920 GE Telephone from K-Mart @ $18.99

Total cost: $24.35 + tax



MCI Telecommunications Corporation

MCI

1801 Pennsylvania Ave., NW
Washington, DC 20006

Donald F. Evans
Vice President
Federal Regulatory Affairs

July 12, 1995

Dear Telecommunications Customer:

Based on a review of publicly available records at the Federal Communications Commission, I understand that you recently experienced a problem trying to place an operator-assisted call from a pay phone or hotel phone. MCI requested information from the FCC about such complaints solely for the purpose of sending this letter and sharing our thoughts about a pro-consumer solution to the problem you experienced.

When a customer uses a calling card or requires operator assistance from a pay phone, it's reasonable to expect the call to go through your own long distance company. But the fact is that such calls can be routed through a company that you've never even heard of -- and at a different rate than you expected to pay. The reason is that when you dial "0" to make an operator-assisted call, you get an operator services company chosen not by you, but by the owner of the place from which you are calling (for example, a hotel or airport).

There is a remedy for this problem, and the FCC has the authority to require the nation's telephone companies to use it. The remedy is called "billed party preference." This simply means that if you're the one paying for the call, then you select the company that carries it. No extra digits are required. The telephone system recognizes your billing information and routes the call automatically to the carrier you normally use.

You may have seen the attached article in a recent edition of USA TODAY. Consumer reporters at your local newspaper, TV or radio station might be interested to learn that you too have had such an experience. That's one step you can take to hasten the end of this widespread consumer problem.

Another is to write to The Honorable Reed Hundt, Chairman, FCC, 1919 M Street NW, Washington, DC 20554. Tell him you have heard about billed party preference, and that it could eliminate the kind of problem that you experienced.

Your support for billed party preference puts you in good company. For example, one of the best regarded consumer protection organizations -- The National Association of State Utility Consumer Advocates -- as well as several state public utilities commissions have filed comments with the FCC expressing support for billed party preference.

Whether or not you are an MCI customer, you can be sure that my company supports your power to choose a long distance company in all circumstances. We intend to continue fighting for American consumers on this issue, and we invite you to join us.

Sincerely,

MCI GETS US AGAIN! You would think filing a complaint with the FCC would protect you from those pesky MCI telemarketers. Guess again! Every time you complain about a phone company, you wind up on a list that phone companies have access to! And they get so angry when we find *their* lists.

A PAGE OF REVENGE

by Big Lou

You've seen the titles and heard of the results. However, nothing, I mean *nothing* can compare to the chill down your victim's spine as he/she is blasted for hours or even days by the ever annoying sound of "*ring... ring... Hello, yes this is Dr. Smith, did you page me?*" only to have it happen 45 seconds later "*ring... ring... Hello, yes this is ACE Gravel and Dirt, did you page me?*". So, Walmart pissed you off? Wanna lock up their phones for three or four days? Ex-wife still on your back? The local cops don't like you because you molested your laptop?

Imagine a metropolitan area like New York and how many people there are in it with digital pagers. Imagine only 10 percent of that pager population being paged with your favorite enemy's home or business number. Well folks, imagine no more. The concept is real and it works very well. Now, first, a word of caution. Just like a handgun has potentially deadly ramifications, a program to page at will and en masse can also prove equally devastating. This retribution method should be reserved for only the most serious of paybacks and should be used wisely.

The method for this high tech but very simple method of payback requires a working knowledge of Basic, Quick Basic, or even Assembly (if you're that good), a computer with a modem (laptop preferred), and a small list of pager numbers. First, the program is just a simple dialer that will take a list of pager exchanges (345-XXXX) and randomize the last four digits, dial the resulting number, wait for X seconds, enter the victim's (123-4567), and the # sign, and hang up. Second it is very important to randomize the last four digits of the pager so as to not develop a pattern. It doesn't hurt to sprinkle in a few other numbers at random like your local Radio Shack or Skin Head Society.

A typical menu for the paging program should look like this:

Enter Victim's Number:	**234-6565**
Enter Number of Pages:	**250**
Enter Start Time:	**22:30**
End Time:	**23:50**
Use Lookup Table(Y/N):	**Y**
Enter Exchange:	**XXX***
Enter Randomize Seed:	**6**

***Leave blank if using lookup table, otherwise enter an exchange)**

A progress screen should show the pager dialed, total dials, victim's number, elapsed time, and remaining pages. You may also want to use some of your modem's more sophisticated features like tone detection to speed up the process.

Pager numbers are easy to come by. Almost anyone we know carries them. Determining what numbers to call is equally easy. For instance, pager number 345-1234 can be used as a starting point to search for the exchange's range. Typically a pager company will buy blocks of numbers like 345-1000 thru 345-3000. Determining the range is as simple as dialing a starting number until you hear the classical "Please enter your numeric message..." or you hear a "beep". Chances are that if you cannot figure out how to do this, you are probably not smart enough to figure out the program.

It is best to use several paging companies in a lookup list for the program to avoid repeatedly abusing the same one. If you use five companies and paged the victim 100 times with each, the paging company would not become suspicious considering the thousands of pages cycled on a daily basis, and your victim will have been annoyed 500 times. The best method is to use small doses - say 50 or so pages every three or so hours. This could be built into the program since Quick Basic is very flexible. As a safety feature, compile your program and password in case the victim points the finger at you.

Happy Revenge.

UNSHREDDING THE EVIDENCE

by Datum Fluvius

The key to reconstructing shredded documents is to sort the shreds prior to paste-up. There are so many differences in the angle of each shred, what text each document contained, which color its paper was, and which weight, that the identification of individual documents by their shreds is fairly simple. It is, of course, tedious. It also takes practice. But once the shreds have been properly classified, only a few pages exist in each little group of sorted shreds. These will submit easily to careful paste-up and reconstruction, since only one or two hundred shreds exist in a three page group of average size. (This article assumes you are not dealing with cross-cut, chipped documents, or ashes, but with "paper spaghetti".) A three page group only takes an hour or two to completely reconstruct. The key to paste-up, in turn, is proper and systematic comparison of each and every shred against as many others as seem to fit. This has to be done systematically in order to avoid re-comparisons, and to identify patterns in the reconstructed portions.

The Procedure

Place the sorted shreds into a "raw" area to one side, and place the first shred on the paste-up board, anywhere. (Tape it down with masking tape, top and bottom. Masking tape pulls back off the board easier than clear tape.) Next, pick up the second shred, and place it alongside the first in the same orientation. Compare it against one side, then the other. If it matches, tape it down, and if it does not, tape it down a little farther away, perhaps an inch or so away, parallel to the first. Repeat, repeat, repeat. Uncrook your back every little while. When you compare the shreds in this manner, you are limiting the number of comparisons to a fixed, predictable number. If you run out of room to paste down new strips, grab a fresh paste-up board and keep it handy or prepare to recycle the "no-match" pile which will develop opposite the "raw" pile. But that adds steps, and time, to your task.

Inspect the reconstructed document strips as they grow. Read what develops to guess which shreds match the open edges. The widening strips are compared as if they were shreds, and joined whenever possible. If two matching strips coexist on a paste-up board but remain unjoined, they retard your further comparisons since two of the available edges will not match any free shreds. That also wastes time.

When a few documents have been completed, transparent packing tape can be used to fuse them, or care can be taken to tape only the tops and bottoms of each document with masking tape. That way, when the shreds are cut free of their tape, they are just a bunch of loose shreds again, ready for disposal. Clear contact paper has been used, but it can ruin documents whose shreds will not lay flat anymore due to dampness or lengthy storage. Tape is easier to control than contact paper, but both media will pull shreds up with their static electric charges unless you ground them. Fully taped documents are much easier to store and preserve, if you need the original. If you want the data, invest in photocopies. Press completed documents between plastic (overhead projector) sheets to keep the copier's glass clean and to align the shreds.

One thing to remember is that businesses and governments use forms whenever possible to save cost. These can be roadmaps to incomplete reconstructed documents, and are invaluable to have prior to beginning a project. If need be, clear plastic can be traced over a completed form to outline just the form boxes. When laid over the partial document, these give a clue to what information is missing, and what shred patterns to look for to complete it.

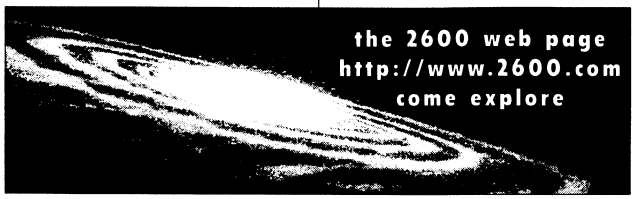
Obviously there are many uses for such a simple technique, even in this "information age" of the brave new world order. But it isn't foolproof. You may see coffee grounds mixed in with the bag, used cat litter, and even lunch waste mixed with the shreds. The targets who do that are probably well aware of this reconstruction technique, and will expect your forays into their dumpster. Their other main defense, subterfuge and decoy, is even more effective. They simply increase the shred volume to include everything available, and overflow the sorting capacity of the reconstructionist. Or they salt the real shredded information with errors and omissions, even fake derogatory documents, to elicit a revealing admission from the snoop.

Burning is best, but is not legal in many urban areas. Even when it's legal, it's expensive; it requires safety equipment and personnel supervising every moment of the burn. The military, however, prefers fire and flushing to any alternative. When it absolutely, positively has to disappear overnight, fire and water should be your choice, too.

Extra Assignment
for the Artful Programmer

Who needs this headache and tedium? Anyone who needs the data would have to give up their job or their social life to have time for reconstruction! Why not let a computer do it?

Of course, feeding the data in is now easy with a flatbed scanner, and can be easier if you have thin sheets of clear, stiff plastic to sandwich/mash the shreds down. A programmer would then want to compare the edges of the images in the computer's memory. The basic idea is to turn the edge of a shred image into a "word" according to its pixel pattern. This "word" would then be sorted with the other "words" and the results would indicate which images are matches. Only a small portion of each edge would be compared, since a close match in one area is a good indicator for the whole. A sample size might be three inches in length, starting one inch down from the top of each shred. Reconstruction would be accomplished by drawing in the images in their relative positions and printing the result, or passing the image to an OCR routine for translation into completed ASCII text pages. Have fun, but publish your results!



confessions of a beige boxer

by RedBoxChiliPepper

Here's what happened when I took beige boxing just a little too far while living in Celina, Ohio (population 8000). I started out like most people, just finding a telco box or a neighbor's box on the side of their house, plugging in my phone and dialing away at the 900 numbers and harassing operators. But that got really old after awhile. So I set up sort of a permanent beige box on my next door neighbor's line. I hooked a line into their box, ran it under the siding to make it invisible, down next to a basement window and into the ground. From there I dug a trench in the ground about 3 inches deep from their box to my box and hooked the wire into my box, to the yellow and black wires.

Now I could use their line to call BBSes around the world for free! I decided not to make any direct long distance calls so they wouldn't start investigating and find the extra line going into the ground. So I only third-number billed and used calling cards from their line and tried as best as I could not to annoy the operators too badly.

So you see, it started out sort of innocently, but then I began to eavesdrop on a lot of my neighbors' conversations. After awhile the conversations got sort of boring so I hooked up my two-line phone to both of the lines and started conferencing total strangers onto their line while they were in the middle of a conversation, which caused quite a bit of confusion, especially when I hooked them up to overseas people. Then to make things worse, I'd pop in and say in a deep voice, "Please deposit 25 cents!"

Pretty soon, my neighbors got to be too boring for me. I mean, they reacted to my pranks on their line the exact same way every time and their conversations without me were totally boring, hardly worth listening to. So I went to my *other* next door neighbor's house one night to check out the possibilities on their line and ended up doing the same thing to their line only running the line in my basement window and upstairs to the spare bedroom where the other two lines were hooked up.

Since I only had one conference phone that didn't work very well to begin with, I decided to build a simple switchboard on top of my desk. It ended up being a piece of sheet metal with five two-position switches on it. Switch 1 was my own phone line, switch 2 was the first neighbor's line, and switch 3 was the other neighbor's line. Also, each switch had a light above it to indicate In-Use. Normally, the switches would be in the "off" position. If I wanted to use a line, I flipped it on and hit the speakerphone button on my desk phone or used my official Bell operator headset. (Actually, one of those cheap headsets that you buy from Radio Shack but hey, I drew a Bell symbol on it, okay?)

So now with their two lines and my own three-way calling line, I had a total of four phone lines to play with. The new neighbor's calls proved to be much more interesting that the others. They had a son and teenaged daughter who liked to talk on the phone a lot. And when their conversations *did* get a little boring, I helped them out by patching my Sound Blaster card directly into my switchboard so I could add sound effects, movie clips, and rude noises to their conversation. Lemme tell you, their reaction to this was fantasic. Each kid would blame it on the other and when I did it to either of the parents, they would yell at their kids to quit playing around on the phone.

Now I was happy and had plenty of things to do with my spare time which I had a lot of. I'd been using various calling cards from both of their lines late at night to call bulletin boards for about a month and a half and still Telco Security hadn't called them up questioning them about anything. I thought maybe they were just trying to build a case against them and were holding out for more fraud. In any case, I decided to keep close tabs on their phone calls in case AT&T called them questioning anything so I'd have advance warning to sneak back over and disconnect their lines. To help with this I bought a few of those cool Radio Shack deals that automatically record all incoming and outgoing calls on your lines so I could keep up with their phone calls while I was at work.

Then something horrible happened. Most of my favorite phone companies around the United States figured out that they were being ripped off big time by people who order calling cards with personalized pin numbers for other people. This security flaw was my major source of calling cards and now they had set it up so if you wanted to do this you needed the victim's social security number. Getting their social security number wasn't a super hard task but it sure was a pain in the ass to have to do that every time I wanted a new calling card. They were making things *hard* for me. I only had about twenty cards left and my cards went dead pretty quick lately because of my extensive international calling. I could third-number bill everything but if you've ever tried to do that for a BBS call you know that it's a pain in the ass to get it right.

That's when I went over to the window and looked across the street. I saw a little shop with a pay phone next to it and a guy in a suit talking on the pay phone. Since car phones weren't a big thing yet in this little town, the few yuppies that there were usually stopped by this phone to make their important phone calls. And of course they preferred credit cards to pocket change. A plan started to form in my head. Of course I couldn't run a phone wire underneath the street because the police probably wouldn't be too happy if I used a jack hammer. So....

That night at 3:00 a.m. I got on my cellular phone and dialed the direct line to the Celina police. I explained to them that I had just seen a few kids jump the fence to the boatyard by my house and break into the office. I listened in on my scanner as the dispatcher sent all available units to the boatyard. (All two of them, eh?) I was ready when I heard that and I ran across the street to the pay phone. I had done this a million times before but usually it was in a secluded area and there wasn't such time pressure.

I pulled out my specially cut alan wrench and opened the bottom panel of the pay phone. I set the base unit of my cordless phone there in the bottom and clipped the wires into the pay phone line. Then I plugged the AC cord into the receptacle. (Most phones have these in the bottom panel to power the light on top of the phone.) I wrapped a garbage bag around the phone to protect it from water damage and the evil GTE linemen and put the panel back on. The whole thing took less than four minutes. Meanwhile, the brutal Celina police force was crawling around the boatyard with flashlights, looking underneath all the boats for these hardened criminal kids. They never found them, though.

I went back home and picked up my cordless handset. I turned it on and dialed the local Wal Mart. A recording came on, telling me to deposit twenty-five cents. So I called a number a little further away. I called Mann's Chinese Theater in Hollywood, California and was asked to deposit $2.25. I tried red boxing the coins in but I think the reception was screwing it up. I ended up going through a live operator who put the call through for me.

I decided I'd better get this fixed. I didn't need GTE dropping a trouble card on my pay phone and discovering my cordless base unit in there. So I took the handset apart and hard-wired it into my switch-

board. I replaced the rechargable batteries with an AC line and built a red box on the switchboard that was hooked directly into the cordless phone's microphone. Then I boosted the antenna by hooking it to the old TV antenna on top of my house. This was getting to be pretty fun!

The next morning I had the alarm set for 10:00 a.m. so I could sit at my window and wait for yuppies to use my pay phone. My first customer came at 10:18, a little kid who used a copper slug. Damn him, I should call his parents for this. Anyway, I came on and impersonated the operator, telling him he was in big trouble and if he didn't put in a real fifty cents immediately I would come over there and rip that St. Louis Cardinals hat right off his head and hit him with it. He hung up, looked nervously around and quickly disappeared into the alley.

At 10:57, while I was in the middle of my Frosted Flakes breakfast, the neighborhood mailman stopped by to use the phone. I looked through my binoculars and saw him punch a "zero" first. I was so happy, milk came out of my nose. When he tried to enter his calling card number, I interfered by hitting some extra numbers. He tried it again and I messed him up again. Then I heard the AT&T recording, "Please hold for operator assistance." An operator came on and asked for his card number. He read it off as I wrote it down. I was so grateful to him that I didn't even harass him during his call.

I got three calling card numbers that day. The next day I got a little more creative. I got on the pay phone line and dialed a phone company number that just sat there, blank. When a guy picked up the phone, I played a recording of a dial tone into the phone. When he began dialing I stopped the recording and when he finished dialing I played the recording, "AT&T! Please enter your calling card number now...." He began to enter his calling card and I came on and talked to him in a really annoying nasal voice.

Me: "AT&T, what seems to be the problem?"

Him: "I'm just using my calling card."

Me: "Okay, what's your calling card number?"

Him: [gives me his number]

Me: "That card's not going through here. Do you have another card?"

Him: "Uh... yeah, I have my AT&T calling card."

Me: "Okay, let's try that one."

Him: [gives me his number]

Me: "Okay... yep, that one's okay. Here's your call and fuck you for using AT&T!"

I had no idea what number he had dialed in the first place so I got an old recording of Tina, the phone sex operator and put it on the line. "Hi, this is Tina.... Are you ready for a hot time?" The poor guy tried to talk to her and finally realized that it was a recording and hung up. I watched him walk down the street and use the phone booth a few blocks away.

A few days later I bought one of those touch tone decoders. It had an LCD display that showed me exactly what digits were being dialed on any line I hooked it up to. I hooked this into my switchboard and not only was it easier for me to get calling cards, I could see exactly who my neighbors were calling. I started keeping files on the neighbors and who they called. Oh, did I mention that I have no life? You may have figured that out already.

Two months later not much had changed. I still had the same setup and was working on expanding it. I added ten more switches to it for extra lines and started wandering around my neighbors' yards late at night, looking for new possibilities. I also hooked an old bulky cellular phone into my setup so I could connect neighbors to the cellular roaming network and I added another phone so I could listen in on more than one line at a time without them hearing each other.

The little green telco box on our block was very well secluded. It sat near some bushes in the alley behind my house, about three houses over. The only problem with it was that it was sitting right underneath a bright street light. I eventually took care of the street light with my pump pellet rifle. It took an hour's worth of patience to finally hit it just right, but I finally turned it off. That being accomplished, I went to the hardware store and bought a cable. This nifty little cable had 50 separate wires inside of it, enough to hook 25 phones to.

When dark finally came, I grabbed my back pack and hiked over to the telco box. I opened it and started hooking my phone, dialing 1-800-MY-ANI-IS on every set of terminals in there and taking notes of what was what. I was going to go for choice and pick my least favorite neighbors but decided that that would take forever so I hooked up to the first 50 terminals (on the backside, so telco wouldn't notice) and put the box back together. I hoped I hadn't hooked up one of my neighbor's that I already had hooked to my house cause it'd suck to waste a whole line like that.

Now the hard part. I dug a trench a few inches deep from the telco box, down the alley, into my own back yard, then through the yard and into that little hole underneath my basement window. It took me over three hours to complete all of this but when I was finished there wasn't a trace that anything strange was going on. I had to cut a hole in the floor to get the cable upstairs to my switchboard and found myself hoping that my landlord wouldn't drop by anytime soon. He got testy when I drilled holes in his property. So I got that far and went to bed. I couldn't really do much more cause I needed to go to Radio Shack and buy some more switches and a larger piece of sheet metal.

Another month passed. I discovered that I had access to the phones in random houses as far away as two blocks *and* another pay phone. I'd hooked about every sound device I owned into the switchboard, including my computer's Sound Blaster, tape deck, CD player, voice changer, and echo machine. I had the ability to hook 28 lines up to a single phone, creating a monster party line of confused people and my calling card list had reached almost 100 numbers. That's the most I'd ever had all at once.

Then on Friday the power bill arrived. It was an outrageous amount, probably because I had a habit of turning on heaters while opening windows, leaving lights and my computer on all day, etc. It didn't seem fair that I should have to pay so much to them, especially since I stopped going to work as often so I could sit at home and play operator. My neighbors had a receptacle on their deck that they used to plug in the bug lamp and sometimes a radio. I figured if they weren't using it all that much, I'd take advantage of that.

That night I dug down about a foot where the plug was and cut open a section of the plastic pipe to expose their wires. Carefully using rubber gloves and pliers, I managed to splice my orange 100 foot extension cord into their line. I ran that underground to my basement window and start plugging my large appliances in. The refrigerator, space heater, microwave, and electric oven. So I walked over to their power meter and peered in to the glass bubble and noticed the disk was spinning quite rapidly. Oh well. They owned a pool and deck. Obviously they could afford a little more electricity.

I figured that if they were rich, they could probably afford cable TV and I noticed that their cable line was conveniently located next to their phone box. So the day after that I got free cable. A few weeks later, free cable alone just wasn't enough for me. I wanted to be able to control what my neighbors watched. So I hooked up sort of a loop so that their cable line was coming to my house before it got to them. Then I built this little switchboard

next to my phone switchboard that consisted of a few TV monitors, a VCR, a video camera, and some video mixing devices.

By the time I was through hooking it all up, I had the power to change their channels, make them watch my home video collection, or wipe their TV show off the air with a variety of 37 different wiping techniques! I also had a monitor set up showing me exactly what they were seeing in their house. By now you're probably wondering what these neighbors did to me to make me want to be so mean-spirited to them. Well, nothing. They just lived at the wrong house at the wrong time.

I tuned in to their phone and TV. The old lady was talking to Gertrude while watching *The Price Is Right* and her husband was out in back, trying to figure out the problems they've been having with their bug zapper light. I left her TV picture on but muted the sound so I could talk over Bob Barker. Using my voice changer, I announce, "Greetings, Earthling Mildred. I am alien visitor Q359-Kriegsmitzelpapshmeer. I come in peace. Take me to your leader, Bob Barker, or I will disintegrate your house. Oh, and I also want a Metallica box CD set and I want to know what a vacuum cleaner is...."

I left them alone completely until Mildred got back from the hospital. While they were gone, I bought some heavy duty wire and tapped into their circuit breaker box, giving me complete control. I also ran their water line through my house so I could leech and control that. When they got home, Mildred got in the shower and Herb sat down to watch Tammy Faye Bakker on TV. I walked over to my "Department of Water" switchboard and turned a valve. This valve released the five gallon tank of washing machine Blue (dye) into their water lines. Then I popped in the porno video "Edward Penishands" and sent that into their living room TV set. Herb was so engrossed in his show that he didn't even hear Mildred screaming something about alien invasions.

A few months passed. I spent the day mowing my neighbor's lawn while they were gone (I mowed the words "WE COME IN PEACE"). It was 2:30 in the morning and I grabbed my backpack and sprinted over to the Celina Power and Light building. I began to dig a trench from their building to my basement window....

Ahem, wait a second. I think I've been using a few too many illegal substances or something. Actually, I made this whole thing up. I was bored, okay? Anyone who believed any of it even for a second needs to have their head checked out. The story is probably full of holes although I really did live in Celina, Ohio alone and bored for a few months and ran up quite a hefty phone bill. It was my own bill, though. I really hope this article is an inspiration to all and hope that the Celina Police will stop looking for those kids in the boatyard after they read this.

ANNOUNCING

THE 1996 2600 INTERNET SEARCH!

The goal is simple. Find the oldest computer system hooked into the Internet. It could be a UNIVAC. Or a DEC 10. Maybe a Timex Sinclair. Who knows? The only way to find out is to start searching. If you're the first one to find an ancient system and it stays on the net throughout 1996, you'll win a lifetime subscription to 2600! You can even set up your own archaic system but you have to keep it on the net. It has to be the oldest system reported to us, and, in the event of a tie, you have to be the first one reporting it.

If you come under federal indictment for attacking the machine you find, it could affect your chances of winning.

Send entries to:

2600 Ancient Computers
PO Box 99
Middle Island, NY 11953
or email contest@2600.com

MACS AT EASE

by Loogie

Most schools use Macintosh computers because they are easy to use and schools can get them at great discounts. Well, most of the teachers are old farts and the ENIAC wasn't even around when they were young so they have no clue how to use computers. Our generation has grown up in the computer age and many of us know much more about computers than the teachers/faculty. Some of the teachers don't mind admitting their computer illiteracy and love help with their machines from people like me, but then there are the teachers who *think* that they know what the hell they are doing and hate it when a kid tells them how to do something when they are in a jam, or how to do something easier, etc. They also just *hate* it when you hack their crappy little security systems that they thought were so impenetrable. However, I find it rather fun.

The first and most common security system is called AtEase. It is a shell program that I really despise. (Not because it is hard to hack, but because it has such a retarded interface.) This is the easiest to overcome. Here are some ways to overcome it.

The first requires a computer with a programmer's switch. This is a switch on the front of the computer used for programmers that loads a debugger built into the ROM. Not all computers have this, however. There are two buttons. The left one (with the triangle) restarts the computer. The right one (with the circle) loads the debugger. When you are in the regular AtEase selection screen, hit the right one and you will see an empty dialogue box with a ">" at this prompt. Type "G FINDER". After you hit return, the screen will disappear and AtEase will quit and load the regular operating system, the Finder. Then you have full access to everything and can trash or change anything you want!

If the computer you are on does not have a debugger, then try this. Hit command-option-esc. (The command button is the one with the Apple icon on it and the little close-ended pound sign.) You will then get a dialogue box asking if you want to force quit AtEase. Obviously you do, so click the button "Force Quit". Sometimes this will work, quitting AtEase and loading the Finder, sometimes it will quit AtEase and then load it again. (Again, this must be done at the regular AtEase selection screen.)

The third way is as follows. Restart the computer and hold down the shift, disabling all extensions. When you are about to get to AtEase, it will ask you for a password. Just hit cancel. Then keep opening up program after program until you run the thing out of memory. Sometimes AtEase will then quit, leaving all the applications open with no operating system open! Then go to all the different programs and quit them. After the last one, the computer will realize that it has no operating system and it will start up the Finder! However, sometimes this works and sometimes not. It will not work on version 2.0 or higher of AtEase (in my experiments) and it won't work on certain computers, but you may get lucky.

The reason this happens is because AtEase installs a patch in the system itself so that it will launch AtEase at startup even if the extensions are disabled by hitting shift at startup, but there is also an extension. The extension contains a patch for AtEase to make it able to handle running out of memory. This patch is disabled and you can crash AtEase! Nifty, huh?

This last thing is my personal favorite for AtEase. This is not for school but rather office supply stores and department stores like Sears. Most commercially sold Macs (dubbed "Performas") are bundled with lots of software, including AtEase. AtEase is left running on the demo Macs. If they are running a little presentation program, it can easily be quit by using the command-option-esc method mentioned above. Then you will be at AtEase. The software comes with a default password, "familymacintosh" (no caps, no spaces) which most places don't bother to change. (Every place I've visited, it worked.) If you use this, then you can even change the password! Hahahaha!

Also, many department stores just let the screensaver run. It is most often AfterDark 3.0. If they are using the password function, then all you have to do is use the same command-option-esc as used above! This is because with AfterDark 3.0, they made the screensaver a separate program that loads itself when it goes on and quits itself when it goes off. You can force quit it like any other program.

There are many other ways to hack AtEase as well as hundreds of other programs.

SHARP CASH TRIX

Editor's Note: Although readers should always exercise caution in the application of knowledge, the subject matter of this article deserves a special advisory. Do not attempt to take advantage of this security weakness unless you have the approval of those in charge. Doing otherwise could risk your future and possibly your life. Opening a cash register without permission is very different from logging onto a computer without permission, despite what some authorities want us to believe.

by Dennis Fiery

There is an interesting security problem with the Sharp ER-3100 cash register. The ER-3100 is an inexpensive model that can be fully programmed by the user, but the security problem is about as low-tech as you can get. I've seen this model being used in bagel stores, pizza places (including the Sbarros chain), libraries, video stores, and elsewhere, so this is a pretty popular choice as far as registers go. You can recognize the register because it is beige, and it sits on top of a silver-grey cash box. The register and the box appear to be two separate pieces, but actually they are bolted together as one. On the back of the register (the side that faces the customer) there is a moveable lighted display that shows the cash total in green, and it has the word "Sharp" printed on it in white lettering.

We are all familiar with the great precautions that store-owners take to prevent employee theft. If you have someone working the register in your store you have to trust them to a certain degree. But as you know if you've ever had a job behind a counter, the boss usually has a bunch of rules that must be followed so he can keep track of who is using the cash registers and how they are being used. In some stores, receipts are imprinted with the clerk's name. In other places a code letter or number is used (the ER-3100 offers four different letters that can be printed on a receipt: A, B, D, and E). The store owner can insert a key into the register, turn it, and press a button or series of buttons to print out an activity log, giving a complete breakdown of what money is in the register, what was purchased, and what money was refunded. Big Brother is definitely smiling about all these precautions bosses take to spy.

All of the above is a good way to keep track of individual transactions, but whenever the cash drawer is open the clerk can swipe out a handful of money. Cash registers generally have a "No Sale" button on them, which allows the drawer to be opened without a transaction being issued. "No Sale" is mostly used when someone comes into the store and asks for four quarters for a dollar, or other change. The "No Sale" button is dangerous because it opens the drawer, and while it's open anything at all could go on, and the boss doesn't have much control over that, except to trust the cashier's honesty.

There are some precautions taken to try to prevent employee theft when a "No Sale" is rung. First of all, when "No Sale" is pressed, the cash register rings its bell. If the supervisor or manager is on the other side of the room, they will know that the register is open and the employee will realize that he or she is somewhat under the watchful eyes of their boss.

Also, every time "No Sale" is rung up, that fact is recorded. Later when the boss prints out an activity log, he or she will see that cashier B pressed "No Sale" four times that night while cashier D did not press it at all. If some money is missing, the four "No Sales" would lead the boss to suspect cashier B is the culprit. Many bosses forbid their employees to use the "No Sale" button because they don't want the cash drawer opened unnecessarily for just this reason.

How to Get Around This Security

Now we get to the security laxity in the register. There is a way to open the ER-3100 in such a way that the bell does not ring. Completely silent! More importantly, by opening the drawer in this way you also bypass the computerized activity log. The boss will have no records that the register was ever opened.

The cash register rests on four black rubber pads which raise the register off the countertop a little less than half an inch. This is just enough space to slide one's fingertips underneath the register. Indeed, this is the method to opening the register. There is a secret lever under the register. It's towards the front of the machine on the side facing the customer. Because it is on the far side away from the cashier, if the cashier wants to access this secret lever, he must lift the register and slide his hand and arm underneath the register to reach the lever on the other side. That's where the customer has an advantage - it's actually easier for the customer to open the drawer than the cashier! The customer has the lever literally inches away from his or her body. In many pizza parlors and other places that use this register, you can stand by the counter and casually slide your fingers under the register (palm up). Insert your fingers under the center of the register until you find a rectangular hole in the metal bottom of the register, close to the nearest edge. Inside this hole you will feel a vertical strip of metal perpendicular to the floor. Push this metal strip away from you, towards the cashier, and the cash drawer will roll open.

The lever is hard to find at first. The hole in the bottom of the register is pretty big, and the lever is pretty small. Also, the lever does not feel like a lever. It doesn't feel like a "user interface object" that you are supposed to manipulate, and if you were to lift the register and peek underneath you would see that the lever doesn't look like anything special either. In short, the Sharp people are trying to disguise this lever from casual observation and discovery.

But we know it's there! Feel around until you find it in the hole, and push on it. I strongly, strongly advise you to first make sure the store does not have security cameras and no security guards, and preferably that you're good friends with the cashier. Otherwise you could find yourself in a jail cell where there are no secret levers to get you outta there.

Whenever I see one of these registers in a store or restaurant, I always ask the clerk if they know about the secret way to open the register. They never do. I have *never* met anyone working at a store or restaurant who knew about the hidden lever! Usually they express disbelief until I demonstrate how easy it is for me to slide my fingers underneath and give the lever a push.

The instruction manual for the register explains the lever as a way to open the cash drawer "when power failure is encountered or the machine becomes out of order". The brief and grammatically incorrect paragraph describing the lever is pushed all the way to the back of the manual, almost on the last page, and is given under the unassuming title "Opening the Drawer By Hand". If you ever open one of these registers you can find the instruction manual hidden underneath the till. After opening the cash drawer, you will see the compartmentalized till which has sections for different money denominations and coins. Lift out the till slightly to reveal the manual (and possibly other goodies) underneath.

Protecting the Lever

Sometimes a store will install its cash register in such a way that you cannot slide your fingers underneath to access the lever. For instance, the register may be protected by a raised portion of the counter. In one library I saw pieces of metal bolted to the countertop as a protective measure against finger-insertions. There is another way in which the lever can be foiled: if the supervisor locks the cash drawer with the key, then it will not open. It is rare, however, to find a locked cash drawer, especially during the day when people are coming into the store to buy stuff! The vast majority of the registers I've seen were freely accessible to anyone who knew about the lever.

Conclusion

One time I was in a music store that used one of these registers, and the cashier was talking to his friend who was leaning against the counter. The friend happened to bang his elbow on the cash register, and the drawer flung open of its own accord. The two were surprised (as was I), but I also knew what had happened: the shock of his arm had conducted to the lever, which got rattled back and caused the drawer to fling open.

The ER-3100 is a good cash register, easy to use, highly programmable, and expandable. But it does have this one problem. If you use this model in your store, you should make sure the back is closed off so customers cannot slide fingers underneath. Either put up a piece of wood or metal in front of the register, or lower the register into a niche or put it up against a wall. Another alternative is to put a big piece of duct tape over the hole in the bottom of the register.

HACKING DOORS

by Clark W. Griswold

I thought it would be fun to share some interesting things I've learned about something we've all seen, dealt with, and sometimes cursed at. I'm talking about those telephone security systems in the front of apartment buildings. You know what I'm talking about, those damn phones - you have to pick up the receiver and push a button and wait for your friend/relative to pick up the phone, and then decide whether to let you in the building or not. Then they push a magic button, and the electric lock on the front door opens for a few seconds, and you have to hurry and put the phone back and run to the door and open it before the buzzing stops. I'm not talking about the simple intercom types, but the ones where you hear a dial tone, and the button you push speed-dials their apartment phone number (dial tones, can you see where I'm going already?).

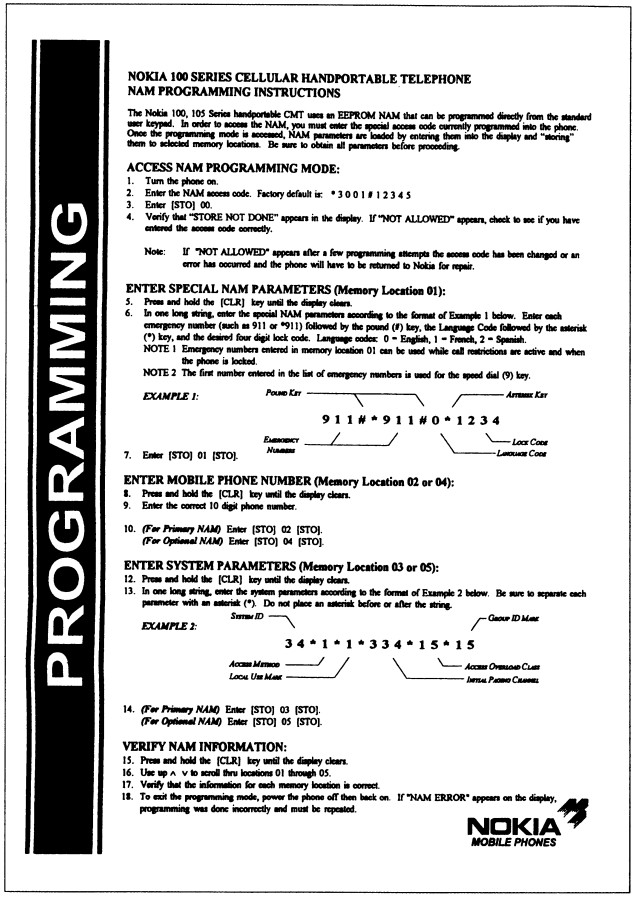
I started to get curious when I saw how my friend lets people in when he gets a call from the lobby on his phone. When whoever it is says "I'm downstairs, let me in" the resident then pushes a button on his phone and holds it for two or three seconds and lets go. The security phone downstairs senses this signal and energizes the electronic lock from my friend holding down the "6" key on his phone for a few seconds and letting go.

All fine and well, you say, but what does this do for my curious mind? Well to begin with, most of the security phones in the front of the building have a standard telephone keypad built in, but you cannot get any tones when you push the buttons, except for the two or three digit code you put in to speed-dial the individual apartments. When you pick up the receiver to either put in the speed-dial number or push a single button next to the particular person's name, try using your pocket tone dialer (Radio Shack or equivalent type that you put up to the mouthpiece and send DTMF with) and see if you can make a local or even long distance call! Wow!! A free phone to call anyone you want. Of course you would want to be careful on making a number of long distance calls that would be billed direct to that number, but using calling cards, PBX's, extenders, or just local calls should not arouse any suspicion, or raise the phone bill of the party who gets the bill for that number. Keep in mind that you are at the front door of people's residences, so just being there for an extended period of time might be a little obvious, so use discretion.

Also, try dialing an ANI number and see what happens. If you get a valid number, have someone try to call you at that security phone and see what happens! Sometimes it will ring on its own, and sometimes it may be an actual zextension of one of the phone numbers in the manager's apartments. If you really want to get back at the manager cuz he kicked you out or something, I suppose you could run his bill sky high with 900 numbers, but that would be illegal.

Just one more thing. You pick up the receiver, push the button for your friend's apartment, and no one answers. Now what??? Well, the next time you are in his apartment and he lets someone in, notice what button(s) he pushes on his phone to open the door. The next time you try to get in and he is not there, whip out your trusty pocket dialer, hold it up to the mouthpiece, and push the same tones for the same length of time, and I bet the lock will open on the door!! If you don't believe me, try it for yourself. The look on my friend's face when he's late to meet me at his apartment, and I'm sitting at his apartment door, inside the building waiting, or just all of a sudden knock on his door without calling first to be let in, is worth a million bucks. He still can't figure it out.

Since I figured this out, I can either get free phone calls and/or get into about 30 percent of the buildings that I mess around with.



PROGRAMMING

NOKIA 100 SERIES CELLULAR HANDPORTABLE TELEPHONE
NAM PROGRAMMING INSTRUCTIONS

The Nokia 100, 105 Series handportable CMT uses an EEPROM NAM that can be programmed directly from the standard user keypad. In order to access the NAM, you must enter the special access code currently programmed into the phone. Once the programming mode is accessed, NAM parameters are loaded by entering them into the display and "storing" them to selected memory locations. Be sure to obtain all parameters before proceeding.

ACCESS NAM PROGRAMMING MODE:

1. Turn the phone on.
2. Enter the NAM access code. Factory default is: * 3 0 0 1 # 1 2 3 4 5
3. Enter [STO] 00.
4. Verify that "STORE NOT DONE" appears in the display. If "NOT ALLOWED" appears, check to see if you have entered the access code correctly.

Note: If "NOT ALLOWED" appears after a few programming attempts the access code has been changed or an error has occurred and the phone will have to be returned to Nokia for repair.

ENTER SPECIAL NAM PARAMETERS (Memory Location 01):

5. Press and hold the [CLR] key until the display clears.
6. In one long string, enter the special NAM parameters according to the format of Example 1 below. Enter each emergency number (such as 911 or *911) followed by the pound (#) key, the Language Code followed by the asterisk (*) key, and the desired four digit lock code. Language codes: 0 = English, 1 = French, 2 = Spanish.
   NOTE 1 Emergency numbers entered in memory location 01 can be used while call restrictions are active and when the phone is locked.
   NOTE 2 The first number entered in the list of emergency numbers is used for the speed dial (9) key.

EXAMPLE 1:

7. Enter [STO] 01 [STO].

ENTER MOBILE PHONE NUMBER (Memory Location 02 or 04):

8. Press and hold the [CLR] key until the display clears.
9. Enter the correct 10 digit phone number.
10. *(For Primary NAM)* Enter [STO] 02 [STO].
    (For Optional NAM) Enter [STO] 04 [STO].

ENTER SYSTEM PARAMETERS (Memory Location 03 or 05):

12. Press and hold the [CLR] key until the display clears.
13. In one long string, enter the system parameters according to the format of Example 2 below. Be sure to separate each parameter with an asterisk (*). Do not place an asterisk before or after the string.

EXAMPLE 2:

14. *(For Primary NAM)* Enter [STO] 03 [STO].
    (For Optional NAM) Enter [STO] 05 [STO].

VERIFY NAM INFORMATION:

15. Press and hold the [CLR] key until the display clears.
16. Use up ∧ ∨ to scroll thru locations 01 through 05.
17. Verify that the information for each memory location is correct.
18. To exit the programming mode, power the phone off then back on. If "NAM ERROR" appears on the display, programming was done incorrectly and must be repeated.

NOKIA
MOBILE PHONES

THIS KIND OF INFO can really get you in hot water if the Secret Service finds it in your possession. It's probably not a good idea to keep looking at it. No kidding. Really.

hacking caller id boxes

by Dave Mathews

Because the Caller ID system uses out of band signaling that is set up in the 5ESS switch, there is no way to "fake" your outcalling number unless you make an operator assisted call, or dial through a company PBX. You can, however, hack the box that sits in your house up to more than eight times its capacity if you have the right revision! Here's how you do it:

Most Caller ID boxes you see in stores are sold according to the capacity of numbers they can store. The more you pay for the box, the greater storage capacity of numbers (between 60 and 99 for example) you obtain over the cheaper boxes which only hold between 10 and 30 numbers.

CIDCO, or Caller ID Company, is one of the most popular manufacturers of Caller ID hardware, and is publicly traded on the stock market. CIDCO's boxes are sold in stores under names such as AT&T, GTE, Radio Shack, and others.

Because CIDCO concentrates on mass production and OEM sales, it is less expensive to manufacture one CID circuit board that is "jumper" (solder points instead of jumper pins) selectable for the capacity of numbers that it can store. The good news is you can buy the cheapest CIDCO Caller ID that you can find (10 number memory is *perfect*) and upgrade it to handle 85 numbers!

How to buy it:

Before you buy, it's important to know first that you have a CIDCO unit (remember, lots of companies show their names on the outside of the case) and which ROM revision you have. Fortunately for us, the CIDCO engineers tell us this when the unit is "booting up". When you insert the nine volt battery, watch the display. You will see "C-NAM ver 1.2A" or "C-NAM ver 1.4". After this, you will see the capacity of the unit. If it is a "10-call" or "30-call" unit, buy it as it should be *very* inexpensive. If it is a 60 number unit, you can now make it hold 25 additional numbers. If it says "85 call", it is maxed out and you cannot increase the storage.

How to hack it:

So your unit says 1.2A or 1.4 when you power it up, and you saved tons of money by purchasing the 10 number version. Get out your Phillips screwdriver and take out the two visible screws on the bottom of the unit. Peel off the rubber feet on the opposite side of the two screws you just removed and you will find two additional screws (total of four) that will let you open the box (just peel the feet off and save them). Now we can see the circuit board. In the off-set in the middle side of the board you will see a GoldStar chip with the number GSN15 GM76C28AFW-10 or somthing similiar. Beside it you will see one of two jumper pads depending on the ROM version you have.

The two versions are as follows:

Version 1.2A
One pad unlabeled with four solder points:
Blue trace wire from GS Chip to:

A	**10**	**number**	**Eng/Spanish**
B	**85**	**number**	**Eng/Spanish**
C	**10**	**number**	**Eng/Spanish**
D	**10**	**number**	**Eng/Spanish**

(Make sure you solder the wire to the correct side of the pad)

Version 1.4
Two sections labeled:

X2	**C**	**o o**	**10**	**Call**
	B	**o o**	**30**	**Call**
	A	**o o**	**60**	**Call**
	(None)		**85**	**Call**

(Remove solder b/t pads)

R17	**D**	**o o**	**French/English**
	E	**o o**	**Spanish/English**
	F	**o o**	**English Only**

With version 1.2A you must solder the trace wire from the GoldStar chip to the "separated" gold pad on the circuit board that is labeled "B" to obtain full capacity of 85 numbers.

With version 1.4 you will need to remove the solder that is "bridged" between the circuit board pads (labeled as "o" above) to increase the capacity.

You will most likely have solder "bridged" between the A, B, or C pads.

Your language will most likely be jumpered between the pads labled E which lets you select English or Spanish after bootup. If you want to force English, or allow French and English, just remove the bridge from pad E and span the pads between D or F with solder.

That's all there is to it! As new Caller ID/Call Waiting (displays who is calling you while you're on call waiting) boxes come out, I'll have a fix for those as well (most store 99 numbers initially). I've hacked around with half a dozen different boxes and CIDCO's are the best. Others like TT Systems will only change button features when you cut traces instead of increasing capacity, so it's no use explaining those. If you have a different CIDCO ROM revision or another CID box, look for a jumper pad, or solder points! Chances are you might be able to hack it in the same manner that we can with these!

WRITE FOR 2600!

Apart from helping to get the hacker perspective out to the populace and educating your fellow hackers, you stand to benefit in the following ways:

A year of 2600 for every article we print
(this can be used toward back issues as well)
A 2600 t-shirt for every article we print
A voice-mail account for regular writers (two or more articles)
An account on 2600.com for regular writers
(2600.com uses encryption for login sessions and for files so that your privacy is greatly increased)

PLEASE NOTE THAT LETTERS TO THE EDITOR ARE NOT ARTICLES

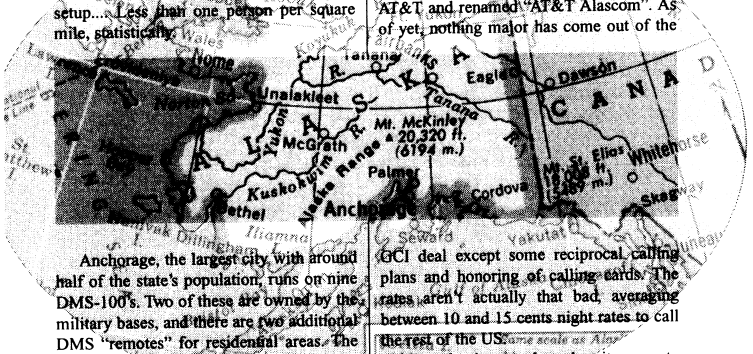
Send your articles to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099

THE ALASKAN PHONE SYSTEM

by Ice

You're probably looking at the title of this article. "The *Alaskan* phone system? Who *cares?!?!?!?*" But the Alaskan phone system is actually very interesting and different from most others. Alaska was admitted into the union second to last from Hawaii, currently has the largest land mass by far (more than 500,000 square miles), and has the second-to-the-last population of any state with roughly 500,000 people. This makes for a very interesting telco setup... Less than one person per square mile, statistically.



Anchorage, the largest city with around half of the state's population, runs on nine DMS-100's. Two of these are owned by the military bases, and there are two additional DMS "remotes" for residential areas. The local telco, ATU (Anchorage Telephone Utility, recently named "ATU Telecommunications"), is the only one owned by the local government in the nation (we aren't in an RBOC - no USWest, etc.), but it's at least as lame as other telcos. A residential line is about $16 a month, and a business one is $30 a month. We have CID, Last Call Return, and Continuous Redial as of a few months ago, but no other other CLASS features to speak of. We don't yet have ISDN available, in-town T1's cost from $160 to $200 a month (*plus* $137 a mile!). Fiber ethernet links are a minimum of $600/month. The payphones were 15 cents until about two years ago when they went to 25. I've not had much success blue boxing off of our lines, but that's just within Anchorage.

There are two long distance carriers in Alaska. General Communications Inc. (GCI - 10077) and Alascom (10866). No AT&T, no Sprint, no MCI. However, GCI formed an alliance with MCI in the last year, and Alascom (who was owned by Pacific Telecom) was recently bought by AT&T and renamed "AT&T Alascom". As of yet, nothing major has come out of the GCI deal except some reciprocal calling plans and honoring of calling cards. The rates aren't actually that bad, averaging between 10 and 15 cents night rates to call the rest of the US.

The telco has no clue when it comes to their tariffs. 30-way Meet-Me's are only $2/month, and there's a feature named "Malicious Call Hold" which they forgot to omit - if someone calls you from within your wire center, you press the button on your Meridian phone and they can't hang up. It's fun... Customer Data Change (you get an account on the switch and get to play with your lines) is only $4/month, but there's a $7,500 startup! SMDI (Simplified Message Desk Interface - read your philes) costs $600/month! These are only available under Centrex (yes, we *do* have Centrex...), but the even funnier part is that a normal Centrex line is two dollars a month *cheaper* than a normal business line! I don't know what they were smoking when they came up with their pricing (including their inflated leased line prices above), but it's the government - what can you say?

The rural telcos are a lot more fun to play with. Alaska has two of our own communications satellite, "Aurora" and "Aurora II", stationed in geostationary orbit above us. They're owned by Alascom, but GCI gets access to it (as with all of Alascom's equipment). Alascom makes these crappy "CO-in-a-trailer" things that they ship off to all the Eskimo villages and such, which, from what I can tell, are some old Crossbar stuff with a transmitter/controller. There's a 14 foot dish or so aimed at the satellite. These trailers are capable of handling 100-200 numbers in a single exchange, and they actually have payphones on some of them. I got a trunk tone once, *without* using any illicit means to get it! I received an incoming call, the operator wanted to bill me something for it, so I chucked in a coin (what the hell, I'm just lame), heard a few clicks, and *bam*... I just about killed myself because my BB was 500 miles away in Anchorage. All of the "major" towns (with more than 2,500 people) usually have a microwave tower or a larger satellite setup and switch. The satellite is also nice because you can make calls from just about anywhere if you're 'leet enough to have the suitcase-transciever kit. The rest of the state is littered with Earth Stations and toll complexes, etc. There's also fiber optics from Fairbanks to Anchorage to Juneau, the three major cities, which covers quite a few hundred miles on the way.

We also have a fiber line in between Japan and Portland (don't ask me why they didn't use Washington) named the "Trans-Pacific Cable" that's used for 99 percent of long distance calls, but it has been cut before by boats and other "unknown causes" (four times in the just the last year!), so the satellite is still used for backup. The long distance companies must make their money through leased lines, as a T1 to Seattle costs in the ballpark of $15,000 bucks a *month!*

Alascom is the long distance company that built most of the statewide phone system, and it got all kinds of concessions from the FCC during deregulation by arguing that we never had AT&T and Alaska was a "special case". As is, we didn't even have the "1-907-" or even the "1-" dialing until fairly recently. Times change so quickly - I still remember the "You do not need to dial a 1..." recording when you *did* use it. To my [probably inaccurate] knowledge, I was the last person in the state to dial long distance without a 1.

The cellphone setup isn't that different from other places. We have Cellular One and MacTel (wireline) within the Anchorage-and-vincinity area. There are other carriers that handle farther-out communications, which can be tricky with the 2 carrier FCC limit (and other cell sites so nearby). A really cool thing is that the cellular systems extend through in-state long distance boundaries, so you can place calls to some areas for just the normal airtime fees. They actually route the calls through the towers to evade the long distance company.

With the exception of Anchorage, Alaska's phone system is a mixture of old equipment rigged up to new equipment and somehow interfaced with the rest of the network. Anchorage has relatively new switches, but the marketing department is too stupid to realize that they could sell some of the features that they *could* provide.... It makes a great playground for phreakers, at least in places other than Anchorage, and who knows - maybe we could have some con up here sometime. It would be scary but funny watching all of you driving the Alaskan-Canadian Highway.

AVOIDING SUSPICION

by ~Me

Have you noticed that there are certain members of our segment of society who seem to attract trouble? They seem to get caught, need to mount legal defense funds, and ask for help from different professional societies. Please understand that this is not a flame or personal attack on any individual, group, or collection of individuals who have gotten into trouble; this is a "how not to" analysis.

I define trouble as having special attention paid to one's self by members of law enforcement at any level. For purposes of this article I don't care whether certain laws are just, proper, constitutional, or right; I also don't care if the actions, suspicions, or tactics of law enforcement are proper. I want to help the reader (that's you) avoid their attention.

The bottom line is that if you are going to be doing something illegal, you must avoid, at all costs, the attention of Law Enforcement Officers "LEO" (cops or feds; I also use the term for departments or agencies). The other thing to avoid is publicity that can come from formal news media, attaching ones name to viruses or malicious attacks to systems, writing for paper or e-zines, or being very "vocal" electronically or verbally.

Learn the local laws and conditions - wherever you are! They may be petty and they may be unconstitutional, but if they give an LEO some reason to pay special attention to you, watch out! Remember what happened to our friend at the convenience store in Haverford Township who did federal time because he attracted the attention of a Haverford Township cop. Was he doing something that was illegal when viewed by an LEO driving by? I don't know, but from accounts I've read, there was some "hanging out" or maybe a van full of racially disadvantaged males sitting in the parking lot.

LEO's look for that kind of thing. They also watch "gangs" of youths hanging around in malls. Especially if they (in the perception of the LEO) are speaking in a weird language or carrying weird devices. If you are under 18 (or look it), pay attention to local curfew laws. Pay special attention to vehicle safety, parking, and driving laws.

Many people casually violate the speed limit, ease through intersections with stop signs without really stopping, park on the wrong side of the street, drive after drinking too much, drive after drinking at all (if under age), or drive a fast looking car with minor defects (cracked windshield, broken tail light, plastic cover over the license plate). LEO's usually ignore these actions unless they become too obvious or they are in the mood to pick on someone. They usually do not bother the WASP male businessman in a clean suit (who may know the local politician or be able to afford a lawyer) if he has a broken tail light; but they are more likely to pull over a younger person, someone with long hair, or a member of racial minority.

Once they pull you over, anything in plain sight is fair game - if they can see it (back seat, floor, in the glovebox when you reach for insurance card), they can legally look at it. If you give them problems (make furtive movements, move like you are reaching for a weapon, or are verbally abusive), they can search your person - for the LEO's safety - all very legally. They can also look in your trunk if you give permission (of free will or under pressure), if they get a search warrant (properly or improperly), if they have reason to believe there is imminent danger to public safety, or if they just feel like it (illegally). If they see anything illegal in plain sight, they can search your person and trunk; if they find anything illegal on your person, they can search your trunk. If they find anything - in plain sight, on your person, or in your trunk, then the real problems begin!

Although it can be tough at times, treat all LEO's with respect - especially during a traffic stop. Turn your inside light on and place your hands on the dash or wheel where they can be seen. Think of the LEO as someone to social engineer - you want them to like you, not think you are slime.

If you do anything to get yourself arrested, you are wide open for search of person and personal possessions like book bags. If you are arrested some place like home, they can visually search the immediate premises - any point from where they can enter to where they find you. Then the same parameters apply as an automobile search.

Never, ever, ever carry a concealed firearm unless you have a permit for it. This really upsets LEO's and can cause all kinds of problems (even federal charges if you crossed state lines while carrying). It is fairly easy to get a permit in many states - Pennsylvania will provide one after a background check. Basically, you must have a clean record, be of age (18 or 21 - I forget), and be of "good character" - that means you cannot be a habitual drunkard or spouse beater. You have to provide a reason, something like a work schedule requiring you to work odd hours and travel through dangerous areas. An interesting tidbit: concealed carry permit holders are not subject to the Brady Bill background check! The supposition is that they already passed it to get the permit.

Also, avoid the fancy knives! You are much better off carrying an X-acto blade or a good "electrician's" knife (scrape some wires with it so you can easily claim that it is a "tool" not a "weapon").

In this day of cyber-phobia and "get tough on criminals", the courts are much less likely to disallow evidence gathered illegally (pulling you over without reason or searching your trunk illegally). Even if the courts throw out *everything* from that LEO acting improperly, they can still use the information gathered to look into your life further. If you were carrying a laptop in your trunk and it was confiscated, they would search the disks, even if they could not use the evidence on the disk, they could use the information to investigate further. Do you have a copy of *Phrack* laying around? Do you have any codes or an Elite BBS in your terminal emulator dialer directory? Any cracked or pirated software? How about TBBOM?

Yes? Then they have more reason to watch you and gather evidence. You have given the LEO what they need most: probable cause. Probable cause is a legal term defined as: "Reasonable grounds for belief that an accused person is guilty as charged" by the American Heritage Dictionary. It means that you have given them reason to believe that an illegal activity has or is occurring. It is the requirement for the issuance of search warrants, arrest warrants, subpoenas of financial and telephone records, and for wiretaps.

When they catch you saying, e-mailing, or downloading something that violates some law - then you are one of those "dangerous hackers" and should be thrown away to protect society before you decide to launch nuclear warheads at Washington DC or steal credit card numbers and charge $1,000,000 to some grandmother's Visa card.

Do you do things that gain the attention of telephone company security officials? They monitor patterns, look into people who receive fraudulent telephone calls (do you get many calls from people using codes or cracked PBX's?), into people who make fraudulent telephone calls (you never card from home, dorm, work, or friend's), and into people who call telephone numbers that make or receive fraudulent calls (do you call phones that have that kind of activity - people or Elite boards?). The security forces can gather information and then give the LEO their probable cause.

Anyone who brags about illegal activities is bringing attention to themselves. This is publicity. Who hasn't bragged about cracking some software or a system or figuring out codes - but remember, the only way to keep a secret is not to tell anyone. If you want to spread information, you must ensure anonymity or safe pseudonymity. Anonymity occurs when a creation (document, note, message, poem, book, flyer, picture, etc.) is not signed. Pseudonymity occurs when a creation is signed with a false or made up name - one that cannot be traced back to you.

It is not illegal for an LEO or a telco security official, as a private citizen, to read messages on a BBS or netnews. This is the same as that person reading the business cards or for-sale notes on boards in some stores - it is publicly available information without the expectation of privacy. Many boards have LEO's of telco as members - usually without the SYSOP's knowledge. Posted messages have timestamps; telco records have timestamps (traces or illegal calls); the two can be matched up.

Speaking to the media, baiting LEO's, writing articles, and publicly displaying illegal activities is publicity. LEO's go after those that are most visible - especially when that person has had media exposure because it makes the LEO look more effective.

Think about it! I am not an LEO nor related to one and I don't play one on TV. I've been pulled over a number of times for minor traffic violations. I avoided arrest for some fairly serious activities a few years ago by insulating my public and private persona.

WHERE THE LETTERS ARE

Opening More Doors

Dear *2600*:

Concerning garage door openers: ours has an 8-bit DIP switch inside, giving a whopping 256 different codes. We replaced the switch in ours with a CMOS 8-bit counter and 555 timer to drive it. Now it counts through all the codes in under a minute. We drive around to see who has the same brand of opener. The local fire department does. You'd be amazed who else does....

RB
San Francisco, CA

Eastern Europeans

Dear *2600*:

I received two issues of your magazine that I liked very much. I believe that I am the first Croatian contacting you. In Volume 12, number 1, in "The Better Letters", I read that you were still offering free subscriptions to Eastern Europeans. As I would be very much interested in getting your magazine regularly I am herewith applying for this subscription.

Hrvoje Vukovic

All you have to do to get a free one year subscription from Eastern Europe, the former Soviet Union, and Cuba is write to us and ask for one. No email, no faxes - just a letter from the country you live in. You'd be amazed how few people put in that little effort.

ANAC Change

Dear *2600*:

A quick update on the letter (in the Winter 1995-1996 issue) from Percival regarding AT&T's universal ANAC number. The universal ANAC has been hit by the recent area code rearranging that will likely soon confuse a great number of hapless telephone users. The number has moved from 404 to 770, so the complete ANAC number is now 10732-1-770-988-9664. Undoubtedly countless others have discovered this by now, but I figured I'd dash off a quick note anyways. By the way, does anyone know the meaning of the numbers reported by the ANAC after my phone number? The sequence I receive is: tone (my phone number here) 8 pause, tone, 0000000001.

woodrat

Thanks for the update. Unless we've somehow missed it, we've never seen a bill come in with that number on it, so this could be a toll-free call, though not from payphones. The numbers following the readout remain a mystery.

Points on Interrogation

Dear *2600*:

I read your mag regularly and find the information timely, useful, and fun. I do, however, take *major* exception to the Autumn 1995 article "Hacking a Police Interrogation" - by Darlo Okasi. While there are some good points, much of the information presented is flat out wrong and dangerous. Darlo makes a point that the reader should try to be in control of the interrogation. You are *not* in control. That is what an interrogation is all about. If you challenge the control of a natural control freak (the cops), you put yourself in jeopardy. If your readers were to put these principles into practice, they risk being locked up for extended periods of time on no charges. (Against the law, you say? The cops will say "Sue us!", and even if you do, it will take years and thousands to settle). Darlo is fond of expressing false bravado or attitude, telling the cops they "are dirty" and cursing. This is dead wrong. If your readers put on such a belligerent attitude with the cops, they risk being hit and beaten, or, depending on their social status, even killed. Again the cops will say "Don't like it? Sue us!" This happens all the time.

What should someone do in case of interrogation? Keep cool. Be friendly, helpful, courteous... just like a boy scout. Don't say an incriminating word, and *lie till you die*, but be nice and smile at their attempts at humor as much as you can muster. If they try to "be your friend", you should "be their friend". Tell them you want to help them, but you just don't know what they are talking about. *Do* demand a lawyer. *Do* make a story with your friend(s) if planning some "gray" activity. *Do* tell the same story over and over and over and over. *Do* wait them out. It is a game, but a game of the most serious nature with your physical body on the line.

The Prophet

Dear *2600*:

I would like to make a few comments about the article "Hacking a Police Interrogation" (Autumn 1995). The advice the author gave ("don't tell them anything") was pretty good for starters. You have to remember that the process of interrogation is considered an art in the field of criminal justice. That means when you decide not to tell the police anything - they can still tell that you are lying.

How, you may ask? Well, simple - your body language tells it all. There is a new interview (interrogation) technique being taught to criminal justice personnel called the Kinesic Interview Technique. I have also been trained in using this new method, and would like to stay anonymous for the most part, since giving out this information could eventually hurt me in the future.

"The Kinesic Interview Technique is a multi-phase behavioral analysis system that is used to improve the communications process in order to conduct more effective and efficient interviews and interrogations. The foundation of the technique rests on the common everyday behavior of human beings and their diverse communication skills." The preceding text was quoted directly from the handy police training manual I got to keep after completing the course. Please notice that victims and eyewitnesses are interviewed by the police while suspects are interrogated. The only difference between the two methods is that one can get rough with suspects.

The Kinesic Interview Technique consists of three parts: 1. Body language; 2. Verbal behaviors; 3. Statement analysis.

Part 1. Body language is exactly that. The person interrogating the suspect may look for various clues that the body gives off without one knowing it. When asking the suspect a critical question, the person might rub their nose, shift their body from one side to another, cross their arms, give off a fake cough, etc.

Part 2. Verbal behaviors include speech disturbances (sounds that are not words) such as "ah, er, uh, um." The suspect will often omit article words in sentences (a, the, and, for), clip words in half, drop suffixes off words (ing), drop word endings (es, ed), and will often self-correct themselves in the middle of sentences.

Part 3. Statement analysis is done after the suspect writes down exactly what happened or what they were doing at a certain time (alibi). Experts will then examine the document very closely and look for signs such as handwriting pressure, curved lines, frequently misspelled words, etc.

What makes the Kinesic Interview Technique so successful is that it uses the above three mentioned parts together to come to a conclusion. The Kinesic Interview Technique is very complex and too elaborate for me to explain in detail to you without having to write a book on the matter. The police manual I had to train with goes over several hundred pages, and I highly suggest taking a class on this subject in order to get all of the necessary information about this technique. How about infiltrating a police training seminar?

Did you know that the police can even lie to you during an interrogation and tell you that if you cooperate you will get a lesser sentence? The truth of the matter is that the police do not have the power to grant you immunity from prosecution or lessen your sentence in any way - only the district attorney can do this. One can also be held by the police for up to 48 hours without any charges ever being brought up. Also, one does not have the right to make a phone call - it is a privilege in most states. So, be extra nice to the police officer when being arrested, since you definitely want to make a phone call to inform your lawyer. That brings me to another point. Don't be stupid and talk to the police without a lawyer! Keep your mouth shut! The less they know, the harder they have to work on cracking the case. Plus, you don't want to say something stupid that can be used against you at a later date. A nice thing about most interrogations is that the police can record or videotape the interrogation without giving you notice or asking for your permission.

Well, to finish things off... the best advice I can give you is don't do anything stupid that will get you caught!

System Default

Dear *2600*:

I would like to comment on Darlo Okasi's article "Hacking a Police Interrogation" in the Autumn 1995 issue. Okasi is dead right that understanding what police do during an interrogation greatly improves your ability to come out looking innocent. In the article Okasi correctly points out that the police can say anything they want in an attempt to get you to confess. Your confession is, of course, the whole point of the questioning. It's important to note that in the area of "high-tech" crimes, without the help of the person who committed the act, the police probably will never be able to figure out what was done, let alone prove that any particular person is responsible. Remember, anything you say *can and will be used against you!* Don't forget it. Also, the police will lie to you. (There may be a few idealists out there who don't believe this, but it's true.) They can say they have any manner of evidence - eyewitnesses, surveillance video, fingerprints, bloody gloves, etc. in an attempt to get you to "give it up". All of the "evidence" they say they have may be false; they may only have a hunch that you're the guy. Lying about the evidence is allowed based on this logic - *an innocent person will not confess, no matter what the evidence implicating them.* If they really have the evidence, then they don't need your confession - let them prove their case in court. The best piece of advice, as any defense attorney will tell you, is that you have the right to remain silent - *use it!*

Further, if you understand that the police aren't just interested in what you say, but also how you act, you can gain a real advantage. Are you sitting back in your chair with your arms folded and not making eye contact? (Guilty) Or, are you sitting forward, hands down, looking at them when they speak? (Innocent) But, most importantly is they way in which you profess your innocence. (Almost all guilty people start out denying that they did it.) A guilty person will start out vigorously denying the allegations. Then, slowly, that vigor begins to decline, until they are just sitting there quietly, looking at the floor, listening to the interrogator outline the charges and (maybe bogus) evidence, until finally they confess while looking down at their lap. An innocent person, however, begins much the same way denying their involvement, maybe even laughing at the suggestion. Then, as the interview continues, while a guilty person gets quieter, an innocent person continues to deny the

allegations, or they become even more adamant in professing their innocence. They start by saying "no", then after an hour they pound the table, and after two or three hours throw a chair against the wall. (Never anywhere near a police officer - this will get you in trouble, guaranteed!) If you follow this pattern, the investigators will come out of the interview room scratching their heads saying "Gee, maybe he really *is* innocent!" But remember, *never, never* let on that you know this information. If they know that you know about these "patterns of denial", then all bets are off as far as convincing them of your innocence.

Robin Scurr
White Lake, MI

Bernie S. Fallout

Dear *2600*:

I have been a proud reader off and on for a long time. (I buy at the stands.) But I am totally confused and scared about placing an ad in your Marketplace after reading the article "No More Secrets" (Bernie S.). Being in business selling info of this matter I see that the Marketplace is still full of this type of info. What does this mean? Is this kind of info now illegal to sell, buy, or even for you to allow such ads? From *Popular Mechanics* to *Soldier of Fortune* there are many people and companies with ads selling this type of info. How about companies like Loompanix, Delta Press, and many others - are their books now illegal? Is some of the info *2600* prints now illegal, under the current law (title 18 U.S.C. section 1029)? It sure sounds that way to me. Did this law go into effect in October '94 or '95? I don't know if I am breaking the law or not.

What should we (underground info sellers) do? Should I quit my business? I have about 170 publications that took me a few years to work up to! How can you keep your magazine going with a law like this? Does "For Informational Purposes Only" mean anything anymore? I am one worried man.

Name Withheld

The way the law (passed in October 1994) now reads, we could indeed be guilty of the same crimes Bernie S. was imprisoned for. But we believe the law is wrong and is blatantly unconstitutional. It must be challenged on all fronts. Unfortunately, no so-called civil liberties group thinks this is an important enough case to become involved in. This means there could be many more Bernie S. cases before something is done. Weigh all of this before making your decision and then do what's right for you.

Dear *2600*:

This thing going on with Bernie S. has really gotten me pissed off. What right does the government have to prosecute a man who just had the software? It's not like he was using it at the time. Tell me what i can do to help.

Mike W.

The best way to help is to spread the word. Check out the website (www.2600.com), finger bernies@2600.com for the latest info, and distribute what you see in 2600 to as many people as you can. We've made a great deal of progress in the last couple of months in spite of media indifference. There are an awful lot of us and we know how to get the word out. People like you are vital to this.

Dear *2600*:

I was reading your article on Ed Cummings in the Autumn 1995 issue and I stumbled on a fact that I personally was not aware of, and frankly find appalling.... This is Title 18, USC Section 1029: "possession of a technology which can be used in a fraudulent manner..." What's next? In a year, will carrying a pencil in your pocket be considered concealing a deadly weapon? It's amazing that the people supposedly representing us in Congress could pass such an anti-citizen law. How in the world can they make it illegal to distribute information of any type? How can they make it illegal to own a device that maybe, if someone feels like it, could possibly, if they wanted to break the law, be used in a fraudulent manner? Is it actually true now that having a copy of BlueBeep zipped up on my hard drive makes me a felon? This is unbelievable. However, it seems like a law that will disgustingly stay on the books. Is there anything we can do about this? I don't think so! I have already written to my congressman. Is the constitutionality of this law being challenged by *anyone* yet? Please, give me a minute - I have to recover from shock, and then go and clean off my hard drive and hide my red box that has been lying in a desk drawer for a year.

I never thought I'd see the day where I'd have to fear arrest for talking or writing about something. I'm nauseated.

TcP
Denver, Colorado

We're getting letters like yours every day. People are realizing the implications of this law and it's well worth getting upset about. So far, one person is challenging the constitutionality of this law: Bernie S. The problem is that it's very difficult to do this when the Secret Service keeps throwing him into prison. It's a fair bet they're aware of this fact.

Dear *2600*:

Phil Zimmerman, Ed Cummings, the Pentagon mall incident, and countless others.... Are you sure you live in a free country?

Mario
Canada

Dear *2600*:

I think that this whole Bernie S. saga is bullshit! We should all come together to protest (and screw) the government for these unimaginable and cruel punishments they are subjecting him to.

But on the other hand, Bernie S. did commit more crimes than possess and have custody and control of hardware and software such as an IBM "Think Pad" laptop computer and computer disks.

I mean he wrote four articles for *2600* which would imply he is a "Real Hacker". Just look at the shit he knows: "How to Defeat *69", "AT&T Sub Maps", "FAX: A New Hobby", "Paging For Free", "Cellular Phone Fraud and Where It's Headed".

I know that knowledge is not a crime but using that knowledge to commit a crime is! But I *strongly* think that he deserves to be released from prison because he has already suffered enough.

Adam Schoenfeld

We don't know whether to slam you for being dense or congratulate you for being witty. It's probably best just not to say anything.

Military Miscellany

Dear *2600*:

As part of my job I had to go to a high-security military base recently. There were loads of fences and dogs, etc. My escort lead me through four doors with electronic combination locks on them. The combination on each door was 12345. Is this what is known as military intelligence? Also, I have been trying to hack my local USAF base. I have found a phone number that rings, answers, and sends a carrier. My old 2400 baud modem seems to lock on, but nothing comes on the screen. Is this a Defender modem? If so, do I have a cat in hell's chance of getting round this?

Cockroach

It's impossible to say what you're connected to since you're not getting anything back. It could just be a modem connected to nothing. (Some of those "hacker challenge" idiots do that to try to drive us crazy sometimes.) Our advice is to try all kinds of variations to get any kind of a response at all from it. Once you've gotten that far, you're starting to make progress.

Dear *2600*:

Over the past 10 years I have been employed as a U.S. Navy nuclear submarine radioman, and for a short while thereafter for the arch-enemy of your organization, the National Security Agency, so I am no stranger to the world of codes, cyphers, and cryptology. But now due to a difference in political beliefs, I have chosen to wash my hands of the whole mess, deciding to start again in another less taxing field.

During my tenure with NSA, your magazine, along with several others of the same theme were made readily available by the powers that be as a sort of reference material, both as what to watch for and to generate new ideas. But I did not write this to stroke your egos; my concern is for the security of the common man.

I am referring to the PGP or Pretty Good Privacy program. While I am under contract with the government to not speak on issues of national security for the remainder of my lifetime, I can speak hypothetically of a pseudo government with resources that rival that of the United States.

To this government, with the vast monies, machines, and manpower at its disposal, public data security is nonexistent. The use of the PGP program, RIPEM, and others like them is a noble idea - they would probably keep your neighbor out of your email - but realistically to this government they are like the Cap'n Crunch decoder rings of old. Toys. Public digital privacy does not exist where this government is concerned. Publicly the government puts up a huge fight. We don't want the program available, it could be used by our enemies, they say. Anything over 40 bit encryption is a weapon. It's not to be exported, etc., what a better way to play to our enemies. Publicly they proclaim that it is unbreakable, it is to be heavily regulated, and such, while privately they sit back and easily decode anything they have a desire to. Either way they win, they convince the sheep that it's a bad thing used only by hackers, communists, and other enemies of the state. It is outlawed which makes it that much easier for them to operate, or by all the bad press they generate with their claims of its invincibility. They lull everyone into a false sense of security, where they think all of their data is safe from prying eyes when in reality it is easily read whenever it's their turn to be indicted.

At the same time they try an end run with the Clipper Chip and the Capstone Project. The public thinks it has won one, yea! It doesn't matter, it was only a diversion. The Clipper Chip was the equivalent of leaving your car door unlocked. Without it, and given the government's capabilities, it's like locking your car door but leaving the window down. And the PGP program adds all the security of rolling the window halfway up. It is a mere annoyance for them, an added day to the reading of your data. The only secure way to store information is in your head. And given the government's methodology of going about interrogations in issues "concerning national security", that's not really safe anymore. I just want everyone to know Big Brother is still watching, and they are getting better everyday.

On an unrelated note I would like to mention D. Ruduolph Goettel will be missed. Skinny Puppy won't be the same.

Disappointed in our Government

Spanish ANI

Dear *2600*:

Bored one day at home I decided to start dialing a bunch of 800 numbers when I came across a computerized number that spoke in Spanish. I was hitting random numbers when I heard the lady say my phone number. The number is 1-800-235-0900. If you dial the right numbers, you get your ANI in Spanish. I have been accustomed to using the ever famous 1-800-MY-ANI-IS. Lately when I dialed it up, it sent a steady tone over the line, and then stopped when a key is pressed. After

pressing a couple of keys I get the message "The authorization or ID code you have dialed is invalid." Do you know when or why such security would be applied to this number? Overuse perhaps?

The Mad Tapper
Ringwood, IL

What you have is the Spanish AT&T customer service line. Like the English version (800-222-0300), all you have to do is hit 1 to hear your phone number read back. As for the demise of the 1-800-MY-ANI-IS, overuse is probably an understatement. Even after a code was put onto that line, so many people had it (it was only three digits) that we would be amazed if the number still exists by the time you see this.

Cellular Prisoner

Dear *2600*:

My handle is Alphabits and I've been in the H/P scene for over nine years. I'm currently in federal custody in New Jersey waiting to go to trial for cellular phone fraud, mainly "trafficking in counterfeit access devices" in violation of title 18, section 1029(a)(2) of the U.S. code. In September of 1995 I was indicted by the U.S. government, and then shortly thereafter I was arrested by Secret Service agents on a freeway in southern California. I was one of the key figures busted in the "Celco 51" incident. The U.S. Secret Service, Cellular One, and an informant operated an H/P BBS in New Jersey for about two years. To my knowledge there were a total of 15 other people arrested across the country during September. Since Cellular One was a key partner in the operation, they were mainly targeting cellular fraud. On September 3rd I was extradited from Los Angeles to New Jersey in order to stand trial. During my two week journey, I was incarcerated with a few hackers including Agent Steal and Kevin Mitnick. Although I cannot talk specifically about my case now, I can say it is amazing how small the government's knowledge is regarding computers and hacking. One example is that on one of the computers they found a text file of FTP sites. They are trying to figure a loss value of $500 per site, $73,000 for the file. Excuse me, loss value of what? Did ftp.cso.uiuc.edu (exec-pc) lose money somehow? In any case, hopefully I will be free sometime around January of 1997.

I'm currently being held in a 100+ year old jail (similar to Alcatraz), which is a total intellectual wasteland. I would appreciate it if you could post my address or forward it to someone who could. Any letters, printouts, etc. would be greatly appreciated!

Jeremy G. Cushing #63366
Union County Jail
15 Elizabethtown Plaza
Elizabeth, NJ 07207
T8

We wish you luck and encourage people to send mail since prison can be a very lonely and mentally crippling environment. While we don't know particulars about your specific case, we do know that many questions are being raised about the Celco 51 sting operation of 1995. In particular, we have heard numerous reports of the informant you mentioned appearing at 2600 meetings trying to get people to commit crimes. We know this is accurate since we'd been getting complaints about this individual back in 1994. Tainted though this case may be, it's quite likely these questions won't change a thing. But we can learn something important. Odds are that if someone approaches you and tries to get you to turn your knowledge and interests towards the world of crime, they are either trying to trap you or they are trying to con you. If you feel nice and secure because the person you want to commit crimes with is a trusted friend, be aware that nothing tears apart a friendship more quickly than a federal indictment. There is absolutely no way of knowing how someone will react to that kind of pressure until the time comes when they are confronted by it. Take heart in the fact that these days you can still wind up in prison and be considered a major threat to society without committing crimes. When people recognize this, we have a chance of winning some important battles.

Highway Weirdness

Dear *2600*:

My fiance and I have been avid readers of your informative zine for the past two years, and I must say we have learned a lot! I had the opportunity recently to drive myself from Phoenix, Arizona to Springfield, Illinois and thought you and your readers may be interested in what I encountered with our fine highway patrol. I left Phoenix at 4:00 pm Monday evening, the 4th of December. My brother-in-law was kind enough to rent me a car to get to Illinois so that I could be with my mother who is ill. First of all let me start out by telling you that I am on two years probation for computer fraud and/or credit card fraud but that's a whole different story. Anyway, I must carry travel papers from my probation officer which I had. (Thank God!) I was traveling north on I-17 to Flagstaff and yes, I was speeding a tad. They had just changed the speed limit according to each state but it was still posted at 65. I was keeping up with the flow of traffic and passed a Bronco. (No, it wasn't O.J.) The Bronco stayed close behind me and it wasn't long before he passed me. He got right in front of me and slowed down to 55. I stayed in back of him for a few miles until I noticed I was only going 50 m.p.h. I sped up and went around him. He sped up and stayed close behind me. About ten miles down the road I looked in my rear-view mirror and saw that the Bronco was no longer there - in its place was the Highway Patrol. I let my foot off the gas pedal and noticed that he sped up and was right behind me. A couple more miles down the road he hit his lights and pulled me over. He asked for my ID and registration. At this time I told him it was a rented vehicle and gave him my travel papers. He asked me to get out of the car. As I did I noticed that the Bronco I was playing "tag" with was parked behind the squad car! The officer showed my probation papers to this other "gentleman" and they both kind of chuckled. I was later "introduced" to the Bronco man. He was D.E.A. Imagine my surprise! When I was asked why I thought I was pulled over I said, "Well, I guess it's obvious... I was speeding." The officer asked Bronco D.E.A. man, "How fast was she doing?" He replied, "Oh, only about 80, not bad." I had no idea what was going on here! Bronco Man, not Mr. Officer had "clocked" me, and by his own speedometer, not by a radar gun. I must have had this dumb look on my face because Bronco D.E.A. man spoke up. "Where are you headed?" I told him I was on my way to Springfield, Illinois to be with my mother, who has cancer. He asked, "What's with the suitcases?" I told him I expected to be in Illinois quite a while and those were my clothes. When asked what else I had in the car, I told him my dog, and a few of my worldly belongings (you know, computer, scanner, M1200, slippers, housecoat). He then asked me a string of "how bouts", such as how much cash I had, meth, pot, alcohol, blah, blah, blah. I said, "Look, I can't afford any trouble. As you can see I'm on probation, what's going on here?" He (Bronco D.E.A. man) told me that I fit the profile of, get this, a drug runner! I was a white female traveling alone in a rented car with suitcases that had airline tags on them (I never take em off, reminds me of where I've been) and an out of state driver's license. (I still had an Illinois driver's license - yet another story!) Oh my God! My mouth dropped. No way! Bronco Man was cruising the highway just looking for this kind of stuff! When he spotted me he stuck with me, radioed into The Man and I was pulled over! To make a long story not so long, they let me go, but not before they issued me a "Warning" ticket for speeding, of course. They said they weren't going to "search" my car because they didn't think I was running drugs. They also told me to expect to be pulled over again before the end of my journey, because I was considered *high profile!* They were right. I was pulled over two more times before I reached my final destination. One officer said I crossed the center line (I had to, I was changing lanes!) and I didn't give the third officer a chance to tell me why he pulled me over - I blurted out, "This the *third* time I've been pulled over. I'm not running drugs, I'm just trying to get home to my mother who is ill. I'm on probation, I've already been "checked out", and I'm fucking tired!" He said "Go lady, just go"! All three times there was a D.E.A. (white car) agent parked behind the squad car. So my advice to any female traveling alone is: Don't latch onto the car who is traveling a little fast so that he gets the ticket, not you. Get a radar detector (I had one), take airline tags off your suitcases and cover them with blankets or put them in the trunk. Get a dummy (or the next best thing) to sit in the passenger seat, preferably one that looks like grandma. Make yourself look older (I'm 34), maybe stick a pillow up your shirt, be pregnant! They are out there and they are on our highways!

Jus Jizzen

We suspect explaining what a dummy is doing sitting next to you in a car might prove to be more trouble than it's worth. Your other ideas are sound, though.

Dear *2600*:

Lately, I've been experimenting with different numbers, trying to find an ANI number for the 214 area code. Anyway, I dialed one number, 291-9901, and something strange happened. It rang once normally, then I got some digital sounding ring about three times, and then some high pitched tone that lasted about 5-10 seconds. After that a computer voice said, "Hello. K-L-T-Y Transmitter System. Enter security number now." It just repeated that until I entered a number. Do you know what this is?

King Otar

This is probably a system to monitor and possibly control the transmitter for that particular broadcast station. If they're really stupid, the station may allow remote control of room temperature as well as the ability to turn the station on and off. The high pitched tone sounds like a low speed computer carrier that is probably another way into the system.

Meeting Questions

Dear *2600*:

I am an Orthodox Jew and therefore cannot attend any meetings on Friday nights (funny thing how all the *2600* meetings happen on Friday nights). I was wondering if you knew of any meeting in the New York City area that happens on other nights or if such a meeting could be arranged. I am generally new to the H/P scene and although I do not intend to do any major H/P activity I am interested in the stuff. So any help in arranging a meeting of *2600* on a night other than Friday would be of great help to me.

Joshua

Friday night has always been the night for 2600 meetings since their inception back in 1987. Before that, TAP meetings were held on Friday nights as well. It's the whole tradition thing which seems to be clashing with your tradition thing. It's possible we may need to make some sort of a change to accommodate more people since the meetings have grown so much over the years. But this is something that needs to be worked out carefully - right now everyone knows that the first Friday of the month is 2600 meeting day. By branching out to other days, we could lose that recognition factor and also make things a whole lot more confusing for everyone. We're open to suggestion. In the interim, remember that 2600 is only one forum - you're free to do whatever you want under the name of other groups if you disagree with or can't meet our guidelines.

Dear *2600*:

Please give me some more information about the meeting in London. I know that it is at the Trocadero Centre by the VR machines and I know the time. But how should I know who to look for? What age of people? And how should I introduce myself? At the moment i write code in assembly, C, and Visual BASIC, but would like to know some hacking and phreaking basics. Will the people there be willing to teach me or just let me listen to their conversations?

Skywarp

There's usually somebody around with a 2600 shirt on. Ages vary from 10 to mid 70's. Avoid people outside that range. We're very informal so you don't have to worry about protocol. If you don't act like an idiot and aren't committing crimes, you should have no problem being accepted for who you are. Good luck.

Dear *2600*:

In the summer 1994 issue of *2600* (volume eleven, number two), at the bottom of page 17 is an announcement indicating *2600* is on line through IRC channel #2600, the 26th of each month. Is this still in effect? My service offers IRC access. In order for me to successfully connect with #2600 do I need to specify a port number or will I connect through the system's default port connection (6667)? Thank you for an excellent publication.

Frank M.

Any public IRC server should get you into the IRC world we all inhabit. The #2600 channel has sort of developed a life of its own and is no longer controlled by us. Such is the nature of IRC. You will, on occasion, find 2600 people wandering in and out of the channel.

Info

Dear *2600*:

Item of possible interest: 710 NPA belongs to feds. Previously, I have never been able to reach a number in 710 from the POTS network. 710-NCS-GETS (710-627-4387) results in a new dialtone with a request to enter the desired number and passcode.

Interesting things from Bellcore and GTE notes: 710 routed calls have priority if other circuits are busy, etc. On a non-priority call (like yours or mine), the various telco/carrier networks will try alternate circuit routings, but only so many. A 710 GETS call will allow more than the usual alternate routings.

NCS stands for National Communications System, located in Northern Virginia - probably the Pentagon. Be as careful when messing with this as you would be messing with any federal installation... feds don't have much of a sense of humor.

anonymous

Dear *2600*:

This is in response to a letter written in the Autumn 1995 issue by FxPigMan. The "computer" you refer to is a Dynatel 655, which is a loop analyzer terminal, and it does what you said - runs a test on the line - but oh my friend, this little mini-computer can do so much more. By just punching in a number such as, oh "2600", it will produce a 2600 tone for you. I like to refer to it as a waterproof laptop sitting on a 12 volt battery - it also has a lithium battery. This laptop is sold to phone companies for $5000. Not your average laptop, eh? Well, "the place" the Dynatel connected to is the Dynatel host computer. Here's another number on the Dynatel network: 1-800-801-0139. This is the number for US West. There is one for every Baby Bell across the country. And about the ANI number the lineman gave you, I would be willing to bet it's not good anymore. They change them every month. One other note about the Dynatel: since every unit is networked and you need a password for them, it's useless to "acquire" one of them. As soon as they come up missing, even if you do know the password, they get taken off the network. They can still perform some functions, but the point in having one would be so you could explore the vast possibilities. This would be hard to do with a "crippled" 655.

PhreakHolio
Colorado Springs

***Dear* 2600:**

I used a trick I found in an old issue. A laundromat near my place has an old bill/coin changer, so I photocopied a $10 bill and fed it in the slot. I made myself about $200. The guy who owns the place must be on glue, cause he hasn't caught on yet. Whenever I'm broke I just photocopy $10 bills and take 'em down and get the quarters, then take the change to the arcade and get bills. Also for anyone travelling in Vancouver, Canada, the phony bills also work in the Skytrain terminals, a great way to travel for almost free. Also if you buy a 1 zone fare with a 10, you get $8.50 change. Thanks guys, I love my *2600*.

The Mighty Pantharen
N. Vancouver
Canada

Let's get this straight. You're photocopying money, telling everyone in the world about it, announcing your location, and going back to the same places wondering why nobody's catching on? And on top of all that, you're saying that we were the inspiration for all this? It's all very interesting but most people probably want to know when exactly you landed on our planet.

Corrections

Dear *2600*:

I found an error in last quarter's issue. The author of "Stealth Trojans" states that "...the processor will send signals out on the bus telling all the cards that data is being written to port 81F0h. Most cards, however, only look at the lower 16 bits of the address...." Anyone can clearly see that 81F0h fits entirely within a 16-bit address. I believe the intent was that the high bit would be stripped/ignored by the hard disk controller, resulting in a write to port 1F0h.

b00da
Philadelphia

Reality?

Dear *2600*:

Well, first I want to say that your magazine is cool, I just got my first issue. But I have to say something about your movie review of *Hackers*. You said that the raids were like those in real life and I doubt that. I've never been raided, so I don't really know, but it seems wrong to me. He's a hacker.... Why would like 20 guys with machine guns jump through the windows and run upstairs? He's a hacker.... What's he going to do? Throw his computer at them? C'mon now.... They could've sent two guys through the door, with *maybe* a nightstick each and gotten the exact same results!

Also, it says in the back of the magazine that blue box schematic shirts are still only available by request, so here I go.... I'd like a blue box schematic shirt.

Meth

If you look back there again, you'll see that they cost $15 each. We hope you don't think that all letter writers get free subscriptions and t-shirts. That deal only applies to article writers. As for your questions about the reality of raids, we've seen it play out like that all too often. And, like you, we also ask why.

Radio Shack Fun

Dear *2600*:

I have a friend who's homeless. Last year I got him one of those $20 phone cards. He was in a jam and had to use it. He said, "Man, that was a life saver" so this year I thought I would give him the gift that "keeps on giving". I went to Rat Shack. The computer showed they had three tone dialers in the store. After looking around for about 20 minutes the guy told me, "These things always disappear, the drug dealers use them for something." They didn't even have the floor model. I didn't confuse him by telling him drug dealers could afford to *buy* an autodialer if they wanted one. I asked if they had any 6.5mhz crystals. They didn't stock them but he could order it. So he called someone and they had him ask me what it was for. I said, "I don't know, I'm just picking it up." They had him tell me they "don't show anything". I went to another Rat Shack - same story. Three in the computer, none in the store. I'm starting to lose my smile, if you know what I mean. I asked about the crystals - same story. He got someone on the line and asked about the crystal, and listened for a minute. Then he looked at me (I'm 6'4" and weigh 285) and said, "Uhhh, you better talk to him." I told him "forget it". He said thanks and looked relieved. Looks to me like Rat Shack has a new policy. Then I went to a large stationery store near my house and asked for one of those recording greeting cards. The clerk said we usually carry them but Hallmark recalled them all. Nobody knew what the story was. Anybody know anything about the recall?

One last thing: my friend owns a few Chevron stations, so I asked about the satellite dishes on the roofs of the booths. He said it was for credit card verification so they don't use the phone lines. No music, no alarm, just credit cards.

The only way to make anonymous remailers 100 percent secure is to use someone else's account.

Biohazard

Unfriendly Payphones

Dear *2600*:

I went to a restaurant this morning and saw for the first time a Bell Atlantic payphone that didn't accept incoming calls. I understand that cocots wouldn't accept incoming calls for the reason that the owners make no money. But with Bell phones they make out either way. Well, I was curious, so I went to the phone and looked where the number is displayed and the number was there. A wonder since it's not too useful. I checked the number with my ANI (just in case) and went home. At home I called the number and I got a recorded message that said, "The number you have reached... is not in service for incoming calls." How stupid can Bell get? Do you have any ideas for why Bell might do this? I certainly can't understand why.

Michael H.

Whenever something stupid like this happens, you can bet the bottom line is money. The local phone companies don't like it either when payphones are used for incoming calls because the person calling is probably paying much less for the call than an outgoing call from the payphone would cost. Coin calls are grossly overpriced and each calling card call carries a whopping surcharge. Most phone companies are jumping at the chance to turn off incoming service in the name of the fight against drugs or some other nonsense. If enough people fight this, something just might get done.

Questions

Dear *2600*:

For the past several months I have tried and tried to figure out the "free-call" code to SouthWestern Bell telephones. About eight months ago, if you typed in "10362" and then dialed the number you wanted to call, you could avoid the annoying 25 cent deposit. And then it changed to "10649"... but since then, i have yet to figure out the next code. I am fairly new to phreaking, and have since made eight different boxes. I can still easily get a free phone call, don't get me wrong. But I want to figure out *how* to access the codes... and what other codes might lead to. If you try to type in "10362" and the number you wish to connect to, it says "the access

code you have dialed is invalid". So, since you guys are the people to ask, how would I get access to these codes? I have tried the core of SouthWestern Bell, if you know what i mean, and have had no such luck in finding a damn thing. Any suggestions?

NeVeR \FluX/

First off, these "codes" are never intended for free phone service. If you manage to use one of them for that purpose, it's because some dimwit has misprogrammed your central office. It usually doesn't take them too long to realize this. The codes are used to route long distance calls over different long distance companies. But the 10XXX format is becoming obsolete so any list of such numbers won't be telling the whole story. The new format is 101XXXX. That's ten times more codes to find. Good luck.

Dear *2600*:

A friend of mine got the Internet finally. One day while he was swapping files with a guy, he was suddenly kicked off. He went to log back on, and found that in his mailbox was a message. It said something to the point of, "We found you swapping files. Do it again and we'll arrest you." The cool thing is my friend got this guys e-mail address. Now because my friend swears that he was only trading shareware and music, I will give you his address. It reads as follows: Hoover@crc.nsa.gov. When my friend got this e-mail, he was freaked out of his mind. Most of the guys (friends of ours) convinced him that it was a joke. But in the back of my mind, I wonder. Is the NSA taking a part in the crackdown of pirates and hacks?

M

The NSA is a spy organization. That means they're not likely to send out messages announcing their presence. We also doubt they care much about software pirates.

The Winter Cover

Dear *2600*:

I just received the Winter '95/96 issue of *2600* and I'd like to congratulate you on the cover photograph. I was ROTFL.

No doubt critics of the arts could go into detailed analysis and praise of the composition of this work, the stark contrast between the left and right parts of the picture, movement vs. stillness, etc., and the Freudians would be delighted to equate the depicted scene with sexual penetration, etc., but I'll simply say it was hilarious.

I've been a subscriber for a few years and this is by far the best *2600* cover I've seen yet. Again, congratulations!

Christian
Germany

Dear *2600*:

The cover of this month's mag is the best yet!! Is it possible to get it as a .BMP or .GIF once the www site is back up?

Dereks

The .GIF is available on the web site under the "covers" section.

Dear *2600*:

I absolutely love the cover of the Winter 95-96 issue. The look that the dog is giving the camera is the best part of the photo. Anyway, I was wondering if you could tell your loyal readers the story behind the incident depicted on the cover. I noticed that the old Bell van had a *2600* logo on it. Had you guys finally had enough of NYNEX and PSI?

fuLcrum
Miami, FL

The cover was a composite of photos and it also involved a fair amount of touching up. The van that crashed into the phone booths (yes, it really happened) wasn't a phone van at all and had nothing to do with 2600. And Walter (the dog) has never been in New York City. You can check out our web site for a more graphical look at how it was done.

Fun On Planes

Dear *2600*:

For a few years I've used a rather enjoyable "bug" in Airphones. Because I often fly it has actually turned out to be a very convenient method of entertaining oneself on a flight, without causing any major disturbances where something unfortunate may occur (e.g. death). When you use an AT&T Call Me card (a card designed so that one uses it to call a predetermined number, like a parent - but nobody else) with GTE's In Flight phone service, you can use the card to call numbers which have not been specifically configured for the card. What this means is that, using your AT&T Call Me card, you may call any number in the world without the hassle of putting up with their rates which rival 900 numbers in expense.

This little trick has made otherwise boring flights (let's face it, besides being able to start interesting conversations with people around you, there isn't a whole lot that you haven't read in a *2600* over a three hour time period) become even enjoyable.

Oh yeah, thinking that their banning of portable computers on some flights was just another way of controlling us I decided to check it out for myself.... I found my hard drive emits a birdie at 145.150 MHz which actually could be on a comm frequency that they use.

Particle Man (203)

Repression and Hackers

Dear *2600*:

Repressive governments fear open communication. Television and radio stations are often the first targets in military coups. Those who have exceptional skills in dealing with communication technology have a special role to play in supporting or opposing repressive rule. For example, after the coup in Poland in 1981, telecommunications out of the country were cut off for several days. The Indonesian government has prevented radio communication between East Timor and the rest of the world since invading and occupying it in 1975.

Suppose there is a severe clampdown on dissent in your country. Emergency laws are passed limiting free speech. Leading dissidents are arrested. Surveillance of potential opposition groups is intensified. There is a resistance movement, using nonviolent methods such as petitions, rallies, sit-ins, strikes, etc. To be effective, the resistance needs information on impending arrests, information on targets of surveillance, information on opposition activities in other parts of the country, and reliable information to counter government lies. Hackers have skills that could be immensely valuable to the resistance.

What could hackers do that would be most helpful to a nonviolent opposition to government repression? What could and should be done beforehand to make it more difficult for a government to repress dissent? What is likely to encourage hackers to support the resistance rather than (perhaps due to bribes or threats) support the repressive government?

For some years I've been studying nonviolent resistance to repression but have only just scratched the surface. Suggestions would be most welcome.

Brian Martin
Australia

AOL Hell

Dear *2600*:

I have been subscribed to Netcom now for a pretty long time and have been pretty satisfied with their service. Recently I have been absolutely deluged with free disks from AOL in virtually everything I buy. So I thought I would give them a try to find out why so many people have such hate for AOL and its users.

Well I signed on and quickly realized that the AOL interface was a lot more glitter than actual functionality. This is when the real trouble started. I tried to cancel my account online and was presented with the message "to cancel your account please call or write to AOL". O.K. No problem, right? Wrong. I called the 800 number and was sent into their voice mail system.

When you first call you are presented with two choices: 1) To order free software, press one; 2) to cancel your account, press two. So I pressed two and was told by a recorded voice that the current wait to talk to a "customer service representative" was a half hour. I hung up and assumed that they must be busy and I would call back later. Well, I called back for two more days at different times and got the same message.

The third day, just out of curiosity, I pressed 1 on their voice mail to access the operator who takes orders for their free software. *Bingo!* I wasn't even put on hold, my call was put right through. When I explained to the operator what was happening she responded by saying that's just the way it is.

The point is that AOL makes it incredibly easy to sign on by including their free software in just about everything computer related you buy. And they make it incredibly difficult to cancel once you realize how useless and costly their service is.

YUKYUK

We were able to get through without much delay late at night and over the weekend (the number is 800-827-6364). If you're told to wait for a ridiculous amount of time on the phone, you're better off contacting your credit card company and telling them to refuse any further charges. We happen to know Netcom has the same problem - read some of the local netcom newsgroups to see the hell their former customers are going through. In fairness, this kind of thing seems to happen to an awful lot of providers.

Credentials on Credentials

Dear *2600*:

It seems to me that you don't do a lot of research on your zine. In the last issue of *2600*, I read an article about Credentials Services. In this article you start flaming TRW for their Privacy Watch service. Now let's get down to basics about this article. One: Credentials Services is *not* part of TRW. Granted it is a business TRW started but it was sold to an independent company back in October 1994. Two: You fail to explain the rest of the "pitch" and that is that Credentials will remove your name from mailing lists from all major bureaus and keep your name, address, and phone number from being added to any mailing lists that the major three bureaus sell. Three: The letters you can send to telemarketers is one to deter them from continuing to contact you. It does work because you have pre-warned them not to contact them. Four: It kind of bothers me that your zine claims to be informative about things others need to be informed of. But you have an even larger problem when you a) don't research your periodicals and b) purposefully edit the information to suit your needs.

Just for your knowledge I work for Credentials and used to work for TRW. If you have any questions about any of our services please contact us.

Gebby

It seems hard to believe that a credit agency can successfully launch a consumer group whose job it is to keep credit agencies in check. You'll forgive us if we remain skeptical about Credentials' objectivity.

(continued on page 50)

Motorola Cellular Guide

by Mike Larsen

After much deliberation, I decided to include information about Motorola's pagers and their test mode commands. Since pagers aren't as much fun as cellular, along with the fact there isn't much to them, this information is very limited and somewhat brief. I would still like all information pertaing to all of Motorola's pagers sent to me so this article can be updated.

General Disclaimer

This article is not intended to be an aid in cellular fraud. That is both illegal and immoral. Would you like someone to make charges on your phone? If you want free calls, you want to check elsewhere for information pertaining to *boxes*, which is *not* mentioned here.

This article is not intended for use by people with little electronics experience. This is not a tutorial and not intended to be used except by people with previous cellular experience who are familiar with programming cellular phones. There are tons of introductory files all over the net. For more info get into alt.cellular or alt.2600. If you have specific questions, those are the places to start.

I hope to make make future articles more international. However, the U.S. cellular system greatly differs from other countries and we are all ignorant here as to what others are doing (but isn't that *always* the way?).

Any info on hacking the GSM system (at least being able to use different SIM cards in different phones). The term is "SIM locked" and a friend needs to unlock his phone. Please Email *any* info about this.

Send all related info about the new phones with caller ID - manuals, instructions, bugs, etc. If anyone has *any* type of cellular monitoring software that is P.C. based (using a scanner and/or Motorola Bag phone), *email* me immediately!

General User Info

Before getting into the programming of the cellular phone, it is important for the user to know the normal things necessary for day to day operation. While the majority of the stuff in the user's manual is intended for people who have problems programming their VCR, there are a few things that are very important and are only mentioned in the users manual.

I would like to add that while I have extensively worked on finding additional test mode commands, I (nor anyone else) have never worked with the normal operation commands as listed in the sidebar. For example, you will notice sequences with [Fcn], [1] or [Fcn], [0], [7]. This is totally unexplored teritory. Happy hacking! See entering test mode on the new 95xx phones.

Programming Info

Some units have dual NAM's. The ESN prefix is 130 decimal, 82 hex. Motorola can be reached at: 1-800-331-6456.

There are *many* different models of Motorola phones sold under various brand names, if you think it's a Motorola, it probably is.

Determine which access sequence to use:

Hand Held Portable Models

If the phone has an FCN button and no MENU button use sequence 1.

If the phone has no FCN button use sequence 2.

If the phone has a MENU button and an FCN button use sequence 4.

Installed Mobile Phones and Transportable Models

If the phone has no FCN button and no RCL button use sequence 3.

If the phone has an FCN button use sequence 4.

If the phone has a MEM button use sequence 5.

If the phone has an RCL button and no FCN button use sequence 6.

Access Codes for Sequences 1 through 6

1 FCN (SECURITY CODE TWICE) RCL
2 STO # (SECURITY CODE TWICE) RCL
3 CTL 0 (SECURITY CODE TWICE) *
4 FCN 0 (SECURITY CODE TWICE) RCL
5 FCN 0 (SECURITY CODE TWICE) MEM
6 CTL 0 (SECURITY CODE TWICE) RCL

The default security code is 000000. The CTL (control) button is the single black button on the side of the handset.

NAM Programming

1. Turn the power on.
2. Within ten seconds enter the access sequence as determined above.
3. The phone should now show "01" in the left of the display. This is the first programming entry step number. If it does not work, the security code is incorrect, or the programing lock-out counter has been exceeded. In either case you can still program the unit by following the steps under "Test Mode Programming" below.
4. The * key is used to increment each step. Each time you press * the display will increment from the step number, displayed on the left, to the data stored in that step, displayed on the right. When the data is displayed make any necessary changes and press * to increment to the next step number.

5. The SND key is used to complete and exit programing when any STEP NUMBER is displayed.

If you have enabled the second phone number bit in step 10 below then pressing SND will switch to NAM 2. Steps 01 thru 06, 09 and 10 will repeat for NAM 2, the step number will be followed by a "2" to indicate NAM twoT.

6. The CLR key will revert the display to the previously stored data.
7. The # key will abort programing at any time.

Programming Data

Step #	# of digits/range	Description
1	00000-32767	SYSTEM ID
2	3 DIGITS	AREA CODE
3	7 DIGITS	TEL NUMBER
4	2 DIGITS	STATION CLASS MARK
5	2 DIGITS	ACCESS OVERLOAD CLASS
6	2 DIGITS	GROUP ID (10 IN USA)
7	6 DIGITS	SECURITY CODE
8	3 DIGITS	LOCK CODE
9	0333 OR 0334	INITIAL PAGING CHANNEL
10	6 DIGIT BINARY	OPTION PROGRAMMING (SEE NOTE 1)
11	3 DIGIT BINARY	OPTION PROGRAMMING (SEE NOTE 2)

Take care with Motorola's use of "0" and "1". Some options use "0" to enable, some use "1".

NOTE 1: This is a 6 digit binary field used to select the following options:

Digit 1: Internal handset speaker, 0 to enable.
Digit 2: Local Use Mark, 0 or 1.
Digit 3: MIN Mark, 0 or 1.
Digit 4: Auto Recall, always set to 1 (enabled).
Digit 5: Second phone number (not all phones), 1 to enable.
Digit 6: Diversity (two antennas, not all phones), 1 to enable.

On newer models, they have added and changed some numbers. As of the 3/27/92 manual the 6 digit binary field is still the same.

NOTE 2: This is a 3 digit binary field used to select the following options:

Digit 1: Continuous DTMF, 1 to enable.
Digit 2: Transportable Ringer/Speaker, 0=Transducer, 1=Handset.

From the user's manual . . .

Turn On: [Pwr]
Place Call: Enter number, [Snd]
Receive Call: [Snd] or open flip fone
End Call: [End] or close flip fone
Store Number: Phone number, [Sto], 2-digit location number
Recall Number: [Rcl], 2-digit location number
Super Speed Dialing: Directory location number, [Snd]
Changing Entries: Press [Rcl] and the 2-digit location number so that the number to be changed is displayed. Press and release [Clr] to back out each of the digits. Enter a new number and press [Sto].
Call Number Displayed: [Snd]
Microphone Muting: Press [Fcn], [6]. To unmute, press [Fcn], [6]
Lock Unit: [Fcn], [5] or [LOCK]
Unlock: Three digit unlock code. If you make an error, [Clr] and enter again.
Automatic Lock: [FCN], [6] (not all phones) "EnAbLE" will appear if compatible.
Display Unlock Code: Press [Fcn], [0], your six-digit security code, [Rcl].
Changing Your Unlock Code: Press [Fcn], [0], your six-digit security code, your NEW 3-digit unlock code, [Sto].
Review Battery Meter: Press [Fcn], [4] and release.
Adjust Volume: Earpiece - Press and hold [Vol] to increase. Release, press again to decrease. Ringer - [Fcn], then Vol as above.
Recall Last Number Used: [Rcl], [0], [0]
Recall Own Phone Number: [Rcl], [#]
Individual Call Timer: [Rcl], [#], [#]
Resettable Call Timer: [Rcl], [#], [#], [#]
Reset Resettable Call Timer: [Fcn], [0], [7], [Clr]
Cumulative Call Timer: [Rcl], [#], [#], [#], [#]
Access Features: Press [Fcn], [1]. To change features, press [*] and [#] to scroll and [Clr] to change. To exit feature menu, press [END].
Review/Scroll Menu Features: Press [*] or [#]
Status Review: [Fcn], [0], [9], [Rcl], [#] or [*] scrolls messages. To end press [END].
Changing System Type: Press [Rcl], [*]. Repeatedly press [*] until the desired system type appears. To select press [Sto].
Outgoing Call Restrictions: Press [Fcn], [0], 6-digit security code, [1], [Sto]. Phone will place calls only from memory locations 1-10. To change back to unrestricted dialing press [Fcn], [0], 6-digit security code, [4], [Sto].

Digit 3: 8 hour time-out in transportable mode, 0 to enable.

On newer models, they have added and changed some numbers. As of the 3/27/92 manual the 3 digit binary field has become a 5 digit binary field.

Digit 1: Failed Page Indicator (1=Disabled; 0=Enabled)
Digit 2: Motorola Enhanced Scan (1=Enabled; 0=Disabled)
Digit 3: Long Tone DTMF (1=Enabled; 0=Disabled)
Digit 4: Transportable Internal Ringer Speaker (1=Handset; 0=Transdcr)
Digit 5: Eight Hour Timeout (1=Disabled; 0=Enabled)

Test Mode Access

Newer 95xx Phones (Thank you Motorola!!!)

Many newer phones don't require grounding. If your software version number is 9526 (I think) or newer, enter this:

FCN + 0 + 0 + * + * + 8 3 7 8 6 6 3 3 + STO

In case you have trouble remembering the number sequence, it spells out "TESTMODE". Leave it to Motorola to make this easier and easier all the time. I have used this and it does work. This command just backs up my claim even further that ESN changing via handset is a reality. It's a matter of finding the correct combination of keys.

Normal test mode commands work like usual from then on.

For some odd reason, this hasn't been included in all the 95xx phones. I believe they started it in Software 9526. This is only an estimate, so if you have a 95xx flip, let me know what software version you have and whether it works or not so this date can be isolated. Mine is a 9562 that worked.

Installed Mobile Phones and Transportable Models

To enter test mode on units with software version 85 and higher you must short pins 20 and 21 of the transceiver data connector. An RS232 break out box is useful for this, or construct a test mode adaptor from standard Radio Shack parts.

For MINI TR or Silver Mini Tac transceivers (smaller data connector) you can either short pins 9 and 14 or simply use a paper clip to short the hands-free microphone connector.

Hand Held Portable Models

There are two basic types of Motorola portable phones, the Micro-Tac series "Flip" phones, and the larger 8000 and Ultra Classic phones. Certain newer Motorola and Pioneer badged Micro-Tac phones do not have a "flip", but follow the same procedure as the Micro-Tac.

8000 & Ultra Classic Series

If you have an 8000 series phone determine the "type" before trying to enter test mode. On the back of the phone, or on the bottom in certain older models, locate the F09... number. This is the series number. If the *fourth* digit of this number is a "D" you *cannot* program the unit through test mode, a Motorola RTL4154/RTL4153 programer is required to make any changes to this unit.

Having determined that you do not have a "D" series phone, the following procedure is used to access test mode:

Remove the battery from the phone and locate the 12 contacts at the top near the antenna connector. These contacts are numbered 1 through 12 from top left through bottom right. Pin 6, top right, is the Manual Test Mode Pin. You must ground this pin while powering up the phone. Pin 7 (lower left) or the antenna connector should be used for ground. Follow one of these procedures to gain access to pin 6:

1. The top section of the battery that covers the contacts contains nothing but air. By careful measuring you can drill a small hole in the battery to gain access to pin 6. Alternately simply cut the top off the battery with a hack saw. Having gained access, use a paper clip to short pin six to the antenna connector ground while powering up the phone.

2. If you do not want to "destroy" a battery you can apply an external 7.5 volts to the + and - connectors at the bottom of the phone, ground pin 6 while powering up the phone as above.

3. You can also try soldering or jamming a small jumper between pins 6 and 7 (top right to lower left), or between pin 6 and the antenna connector housing ground. Carefully replace the battery and power up the phone. Use caution with this method not to short out any other pin.

4. A cigarette lighter adapter, if you have one, also makes a great test mode adapter as it can be disassembled to give you easier access to pin 6. Many are premarked, or even have holes in the right location. This is because they are often stamped from the same mold that the manufacturer uses for making hands-free adapter kits and these kits require access to the phone's connectors.

Ultra Classic II Series:

Ground Pin 2 to pin 4.

Micro-Tac "Flip" Series:

This phone follows similar methods as outlined for the 8000 series above.

Remove the battery and locate the three contacts at the bottom of the phone. The two outer contacts are raised and connect with the battery. The center contact is recessed. This is the Manual Test Mode connector.

Now look at the battery contacts. The two outer ones supply power to the phone. The center contact is an "extra" ground. This ground needs to be shorted to the test mode connector on the phone. The easiest way to do this is to put a small piece of solder wick, wire, aluminum foil, or any other conductive material into the recess on the phone. Having done this carefully, replace the battery and turn on the power. If you have been successful, the phone will wake up in test mode.

Handsets

Most Motorola handsets are interchangeable, when a handset is used with a transceiver other than the one it was designed for the display will show "LOANER". Some features and buttons may not work, for instance if the original handset did not have an RCL or STO button, and the replacement does, you will have to use the control * or control # sequence to access memory and A/B system select procedures.

Lock/Unlock Procedures

Phones with LOCK buttons: Press LOCK for at least half a second.

Phones with an FCN button: Press FCN 5, note that 5 has the letters J,K, and L for lock.

Phones with no FCN or LOCK button: Press Control 5, control is the black volume button on the side of the handset.

System Select Procedures

Phones with a RCL button: *press RCL *, then * to select, STO to store.*

Phones with no RCL button: *press Control * then * to select, # to store.*

Options are:
CSCAn: *Preferred/Non preferred with system lockout.*
Std A/b, or Std b/A: *Preferred/Non preferred.*
SCAn Ab, or SCAn bA: *Non preferred/Preferred*
SCAn A: *"A" ONLY*
SCAn b: *"B" ONLY*
HOME: *Home only*

These are typical options, some phone's vary. C-Scan is only available on newer models and does not appear unless programed, see below.

Test Mode

Not all commands work on all telephones. If a command is not valid the display will show "ErrOr." Not all numbers have been assigned. Not all numbers have been listed here. Some commands were intended only for Motorola factory applications. (This is the disclaimer in the technical training manual.) I have included all of the other commands I have discovered one way or another. Some that say no function do have a function but it is unknown until it is figured out.

Three test commands are significant for programming and registering the telephone for service: see full descriptions under TEST MODE COMMANDS.

32# Clears the telephone. (Older Motorola allowed either three or fifteen changes in the MIN. After that, the phone had to be sent to Motorola to reset the counter. This is the command they use.)
38# Displays the ESN.
55# This is the TEST MODE PROGRAMMING (as described below).

Test Mode Commands

\# Enter Test Command Mode

00# no function.
01# Restart. (Re-enter DC power start-up routine.) On TDMA telephones, this command has the same effect as pressing the PWR button.
02# Display Current Telephone Status. (This is a non-altering version of the STATUS DISPLAY. On a 14 character display, all the information is shown. On a 7 character display only the information on the second line of a 14 character display is shown. On a 10 character display, all the information on the second line of a 14 character display plus the last three characters of the first line are shown.)
STATUS DISPLAY alternates between:
AAA = Channel Number (decimal).
BBB = RSSI reading for channel.
CDEFGHI are as follows:
C SAT frequency (0=5970, 1=6000, 2=6030, 3=no channel lock).
D Carrier (0=off, 1=on).
E Signalling tone (0=off, 1=on).
F Power attenuation level (0 through 7).
G Channel mode (0=voice channel, 1=control channel).
H Receive audio mute (0=unmuted, 1=muted).
I Transmit audio mute (0=unmuted, 1=muted).
Press * to hold display and # to end.
03# Reset Autonomous Timer. This command results in the reset of the autonomous timer but does not provide any test function on these models.
04# Initializes Telephone to Standard Default Conditions: Carrier Off, Power Level 0, Receiver Audio Muted, Transmit Audio Muted, Signalling Tone Off, SAT Off, Resetting of Watch-Dog Timer Enabled, DTMF and Audio Tones Off, Audio Path Set to Speaker.
05# TX Carrier On (Key Transmitter).
06# TX Carrier Off.

07# RX Audio Off (Mute Receiver Audio).
08# RX Audio On (Unmute Receiver Audio).
09# TX Audio Off.
10# TX Audio On.
11# Set Transceiver to Channel xxxx (receive and transmit in decimal; accepts 1, 2, 3, or 4 digits).
12x# Set Power Step to x; (0, 1-7) 0=Maximum Power (3 Watts), 7=Minimum Power Out.
13# Power Off (shuts off the radio).
14# 10 kHz Signalling Tone On.
15# 10 kHz Signalling Tone Off.
16# Setup. (Transmits a five word RECC message; each of the five words will be "FF00AA55CC33." Transmitter de-keys at the end of the message.)
17# Voice. (Transmits a two word REVC message; each of the two words will be "FF00AA55CC33." Transmitter de-keys at the end of the message.)
18# C-Scan. (Allows for entry of as many as 5 negative SID's for each NAM.)
Newer Motorola phones are equipped with a feature called C-Scan. This is an option along with the standard A/B system selections. C-Scan allows the phone to be programmed with up to five inhibited system ID's per NAM. This is designed to prevent the phone from roaming onto specified non-home systems and therefore reduce "accidental" roaming fees.
1. C-Scan can only be programmed from test mode - power phone up with the relevant test mode contact grounded (see above).
2. Press # to access test mode.
3. Press 18#, the phone will display "0....40000".
4. Enter the first inhibited system ID and press *.

Continue to enter additional system ID's if required. After the 5th entry the phone will display "N2". Press * to continue and add system ID's for NAM 2 as required.
5. If an incorrect entry is made (outside the range of 00000-32767) the display will not advance - press CLR and re-enter. Use a setting of 40000 for any un-needed locations.
6. When the last entry has been made, press * to store and press # to exit, turn off power.

or
(Phones without the C-Scan option used this command to SEND NAM.)
18# SEND NAM. Display shows AA BB where AA=Address and BB=Data. Displays the contents of the NAM, one address at a time, advanced by pressing the * key. The following data is contained in NAM. The test is exited by depressing the # key.

SIDH	Sec. Code
OPT. (1,2,&3)	MIN
MIN1, MIN2	FCHNA
SCM	FCHNB
IPCH	NDED
ACCOLC	CHKSUM GIM

19# Display Software Version Number (4 digits displayed as year and week).
Note: Entering commands 20# through 23# or 27# causes the transceiver to begin a counting sequence or continous transmission as described below. In order to exit from the commands to enter another test command, the # key must be depressed; all other key depressions are ignored.
20# Receive control channel messages counting correctable and uncorrectable errors. When the command starts, the number of the command will be displayed in the upper-right corner of the display. Entering a # key will terminate the command and display two three-digit numbers in the display. The first number is the number of correctable errors and the second is the uncorrectable errors.
21# Received voice channel messages counting correctable and uncorrectable errors. When the command starts, the number of the command will be displayed in the upper right-hand corner of the display. Entering a # key terminates the command and will display two three-digit numbers in display. The first is the number of correctable errors and the second is the uncorrectable errors.
22# Receive control channel messages counting word sync sequence. When the command starts, the number of the command will be displayed in the upper right-hand corner of the display. Entering a # key will terminate the command and display the number of word sync sequences in the display.
23# Receive voice channel messages counting word sync sequences. When the command starts, the number of the command will be displayed in the upper right-hand corner of the display. Entering a # key will terminate the command and display the number of word sync sequences in the display.
24# Receive control channel data and display the majority voted busy/idle bit. 0=idle 1=busy
25x# SAT On. When (x=0, SAT=5970HZ; x=1, SAT=6000HZ; x=2, SAT=6030HZ)
26# SAT Off.
27# Transmit Data. (Transmits continuous control channel data. All words will be "FF00AA55CC33." When the command starts, '27' will be displayed in the right side of the display. Entering a # key will terminate the command. The transmitter de-keys when finished.)
28# Activate the high tone (1150 Hz +/- 55 Hz).
29# De-activate the high tone.
30# Activate the low tone (770 Hz +/- 40 Hz).
31# De-activate the low tone.
32# Clear. (Sets non-volatile memory to zeroes or factory default. This command will affect all counters, all repertory memory including the last number called stack, and all user programmable features including the setting of System Registration. It does not affect the ESN, NAM, phasing data, or lock code. This takes a minute or so. *Do not turn off the telephone while this is showing '32' on the display. Wait until the normal service level display resumes!*)
33x# Turn on DTMF for x (1-9, *, 0, #, plus the single tones)
x= 1: 697 Hz + 1209 Hz
x= 2: 697 Hz + 1336 Hz
x= 3: 697 Hz + 1477 Hz
x= 4: 770 Hz + 1209 Hz
x= 5: 770 Hz + 1336 Hz
x= 6: 770 Hz + 1477 Hz
x= 7: 852 Hz + 1209 Hz
x= 8: 852 Hz + 1336 Hz
x= 9: 852 Hz + 1477 Hz
x= *: 941 Hz + 1209 Hz
x= 0: 941 Hz + 1336 Hz
x= #: 941 Hz + 1477 Hz
x=10: 697 Hz
x=11: 770 Hz
x=12: 852 Hz
x=13: 941 Hz
x=14: 1150 HZ (not used in cellular)
x=15: 1209 Hz
x=16: 1336 Hz
x=17: 1477 Hz
x=18: 1633 Hz (not used in cellular)
x=19: Turn DTMF off
x=20: 2087 Hz
x=21: 2308 Hz
x=22: 2553 Hz (not used in cellular)
x=23: Turn DTMF off
x=24: 3428 Hz (not used in cellular)
x=25: 3636 Hz (not used in cellular)
x=26: 4000 Hz (not used in cellular)
x=27: 3555 Hz (not used in cellular)
x=28: 4571 Hz (not used in cellular)
x=29: Turn DTMF off
(Someone please check out 24 thru 28 for accuracy. I had weak equipment.)
34# Turn DTMF Off.
35# Display RSSI ("D" Series Portable Only).
or
35x# Set Audio Path to x.
x=0 V.S.P Microphone (applies to mobiles only)
x=1 Speaker
x=2 Alert
x=3 Handset
x=4 Mute
x=5 External Telephone (applies to portables only)
x=6 External Handset (applies to *newer* portables)
36nnn# Scan. (TDMA telephones only. Scans the primary control channels and attempts to decipher the forward data stream. The display will show PASS1 if the strongest control channel was accessed, PASS2 if the second strongest was accessed, and FAIL if no control channel could be accessed.)
(nnn=Scan speed in milliseconds) Tunes from channel 1 to 666 in order. Entering a * pauses the scan and displays current Channel Number and RSSI reading (AAA=Channel Number and BBB=RSSI Reading). When scan speed is 300 milliseconds or greater, the current status is displayed during the scan; when less than 300 milliseconds the status is displayed only during pause. Entering * during a pause causes the scan to resume. Entering # aborts the scan and leaves the mobile tuned to the current channel. During this command only the * and # keys are recognized.
37# Sets Low Battery Threshold. Usage: #37#x# where x is any number from 1 to 255. If set to 1, the Low Battery indicator will come up when the phone is powered on. If set to 255, it may never come up.
38# Display ESN. (Displays ESN in four steps, two hexadecimal digits at a time in a four digit display. The decimal shows the address, 00 through 03 as the first two digits, and two digits of the ESN as the last two digits. Use the 'G' to step through the entire hexadecimal ESN.)
Compander OFF. ("D" Series Portables)
or
38# SND-SNM. Display shows AA BB. Where AA=Address; BB=Data. Send the SNM to the display. All 32 bytes of the SNM will be displayed, one byte at a time. The byte address will be displayed in the upper right-hand corner and the contents of that address will be displayed in the hex. The * key is used to step through the address similar to the SEND-NAM (18#) command.
39# Compander ON. ("D" Series Portables)
or
39# RCVSU. Receive one control channel word.

When the word is received it is displayed in hex. This command will be complete when a control channel word is received or when the # key is entered to abort the command.

40# RCVVC. Receive one voice channel word. When the word is received it is displayed in hex. This command will be complete when a voice channel word is received or when the # key is entered to abort the command.

41# Enables Diversity. (on F19CTA... series only)

42# Disables Diversity. (on F19CTA... series only)

43# Disables Diversity.
Use T/R antenna (on F19CTA... series only)
Use R antenna (on D.M.T./ mini TAC)

44# Disables Diversity.
Use R Antenna (on F19CTA... series only)
Use T/R antenna (on D.M.T./ mini TAC)

45# Display Current Receive Signal Strength Indicator. (Displayed as a 3 digit decimal number) The strongest signal I have ever received was 179 and I was sitting directly below the tower *without* an external antenna.

46# Display Cumulative Call Timer.

47x# Set RX Audio level to X.
(For F19CTA ...Series Tranceivers)
X= 0 Lowest Volume
X= 6 Highest Volume
X= 7 mute
Normal setting is 4.
(For D.M.T./ Mini TAC Tranceivers)
X= 0 Lowest Volume
X= 7 Highest Volume
Normal setting is 4.
(For TDMA Tranceivers and F09F... Series and Higher Portables)
X= 0 Lowest Volume
X=15 Highest Volume
Normal setting is 2 to 4. (On TDMA transceivers and Micro TAC portables, settings 8 through 15 are for DTMF applications only.)

48# Side Tone On. Use this command in conjunction with 350# to test the entire audio path in hands-free applications.

49# Side Tone Off.

50# Maintenance data is transmitted and test results displayed:
PASS =received data is correct
FAIL 1 =2second timeout, no data rec.
FAIL 2 =received data is incorrect

51# Test of mobile where maintenance data is transmitted and looped back.
Display is as follows:
PASS =looped-back data is correct.
FAIL 1 =2 second timeout, no looped-back data.
FAIL 2 =looped-back data is incorrect.

52x# SAT Phase Adjustment. A decimal value that corresponds to phase shift compensation in 4.5 degree increments. Compensation added to inherent phase shift in transceiver to achieve a total of 0 degrees phase shift.
Do *not* enter any values except those shown below.

0 = 0	121.5 = 59	243.0 = 86
4.5 = 1	126.0 = 60	247.5 = 87
9.0 = 2	130.5 = 61	252.0 = 112
13.5 = 3	135.0 = 62	256.5 = 113
18.0 = 4	139.5 = 63	261.0 = 114
22.5 = 5	144.0 = 40	265.5 = 115
27.0 = 6	148.5 = 41	270.0 = 116
31.5 = 7	153.0 = 42	274.5 = 117
36.0 = 16	157.5 = 43	279.0 = 118
40.5 = 17	162.0 = 44	283.5 = 119
45.0 = 18	166.5 = 45	288.0 = 120
49.5 = 19	171.0 = 46	292.5 = 121
54.0 = 20	175.5 = 47	297.0 = 122
58.5 = 21	180.0 = 64	301.5 = 123
63.0 = 22	184.5 = 65	306.0 = 124
67.5 = 23	189.0 = 66	310.5 = 125
72.0 = 48	193.5 = 67	315.0 = 126
76.5 = 49	198.0 = 68	319.5 = 127
81.0 = 50	202.5 = 69	324.0 = 104
85.5 = 51	207.0 = 70	328.5 = 105
90.0 = 52	211.5 = 71	333.0 = 106
94.5 = 53	216.0 = 80	337.5 = 107
99.0 = 54	220.5 = 81	342.0 = 108
103.5 = 55	225.0 = 82	346.5 = 109
108.0 = 56	229.5 = 83	351.0 = 110
112.5 = 57	234.0 = 84	355.5 = 111
117.0 = 58	238.5 = 85	360.0 = 70

53# Enable scrambler option, when equipped.

54# Disable scrambler option, when equipped.

55# Display/Program N.A.M. (Test Mode Programming).

Test Mode Programming:

The following steps are for software version 9308 and older. If you have a newer phone they will most likely be different. The newer phones with Caller ID are for sure. *Send me the new programming steps so I can update these!!!* I don't want to hear that they were wrong unless there are corrected steps following!!!

Assuming you have completed one of the above steps correctly, the phone will wake up in test mode when you turn the power on. When you first access test mode, the phone's display will alternate between various status information that includes the received signal strength and channel number. The phone will operate normally in this mode. You can now access Service Mode by pressing the # key, the display will clear and a ' will appear. Use the following procedure to program the phone:

1. Enter 55# to access programing mode.
2. The * key advances to the next step. (Note that test mode programming does *not* have step numbers. Each time you press the * key the phone will display the next data entry.)
3. The CLR key will revert the display to the previously stored data.
4. The # key aborts programing at any time.
5. To complete programing you must scroll through *all* entries until a ' appears in the display.
6. Note that some entries contain more digits than can be displayed by the phone. In this case only the last part of the data can be seen.

Test Mode Programming Data for AMPS and NAMPS Cellular Telephones:

Step #	# of digits/range	Description
1	00000 - 32767	SYSTEM ID
2	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 1 BELOW
3	10 DIGITS	MIN (AREA CODE & TEL#)
4	2 DIGITS	STATION CLASS MARK, SEE NOTE 2 BELOW
5	2 DIGITS	ACCESS OVERLOAD CLASS
6	2 DIGITS	GROUP ID (10 IN USA)
7	6 DIGITS	SECURITY CODE
8	3 DIGITS	LOCK CODE
9	3 DIGITS	SERVICE LEVEL, SEE NOTE 3 BELOW
10	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 4 BELOW
11	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 5 BELOW
12	0333 OR 0334	INITIAL PAGING CHANNEL
13	0333	"A" SYSTEM IPCH
14	0334	"B" SYSTEM IPCH
15	3 DIGIT	NUMBER PAGING CHANNEL (021 IN USA)
16	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 6 BELOW

Steps 01 through 06 and 12 will repeat for NAM 2 if the second phone number bit has been enabled in step 11.

Test Mode Programming Data For TDMA Cellular Telephones:

Step #	# of digits/range	Description
1	00000 - 32767	SYSTEM ID
2	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 1 BELOW
3	10 DIGITS	MIN (AREA CODE & TEL#)
4	2 DIGITS	STATION CLASS MARK, SEE NOTE 2 BELOW
5	2 DIGITS	ACCESS OVERLOAD CLASS
6	2 DIGITS	GROUP ID (10 IN USA)
7	6 DIGITS	SECURITY CODE
8	3 DIGITS	LOCK CODE
9	3 DIGITS	SERVICE LEVEL, SEE NOTE 3 BELOW
10	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 4 BELOW
11	8 DIGIT BINARY	OPTION PROGRAMMING, SEE NOTE 5 BELOW
12	0333 OR 0334	INITIAL PAGING CHANNEL
13	0333	"A" SYSTEM IPCH
14	0334	"B" SYSTEM IPCH
15	3 DIGITS	DEDICATED PAGING CHANNELS (021 IN USA)
16	3 DIGITS	SECONDARY INITIAL PAGING CHANNEL. 708 for system A, 737 for system B. Allows the TDMA telephone to be assigned to a TDMA channel in a call
17	708	SECONDARY INITIAL PAGING CHANNEL FOR SYSTEM A
18	737	SECONDARY INITIAL PAGING CHANNEL FOR SYSTEM B
19	8 DIGITS	OPTION PROGRAMMING, SEE NOTE 6 BELOW

NOTES

Take care with Motorola's use of "0" and "1". Some options use "0" to enable, some use "1".

These are eight digit binary fields used to select the following options:

1. (step 02 above, suggested entry is: 11101001 for "A" system, 10101001 for "B" sys)

Digit 1: Local use mark, 0 or 1.
Digit 2: Preferred system, 1=system A, 0=system B.
Digit 3: End to end (DTMF) dialing, 1 to enable.
Digit 4: Not used, enter 0. Formerly used for test mobile.
Digit 5: Repertory (speed) dialing, 1 to enable. (Not used in TDMA)
Digit 6: Auxiliary (horn) alert, 1 to enable.
Digit 7: Hands free (VSP) auto mute, 1 to enable (mutes outgoing hands free audio until the MUTE key is pressed). (Not used in TDMA)
Digit 8: Min mark, 1. NOT CHANGEABLE.

2. Station Class Mark

SCM	666 or 832 Ch.	VOX	Max Power
0	666	N	3.0 W
1	666	N	1.2 W
2	666	N	0.6 W
3			
4	666	Y	3.0 W
5	666	Y	1.2 W
6	666	Y	0.6 W
7			
8	832	N	3.0 W
9	832	N	1.2 W
10	832	N	0.6 W
11			
12	832	Y	3.0 W
13	832	Y	1.2 W
14	832	Y	0.6 W
15			

3. Service Level Codes:

1 The telephone will only dial numbers in memory locations 01, 02 and 03. No keypad entries or memory storage is possible. Restrict *all* outgoing calls by clearing locations 01, 02, and 03 and place the phone in servicing level 001. In some phones this applies to memory locations 01 - 10.
2 The telephone will dial only numbers from memory locations. The keypad is disabled and super speed dialing is not enabled.
3 Keypad dial only; no memory recall allowed.
4 Unlimited keypad and memory dialing. (DEFAULT)
5 Seven-digit dialing only
6 Full keypad and memory dialing, but memory locations 1 through 10 cannot be changed.
7 The phone will dial only from as many as 50 programmable memory locations

4. (step 10 above, suggested entry is: 00000100)

Digit 1: Not used in USA, enter 0.
Digit 2: Not used in USA, enter 0.
Digit 3: Not used in USA, enter 0.
Digit 4: Extended Field. When enabled, the telephone will scan more than 32 paging channels. Not used in USA, 0 to disable.
Digit 5: Single system scan, 1 to enable (scan A or B system only, determined by bit 2 of step 02. Set to "0" to allow user the option).
Digit 6: Super speed dial, 1 to enable (pressing N, or NN SND will dial the number stored in memory location NN).
Digit 7: User selectable service level, 0 to enable (allows user to set long distance/memory access dialing restrictions).
Digit 8: Lock function, 0 to enable (allows user to lock/un-lock the phone, if this is set to 1 the phone cannot be locked).

5. (step 11 above, suggested entry is: 00000000)

Digit 1: Handset programing, 0 to enable (allows access to programming mode without having to enter test mode).
Digit 2: Second phone number (not all phones), 1 to enable.
Digit 3: Call timer access, 0 to enable. (Not used in TDMA)
Digit 4: Auto system busy redial, 0 to enable.
Digit 5: Internal Speaker disable, 1 to enable (use with select VSP units only, do not use with 2000 series mobiles).
Digit 6: IMTS/Cellular, 1 to enable (rarely used).
Digit 7: User selectable system registration, 0 to enable.
Digit 8: Dual antenna (diversity), 1 to enable.

6. (step 16 and 19 above, suggested entry is: 0011010 for portable and 0011011 for mobile units)

Digit 1: Enhanced Scan, when enabled, four strongest signalling channels are scanned insted of two. 1=enabled, 0-disabled.
Digit 2: Cellular Connection, used only in series II phones if a series I cellular connection is used with a series II. 0=series II, 1=series I, 0 for ALL TDMA PHONES
Digit 3: Continuous DTMF, 1 to enable (software version 8735 and later)
Digit 4: Transportable Internal Ringer/Speaker. When set to 0, audio is routed to the external speaker of the transportable; 1 routes it to the handset.
Digit 5: 8 hour time-out, 0 to enable (software version 8735 and later)
Digit 6: Not used, 0 only.
Digit 7: Failed page indicator, 0 to enable (phone beeps when an incoming call is detected but signal conditions prevent completion of the call).
Digit 8: Portable scan, 0 for portable, 1 for mobile units.

56# Illumination Diagnostic. Lights up all lights (except the green in use light) and displays all 8's. The phone is also muted until repowered.
57x# Call Processing Mode.
x=0 AMPS
x=1 NAMPS
x=2 RESERVED
x=3 RESERVED
x=4 RESERVED
x=5 TDMA signalling
x=6 TDMA signalling with loopback before decoding
x=7 TDMA signalling with loopback voice after decoding
x=8 TDMA signalling with loopback FACCH after decoding
x=9 TDMA forced synchronization
58# Compander On. (Audio compressor and expander) (See 39#)
59# Compander Off. (Audio compressor and expander) (See 38#)
60# no function.
61# ESN Transfer. (for Series I D.M.T./Mini TAC only)
62# Turn On Ringer Audio Path.
63# Turn Off Ringer Audio Path.
64# Does something, doesn't display anything.
65# Does something, doesn't display anything.
66# Identity Transfer. (Series II Transceivers and some Current Shipping Portables)
67# Displays two 3 digit numbers. If you keep entering this command repeatedly, the first number will constantly change, the second won't (as far as I have seen).
68# Display FLEX and Model Information.
69# Used with Identity Transfer.
70# Abbreviated field transmitter audio deviation command, for transceivers with FCC ID ABZ89FT5668.
71# Abbreviated field power adjustment command, for transceivers with FCC ID ABZ89FT5668.
72# Field audio phasing commands. The left side of the display should read "00" followed by a two digit number. The "00" indicates the first programming step. If you press the *, the 00 changes to 01 and so on until 08. The "06" and "0A" are used to change the audio level (to change: press the volume up or down keys). Other registers... don't know.
73# Field power adjustment command.
74-99# no function.

Commands 74#, 75#, 76#, 77#, 78#, 80#, and 99# actually have unknown functions. As new phones come out, more commands are added/deleted as needed. The majority of these commands were figured using *very* old software versions. Some commands won't work on some phones. If you find a command that does something, please inform me as well as the software version number of the phone it was discovered on.

The author can be emailed at: Mike.Larsen@bbs.uti.com

2600 Marketplace

Happenings

ACCESS ALL AREAS II. Computer Security & Hacking Conference July 6th and 7th, 1996. London, UK. Aimed at computer hackers, phone phreaks, computer security professionals, cyberpunks, law enforcement officials, net surfers, programmers, and the computer underground. It will be a chance for all sides of the computer world to get together, discuss major issues, learn new tricks, educate others, and meet "The Enemy". For further information, contact one of the following - web: http://www.access.org.uk, email: aaa-info@access.org.uk, fax: +44 (0) 1428 727 100, phone: +44 (0) 973 500 202.

DEF CON IV. July 26-28, 1996 at the Monte Carlo Hotel in Las Vegas. Among the fun activities planned: Hacker Jeopardy, Capture The Flag hacking contest. Email: dtangent@defcon.org, website: http://www.defcon.org, phone: 206-626-2526, write: 2709 E. Madison, Seattle, WA 98112. $30 in advance, $40 at the door.

For Sale

CONTRIBUTE TO THE WALTER FUND! Since being hit by a car in October, the *2600* mascot has been featured on the Winter cover, has had over 10,000 visits to his web page, and, most importantly, has gotten back onto his feet. You can help lessen the weight of his medical bills by getting an official Walter t-shirt for $20. We'll even throw in a free HOPE shirt from the 1994 hacker conference! Send cash or make checks payable to cash. 2600 Walter Fund, PO Box 848, Middle Island, NY 11953. Check Walter's progress on the 2600 web site (www.2600.com) or finger walter@2600.com for the latest update. (If you already contributed and you want a HOPE shirt, just contact us.)

DMV 96! Department of Motor Vehicles databases on CD-Rom. Oregon $219, Texas $495, Florida $495. 503-325-0861. Bootleg Software, 392 Alameda, Astoria, OR 97103.

6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S. add $12 per order in U.S. funds. For other quantities, include phone number and needs. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

FREE MONEY! Yes, this method works! You can actually get money from money changing machines without actually breaking into them. Other products such as HOW TO GET FREE ELECTRICITY and How to Beat the Bill Collectors! All of the methods we send out work. AND, you can actually change your fingerprints. This method has helped others make their "move" on society. You can too. Send SASE and $10 to cover expenses. Refunded on any order. Write to Alan, P.O. Box 800066, Houston, TX 77280-0066.

SELLING MICROSOFT OFFICE 95 PROFESSIONAL for $175 brand new. Microsoft Windows 95 training videos all levels starting from $39.95 and up. Call InterSoft Development Group, Inc. at (847) 679-7252.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

6.55 MHZ CRYSTALS FOR SALE CHEAP. 1 for $1.50, 10+ $1.25 each, 100+ $1 each. Contact root@kaht.ponyx.com for info or send orders to B. Buckman, PO Box 225, Middleboro, MA 02346.

THE BLACK BAG TRIVIA QUIZ: On MS-DOS disk. Interactive Q&A on bugging, wiretapping, locks, alarms, weapons, and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining and VERY educational. Includes selected shareware catalog and restricted book catalog. Send $1 ($1.50 for 3.5) and 2 stamps to: Mentor Publications, Box 1549-Y, Asbury Park, NJ 07712.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or first class mail. Copy of 1971 *Esquire* article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

HACK THE PLANET. A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send $3.00 check or money order payable to CASH. Also available is an MCI-style black hat with white lettering that says PHONE PATROL, only $18. 2447 Fifth Avenue, East Meadow, NY 11554-3226.

FREE PHONE CALLS FOR LIFE! New video "How To Build a Red Box". VHS 60 min. Complete step by step instruction on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain FREE calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch, and more! This video will save you thousands of dollars every year. Best investment you'll ever make! Only $29 US and $5 for shipping & handling. We sell 6.50 MHz crystals too! CABLE TV BOXES: Enables you to receive "every pay channel" for FREE as well as pay-per-view. Stop paying outrageous fees for pay channels. You must call or e-mail us first and tell us the "brand" and "model number" of the cable box you have. Only $210 U.S. & $10 shipping & handling. 30 day money back guarantee! Send check or money order to: East America Company, Suite 300H, 156 Sherwood Place, Englewood, NJ 07631-3611. Tel: (201) 343-7017. E-mail: 76501.3071@compuserve.com. Free technical support!

X-PHILES HPA CD-ROM. The most complete HPA CD-Rom available today, containing over 21,000 files about hacking, phreaking, anarchy, occult, drugs, conspiracy, UFO's, programming in all languages, HP48, security, hardware, weapons, science, survival, cellular hacking, cyberspace.... The price is $29.95+ shipping. Write to X-Philes, Tranbaersvaegen 25:14, 37238 Ronneby, Sweden. Email dt93tn@pt.hk-r.se, http://www.algonet.se/~synchron for more information.

THE WHACKED MAC ARCHIVES CD. This CD includes almost 200 different files and utilities including war dialers, virri, phreaking utilities, text files, cracking utilities, and much much more. Everything you need to get your Mac completely Whacked. This collection will be especially useful to all Macintosh users, network administrators, hackers, computer security professionals, phreakers, computer teachers, crackers, lab monitors, virus writers, communication specialists, and anyone who deals with Macintosh systems on a day to day basis. If you have been searching for that hard-to-find utility or program you can probably find it on the Whacked Mac Archives. To learn more about the CD and who we are check out http://www.l0pht.com/~spacerog/index.html. To order your own Limited Edition copy of the Whacked Mac Archives, please send name, address, postal code, and country to: The Whacked Mac Archives, c/o L0phT Heavy Industries, P.O. Box 990857, Boston, MA USA 02199-0857. Please include $19.95 plus $4.50 for shipping and handling in United States dollars for each CD ordered. We will ship anywhere in the world via First Class U.S. Mail. Cash, checks or money orders accepted, sorry no credit card orders. Please make checks payable to L0phT Heavy Industries. Massachusetts residents please add 5% sales tax. Please allow four to six weeks for delivery.

ABSOLUTE POWER CORRUPTS ABSOLUTELY!! Arm yourself with knowledge and information for the Information Age. Get information on hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. We can supply you with files, programs, manuals, and memberships from our elite organization. Legit and recognized world-wide. Our QUALITY information sources and resources will elevate you to a higher plane of consciousness. Coming soon: Hack videos. For a full catalog send $1 to: SotMESC, Box 573, Long Beach, MS 39560, USA. Over 3,000 catalogs distributed.

Help Wanted

NEED HELP to clear my credit reports. Please respond to M.D. Hall, P.O. Box 162, 5025 N. Central, Phoenix, AZ 85012.

PLEASE HELP CLEAN MY CREDIT REPORT. Reward. G. Pierre, 33 S. Broadway #312, Yonkers, NY 10701.

HELP WANTED. I live in England, our telephone system is British Telecom. I keep receiving malicious calls. I use the British version of caller identification device. They type in 141 to block their number from showing up on my caller display. I need either information or a gadget to trace the phone caller or to reveal or unblock their number. I will pay for any equipment, gadgets, and postage in U.S. funds. Please help. Send to: Lee J. Round, 25 Plawsworth Road, Sacriston, Co. Durham, DH7 6PD, England.

Bulletin Boards

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. WWW: http://anarchy-online.com - telnet: anarchy-online.com - modem: (214) 289-8328.

ACCESS DENIED BBS (613) 226 5386. Info exchange for H/P/V/C subjects. Willing to exchange info with anyone. Need info on CID, ANI, and other "phreaking" utils. Send email to visible.daemon@eidetic.takeone.com.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion. Deadline for Summer issue: 5/31/96.

(continued from page 37)

Crippled 911

Dear *2600*:

I was at a Mosholu Woodlawn South Community Coalition meeting in the Bronx recently. The captain of the 52nd precinct told us that the precinct has a highly increased workload over the last month because they got new Caller ID. Now they have to send a car to respond to every aborted call that comes in, even every hang up call. Their caller ID identifies not only the caller phone number but the phone subscriber's name, address, and apartment number.

Ben Stock

It's actually not Caller ID that's causing this problem but, rather, the new Enhanced 911 system. Believe it or not, it's supposed to save time.

Disney Critique

Dear *2600*:

I can't believe how many inaccuracies there were in this article. As a former cast member at WDW I can tell you that the majority of "facts" listed in the article were gross errors. You really should check your articles before they are printed. Not doing so hurts the reputation of your publication.

Michele Warner

It sure would be helpful if you shared with us some of the inaccuracies. Fortunately, someone else did.

Dear *2600*:

I usually find that your mag has well researched, quality information and articles... until I read your Winter 95-96 issue. Don't get me wrong. It was all great, except for one article, "Infiltrating Disney" by Dr. Delam. I would urge the good doctor to quit taking the "Lysergic Acid Diethylamide" as he mentions at the end of the article... and begin checking his facts. Here are just a few minor corrections. WDW in general is not guarded by a moat. The Magic Kingdom is on one side, for a small area. The stupidest place to try and sneak in would be by Space Mountain because that is where there are not only the most guard stations, patrolling security cars, and cameras, but also the so-called moat. In addition, the tunnels are not underground, they are actually at ground level. WDW is built above ground level, and it does not go to each land... only four out of the seven, and I would hardly call it a ring at all. It does not even remotely resemble any standard shape. The second main point I would like to correct is about sneaking down into the "tunnels" (the correct name is utilidoors). It would be *very* stupid to go into the doors that Dr. Delam mentioned because this is one of the ones with the most traffic. It would be a lot smarter (although quite stupid to try and sneak down at all) to go down in the doors by Liberty Square behind the silversmith's shop in the Pocahontas Cove area. Very little traffic back there. Even if you did get down without anyone asking you questions, you very likely would not go more than 50 feet without being apprehended. The castmembers (not actors as the author said) do wear nametags, and you would be questioned very quickly... take this from someone who was escorted down numerous times by castmembers. The computer control room is nowhere near where Dr. Delam said it was and there is *no* security device like the one described on the door. A numerical keypad, yes, but a hand print reader?!?! *No!!!* Another fact that he got wrong was the job interview. These do not take place in any of the parks. These take place in the casting center, a rather large building by Pleasure Island. The only time you would get taken into the park would be after you are hired and that would be for training. Finally, there are a lot less surveillance cameras than people think and a lot *more* undercover security people. If anyone is interested in a real "hacking Disney" article, I was considering writing one detailing the workings of their *huge* VMB system in place at their resort. Anyone interested?

The Imagineer

No article that we have ever printed has resulted in such empassioned and emotional responses. We never cease to be amazed by the power of Disney.

An Edward A. Smith Theory

Dear *2600*:

In the Autumn 1995 issue letters column, pbixby writes of the AT&T cable ship "Edward A. Smith", with an editorial comment about its reserved exchange in the 500 area code. I'd like to speculate about the purpose of assigning the exchange to the ship. It seems logical to have a permanently assigned exchange that will follow the ship no matter where it goes. After all, won't the cable the ship lays need to be tested? If so, having a reserved exchange would be extremely convenient for this purpose. No matter where in the world the ship was operating, there would be a phone number that could be routed through the cable being laid, thus providing a ready-made test circuit. If this is true, it would be interesting to see what could be done by dialing numbers in the Edward A. Smith's exchange.

some guy

Cincinnati Bell Nightmare

Dear *2600*:

Recently I had two new phone lines added to my house, bringing me up to a total of four. But the phone company (Cincinnati Bell) had a few surprises for me when they added them. They told me that in order to add the new phone lines, they would have to come out and upgrade the wiring on my private lane because currently you could have no more than two lines per house. So I agreed and all. I was coming home one day, and I found that my street looked like a level on Pac-Man. Different multi-colored symbols and arrows *everywhere*, orange, yellow and green. Sure, you see these things all the time on sidewalks, like maybe one "T-T" or a yellow arrow or something, but this was crazy. And not just on the street, I mean on everybody's lawns and porches too. No lawn on the street was left untouched. So I walk up to the guy doing this (who was armed with 3 or 4 cans of spray paint) and asked him what the hell he thought he was doing. He said that he was from the phone company and that he was just doing what they told him to do. I noticed that his van was not a telco truck, but rather an unmarked Chevrolet van. I figured that since it was the weekend he just drove over in his own van, no problem, so I didn't bother to ask. So a few days later Cincinnati Bell shows up to begin "work" in their marked vans. Four of them. They worked for a few weeks (once about every two or three days) and finally finished up and got the lines installed. But I asked him what the other guy was there for and they gave me the basic equivalent of "Duh, I dunno" and wouldn't listen to my complaints (nor those of the several neighbors who had their houses vandalized). So now my street is painted multi-colored, which hasn't faded at all in the many rains and several feet of snow we have had, thanks to our good friends at the phone company.

Mr iNSaNiTY

Sounds like your local TV news might have fun with this one.

Understanding the Hacker

Dear *2600*:

I'm a new reader to this cool magazine. I picked up a copy of *2600* at a store (Volume 12, number 4, Winter 95-96) and had to buy it. As I was reading it I came across the article "Understanding the Hacker" by Bootleg. I would like to say that I totally agree with everything it said. The greatest part was the idea of no more wars with guns, but with knowledge that hackers crave for and can't get enough of. Thank you Bootleg.

Sevangles (Seven Angles)

56K ISDN Link

Dear *2600*:

In your last issue (and on your web page) I was reading about the ordeal with PSInet. Well, I'm glad you got your money back and such, but I have a question: did you ever find a 56k data-over-voice ISDN provider? I have been desperately seeking one myself (I live in northern NJ). Please let me know if you found any.

I also just read more about Bernie S... the more and more I read about it, the more and more I can't believe that is *actually* happening. The things going on are *so* ludicrous the story just feels fictitious. They were prosecuting him for possession of the *Anarchist Cookbook*? Christ, you can go buy that at Walden Books or B. Dalton! How can the not-so-Secret wanna-be-Service get away with such a horrid event?

ThePawn

We had no problem finding another provider who helped us with 56k connectivity. Not all NYNEX lines can handle this but we knew that when we started the project. We suggest you ask local providers in your area if they support 56K ISDN data over voice and make sure they know exactly what you're talking about. And keep pushing for a flat rate ISDN service so we can just use 64K and not have to pay their ridiculous per-minute surcharge. Good luck.

Netware Nonsense

Dear *2600*:

I have for the most part been very impressed with the level of technical knowledge and creativity that I have found in *2600*. I always wait impatiently for the next issue to arrive at my local Borders Book Store.

Today is the first time I can honestly say that what I was reading was gibberish. I refer to the article titled "Hacking Netware" from the Winter 95-96 issue.

With all due respect to Trap, I would agree with his opening line "Reading through the book..." It would appear that Trap has done little else than that with regard to Netware. (We will not bother with the fact that Netware 3.11 is horribly outdated.)

The first half of the article is purely speculative: "What if I could dial in...." and "If I can get access to the backup account by going to work after hours...." types of fantasy. There are two Netware backup solutions that are the most prevalent.... Both are based on the server console which means that day to day operations *do not require* you to login to a workstation. Only when you desire to modify or add additional sessions is there a need to login, and that login account does not need any exceptional privileges to execute the management software.

There is no knowledge or experience showing here on the part of Trap.

Further statements such as "All information about where and when a specific login ID has logged in is recorded in the Bindery..." is just simply wrong. Login/out info is recorded in a file called NET$ACCT.DAT, and *only* if the accounting feature is enabled on the server. Do not mistake all NET$ files as Bindery files.

Also make note that the correct spelling is BINDERY not BINDARIES.

The second half of the article is partially right... the correct part is that Novell *will* ask for the name of the licensee. The wrong part is that they would ever give out a "back door" password. Anyone even remotely familiar with Netware should know that you can always re-enable the supervisor password at the console, or in the worst case by power cycling the server. (Not the preferred

method but Novell would rather have you do this than admit to having a back door into every Netware server.)

Another important thing to note is that not only will Netware report failed login attempts to a file, but also to the System Console (by default) with the Network ID (wire number) and ethernet card address. So be prepared to spoof IPX packets with Packet Signatures (something I would personally like to see).

Trap's article does make one point very clear to Novell CNA/CNE types though... people *do* think about how to break into Netware systems, however misinformed they may be. I would hope that before Novell Hack II comes out, that Trap gets some experience and *does his research!*

Gandolf

Words of Praise

Dear *2600*:

I just bought my first copy of your mag. Wow. Nice to know there are people out there who are actively defending the liberty that this country was founded upon - liberty that has since become corrupted by power-hungry feds.

Of course that's not the real reason I picked out your mag among the hundreds of glossy "commercialized" computer selections. It's nice to finally have a publication that isn't totally controlled by industry and political correctness.

What a thrill it was to open it up and find actual "paper" white pages filled with nothing but clear-cut information. I also appreciate your boldness concerning "controversial" issues such as phreaking and other so-called illegal activities. These laws against us "criminals" are nothing but the feds' way of protecting industry giants' profit margins - it is a travesty of free communication and liberty that there must be a group of people who are forced to break laws and be a secretive society all in the pursuit of knowledge.

The Cyber Hitchhiker

Words of Shame

We recently received this letter from a justifiably upset reader:

Dear *2600*:

The most recent Issue of *2600* contains an article entitled "Understanding Verifone Machines" attributed to "Dr. No" on the Verifone credit card authorization machine. (Volume 12, Number 4, Winter 1995-96, pps 22-24) Except for the first and last paragraph, this article is a verbatim duplication of an article I wrote and published, including ASCII diagrams, under my own name to alt.hackers in 1992 entitled "Credit Card Authorization Machines". My article was later published in Issue 03 of the e-zine *Informatik* (available at http://www.eff.org/pub/Publications/E-journals/CuD_and_hacker_zines/Inform/inform-3.gz and at other archives.)

I do not now go by, nor have I ever gone by, nor do I intend to go by the pseudonym "Dr. No". Furthermore, to the best of my knowledge, I have never conversed with anyone calling themselves "Dr. No".

My permission was neither sought nor obtained for the publication of this article in *2600*.

I hereby demand public apologies/retractions/corrections from those parties who perpetrated this fraud. I also request that these apologies appear as prominently as the plagiarized article in the next issue of *2600* magazine.

Emery W. Lapinski (ewl@panix.com)

We contacted the "author" of this article and got the following response:

emmanuel and the entire staff of *2600*:

i must admit that i, Dr. No, pitifully embarrassed myself and the magazine *2600* with this plagirized article. Why you might ask? hmm, that is tough. Who knows what goes on in a young persons head when such an easy thing can be done. I guess i wished i were in the spotlight... Although i did plagirize, i also did do research on this topic. I regret what i have done... i was not trying to take anything away from Emery W. Lapinski, but just try to spread knowledge (in a quite interesting way). So, i must apologize, officially to Emery W. Lapinski, *2600* Magizine, and the entire hacker/information seeker community for this fraudulent act, all i can say is that i was nieve and disrespectful... and i have no excuse. That is that.

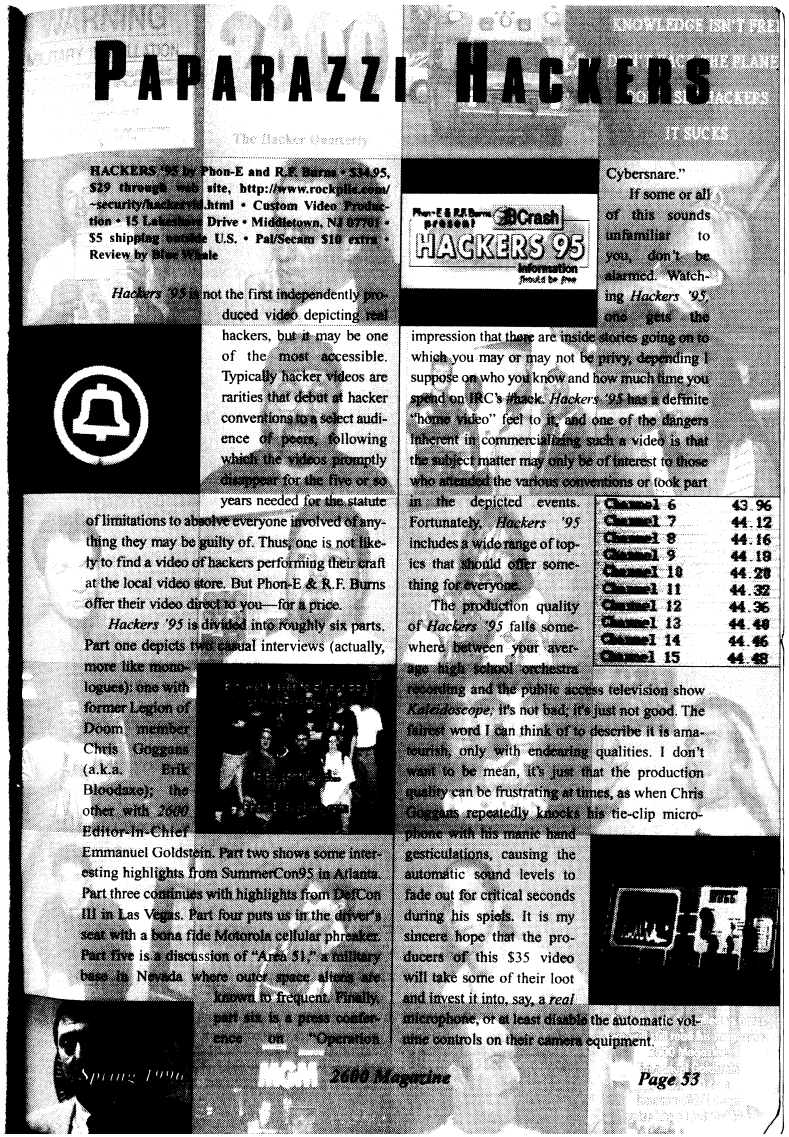
Regretfully,
Dr. No

It's hard for us to imagine how someone could send in an article written by another person and claim it as theirs. With tens of thousands of readers around the world, the odds of getting away with it are pretty slim. In our 12 years of publishing, this is the first case of this that has come to our attention. Since it's not possible for us to know if an article has been lifted from somebody or someplace outside of the hacker world, we rely on the honesty of our writers and the vigilance of our readers. We're sorry this had to happen and we will do everything in our power to keep this kind of thing out of our pages.

Immortalize Yourself

Send your letters to:

2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099



2600 MEETINGS

NORTH AMERICA

Anchorage, AK
Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI
Galleria on South University.

Atlanta
Lennox Food Court near the payphones by Cinnabon.

Baltimore
Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA
In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN
Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID
Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston
Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo
Eastern Hills Mall (Clarence) by lockers near food court.

Charlotte, NC
South Park Mall in the food court near the payphones.

Chicago
3rd Coast Cafe, 1260 North Dearborn.

Cincinnati
Kenwood Town Center, food court.

Cleveland
Coventry Arabica, Cleveland Heights, back room smoking section.

Columbia, SC
Richland Fashion Mall, 2nd level, food court, by the payphones in the smoking section. 6 pm.

Columbus, OH
City Center, lower level near the payphones.

Dallas
Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Houston
Food court under the stairs in Galleria 2, next to McDonalds.

Iowa City, IA
Fourth floor of Pappajohn Business Administration Building by the payphones near the Eleanor Birch conference room.

Kansas City
Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles
Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Louisville, KY
The Mall, St. Matthew's food court.

Madison, WI
Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Meriden, CT
Meriden Square Mall, Food Court. 6 pm.

Nashville
Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans
Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City
Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Orlando, FL
Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Ottawa, ONT (Canada)
Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia
30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh
Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR
Lloyd Center Mall, second level at the food court.

Raleigh, NC
Crabtree Valley Mall, food court.

Rochester, NY
Marketplace Mall food court.

St. Louis
Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento
Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Francisco
4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle
Washington State Convention Center, first floor.

Toronto, ONT (Canada)
Sheppard Centre, Food Court area (around Second Cup). 7 pm.

Vancouver, BC (Canada)
Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 7 pm.

Washington DC
Pentagon City Mall in the food court.

*****

AUSTRALIA, EUROPE, SOUTH AMERICA

Aberdeen, Scotland
Outside Marks & Spencers, next to the Grampian Transport kiosk.

Belo Horizonte, Brazil
Pelego's Bar at Assufeng, near the payphone. 6 pm.

Buenos Aires, Argentina
In the bar at San Jose 05.

Bristol, England
By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

London, England
Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Manchester, England
The Flea and Firkin, Oxford Road.

Melbourne, Australia
Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Munich, Germany
Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

Granada, Spain
At Pilar Del Toro Pub in Plaza Nueva near the Darro Bridget (Puente del Darro).

Halmstad, Sweden
At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

WE GIVE UP

OK. ENOUGH. WE'VE BROUGHT BACK THE BLUE BOX SHIRTS SO YOU CAN STOP COMPLAINING AND BITCHING. SO NOW THERE ARE TWO VERSIONS OF 2600 SHIRTS: THE BLUE BOX SCHEMATIC SHIRTS AND THE MICHELANGELO VIRUS SHIRTS. SAME OLD PRICE. $15 EACH, 2 FOR $26, AVAILABLE IN LARGE AND XTRA-LARGE. WHITE LETTERING ON BLACK BACKGROUND.

I'M A TRADITIONALIST. SEND ME AN OLD-FASHIONED BLUE BOX SHIRT. MY SIZE IS: ____

I WANT TO TRY SOMETHING NEW. SEND ME AN ELITE MICHELANGELO VIRUS SHIRT. MY SIZE IS: ____

❑ 1 shirt/$15 ❑ 2 shirts/$26

AND WHILE I HAVE YOUR ATTENTION, SEND ME:

INDIVIDUAL SUBSCRIPTION
❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE SUBSCRIPTION
❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION
❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION
❑ $260 (you will get *2600* for as long as you can stand it)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)
❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25
❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25 ❑ 1991/$25
❑ 1992/$25 ❑ 1993/$25 ❑ 1994/$25 ❑ 1995/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953
(Make sure you enclose your address!)

TOTAL AMOUNT ENCLOSED: ____