

2600



October, 1984

2600 is published by 2600 Enterprises, Inc., an elementary organization. Subscription rates: \$10 / 1 year, \$3 – 6 months, \$1 per back issue. Overseas: \$13.50 / 1 year. Write to 2600, Box 782, Middle Island, NY 11953-0782, MCI Mail 261UNDREDS; TEL: 630/1994928; ATT: 5167512869

VOLUME ONE, NUMBER TEN

getting caught: hacker's view

Deep down, every hacker wants to get caught. Computer hacking isn't really the same as killing or stealing, after all. You need at least a *little* brains to be able to hop around on the corporations' DECsystems or to know the ARPANet better than your own PC. So if and when you get caught, you wind up getting a little bit of credit for having some brains. Most people exaggerate and call you a genius! Who can resist *this* type of an ego boost?

So when the FBI came knocking at my door early this spring, it seemed like the beginning of an adventure. It was *me* they were after! I had done something to deserve national attention!!

At first I didn't know what it was they wanted. They came to my house before I was awake and showed my mother the search warrant. I'll never forget the tone in her voice when she called me that day. "You'd better come down here right away," she said, sounding very worried and pissed off at the same time. I knew something was up when I heard that.

So then I came downstairs and saw what was happening. I was very calm throughout the whole thing—I even kept my sense of humor. After I figured out which of my many "projects" they were interested in, I showed them where all the good stuff was hidden. "Go tell the world," I said.

I had been hacking for about a year. I seemed to pick up things incredibly fast and before I knew it, I was buried inside the weird world of phones and computers. In this case, I had been running a huge corporation's mainframe for them for a few months. This computer had so much data in it that I could find out (and change) just about anything—paychecks, profit margins, telephone numbers, you name it: I had lots of fun.

My friends used to come over late at night and watch me explore. Nobody they knew had ever been able to do anything like that and it seemed pretty amazing. Then *War Games* came out and I turned into a sort of cult figure in my neighborhood. But it was OK—nobody knew *exactly* what I was doing.

Even my parents didn't seem to mind that much. They'd shake their heads and wonder what kind of mischief I'd get into next. Most people (grown-ups, that is) seemed to act exactly the same. And my friends were all into it as something fun and rebellious.

So now that I was caught, I expected the fun to continue. My parents would be outraged that a mischievous kid was being hounded by the feds while murderers and presidents were roaming free. And of course, my friends would stick by me more than ever. We were pretty tight.

For about a day, that's exactly what happened. My name got in all the papers, I was on a few news shows, and nobody really understood anything. I suddenly became popular at school. Everybody seemed to agree that it wasn't fair for them to come to my house and take away my two computers just like that.

Then, after the initial shock, people's moods started to change. My parents were the first. They suddenly got mad at me. "What a stupid thing to do!" I remember those words. "If

you don't care about yourself, at least think about what you're doing to your family," and so on. They also said that I never listened when they told me to knock it off, which was totally false, since they never really seemed to care at all.

But all that didn't upset me. After all, parents are supposed to say those kinds of things. I knew they really cared, so it didn't matter what they said.

It wasn't until a few more weeks that the really bad stuff started happening. The feds began calling my friends and tried to scare them into saying incriminating things about me. They told them they'd be in just as much trouble if they didn't say anything. I could tell something was wrong when all of a sudden no one was talking to me. People I used to hang out with suddenly seemed uneasy when I was around.

Then the feds started calling *me*. And I could tell from the pointed questions they were asking, that someone I trusted had told them a lot. Much more than they had to. It wasn't like they had just cracked and said, yes, he did this and that. They *volunteered* information!

I tried to figure out why someone would do this—no one knew had any grudges against me. I didn't really have any enemies. They must have thought that telling everything was for my own good. The feds had probably told them that I was really sick and needed help and that only the truth would set me free. Could that have been it?

It might have been. But there was definitely more than that. When the feds started scaring my friends, that was my fault. At least it seemed that way to my friends. A couple of them got so scared that their families hired these big, expensive lawyers. And that was my fault, too, even though I knew they were being ripped off.

So what did I get out of the whole thing? Well, nobody trusts me anymore—people are even afraid to let me use their phone. I've gotten a reputation as someone who doesn't care at all about his friends, otherwise how could I have put them in such a spot? Everyone in town knows that I did something bad to some corporation somewhere, but nobody understands how much of a game the whole thing seemed at the time. The newspapers were never really interested in my side and nobody else seems to be either.

Maybe this is good in a way, because I found out that most people value friendship less than their own safety. As soon as the pressure is applied, they lose all feeling for you. Then they trick themselves into believing that you were always a bad seed from the start. They do this so they won't feel guilty about the way they shafted you. But there were a couple of others who didn't desert me because they knew who I really was. If it wasn't for them, I might have just jumped off a building one night. That's how bad it makes you feel sometimes.

Yes, I'm through hacking. Let the professionals do it—they can't get hurt like I was.

Name withheld by request.

VITAL INGREDIENTS

SWITCHING CENTERS AND OPERATORS

Every switching office in North America (the NPA system) is assigned an office name and class. There are five classes of offices numbered 1 through 5. Your CO is most likely a class 5 or end office. All Long-Distance (Toll) calls are switched by a toll office which can be a class 4, 3, 2, or 1 office. There is also a 4X office called an intermediate point. The 4X office is a digital one that can have an unattended exchange attached to it (known as a Remote Switching Unit—RSU).

The following chart will list the office number, name, and how many of those offices existed in North America in 1981.

Class	Name	Abb.	# Existing
1	Regional Center	RC	12
2	Sectional Center	SC	67
3	Primary Center	PC	230
4	Toll Center	TC	1,300
4X	Toll Point	TP	
4X	Intermediate Point	IP	
5	End Office	EO	19,000
R	RSU	RSU	

When connecting a call from one party to another, the switching equipment usually tries to find the shortest route between the Class 5 end office of the caller and the Class 5 end office of the called party. If no inter-office trunks exist between the two parties, it will then move up to the next highest office for servicing (Class 4). If the Class 4 office cannot handle the call by sending it to another Class 4 or 5 office, it will be sent to the next office in the hierarchy (3). The switching equipment first uses the high-usage interoffice trunk groups. If they are busy it goes to the final trunk groups on the next highest level. If the call cannot be connected then, you will probably get a reorder [120 IPM (Interruptions Per Minute) signal—also known as a fast busy]. At this time, the guys at Network Operations are probably going berserk trying to avoid the dreaded Network Dreadlock (as seen on TV!).

It is also interesting to note that 9 connections in tandem is called ring-around-the-rosy and it has never occurred in telephone history. This would cause an endless loop connection (an interesting way to really screw up the Network).

The 10 regional centers in the United States and the 2 in Canada are all interconnected. They form the foundation of the entire telephone network. Since there are only 12 of them, they are listed below:

Class 1 Regional Office Location	NPA
Dallas 4 ESS	214
Wayne, PA	215
Denver 4T	303
Regina No. 2 SP1-4W [Canada]	306
St. Louis 4T	314
Rockdale, GA	404
Pittsburgh 4E	412
Montreal No. 1 4AETS [Canada]	504
Norwich, NY	607
San Bernardino, CA	714
Norway, IL	815
White Plains 4T, NY	914

In the Network, there are three major types of switching equipment. They are known as: Step, Crossbar, and ESS. Check past and future issues of 2600 for complete details on how these systems work.

Operators

Another vital ingredient of the Network is the telephone operator. There are many different kinds. What follows is a discussion of some of the more common ones.

• **TSPS Operator.** The TSPS [Traffic Service Position System (as opposed to This Shitty Phone Service)] Operator is probably the bitch (or bastard for the phemale liberationists) that most of us are used to having to deal with.

Here are her responsibilities:

- 1) Obtaining billing information for Calling Card or 3rd number calls.
 - 2) Identifying called customer on person-to-person calls.
 - 3) Obtaining acceptance of charges on collect calls.
 - 4) Identifying calling numbers. This only happens when the calling number is not automatically recorded by CAMA (Centralized Automatic Message Accounting) and forwarded from the local office. This could be caused by equipment failures (ANIF Automatic Number Identification Failure) or if the office is not equipped for CAMA (ONI—Operator Number Identification).
- (I once had an equipment failure happen to me and the TSPS

operator came on and said, "What number are you calling from?" Out of curiosity, I gave her the number to my CO, she thanked me, and then I was connected to a conversation that appeared to be between a frameman and his wife. Then it started ringing the party I originally wanted to call and everyone phreaked out (excuse the pun). I immediately dropped this dual line conference!

You shouldn't mess with the TSPS operator since she knows where you are calling from. Your number will show up on a 10-digit LED read-out (ANI board). She also knows whether or not you are at a fortress tone and she can trace calls quite readily. Out of all of the operators, she is one of the most dangerous!

• **INWARD Operator.** This operator assists your local TSPS ("0") operator in connecting calls. She will never question a call as long as the call is within her service area. She can only be reached via other operators or by a Blue Box. From a BB, you would dial KP+NPA+121+ST for the INWARD operator that will help you connect any calls within that NPA only.

• **DIRECTORY ASSISTANCE Operator.** This is the operator that you are connected to when you dial 411 or NPA-555-1212. She does not readily know where you are calling from. She does not have access to unlisted numbers, but she does know if an unlisted number exists for a certain listing.

There is also a directory assistance for deaf people who use Teletypewriters (TTY's). If your modem can transfer BAUDOT (45.5 baud—the Apple Cat can), then you can call him/her up and have an interesting conversation. The number is 800-855-1155. They use the standard Telex abbreviations such as CIA for Go Ahead. They tend to be nicer and will talk longer than your regular operators. Also, they are more likely to be persuaded to give more information through the process of "social engineering".

Unfortunately, they don't have access to much. I once bullshitted with one of these operators and I found out that there are two such DA offices that handle TTY. One is in Philadelphia and the other is in California. They have approximately seven operators each. Most of the TTY operators seem to think their job is boring. They also feel they are underpaid: They actually call up a regular DA # to process your request—no fancy computers here! (Other operators have access to their own DA by dialing KP+NPA+131+ST (MF).

The TTY directory assistance, by the way, is still a free call, unlike normal DA. One might be able to avoid being charged for DA calls by using a computer and modem at 45.5 baud.

• **CN/A Operator.** CN/A operators do exactly the opposite of what directory assistance operators are for. You give them the number, they give you the name and address (Customer Name Address). In my experiences, these operators know more than the DA operators do and they are more susceptible to "social engineering." It is possible to bullshit a CN/A operator for the NON-PUB DA # (i.e., you give them the name and they give you the unlisted number). This is due to the fact that they assume you are a fellow company employee. The divestiture, though, has resulted in the break-up of a few NON-PUB #'s and policy changes in CN/A.

• **INTERCEPT Operator.** The intercept operator is the one that you are connected to when there are not enough recordings available or the area is not set up to tell you that the number has been disconnected or changed. They usually say, "What number did you dial?" This is considered to be the lowest operator lifeform since they have no power whatsoever and usually know very little.

• **OTHER Operators.** And then there are the: Mobile, Ship-to-Shore, Conference, Marine, Verify, "Leave Word and Call Back," Route and Rate (KP+800+141+1212+ST—new number as a result of the break-up), and other special operators who have one purpose or another in the Network.

Problems with an Operator? Ask to speak to their supervisor...or better yet, the Group Chief (who is the highest ranking official in any office), the equivalent of the Madame in a whorehouse (if you will excuse the analogy).

Some CO's, by the way, have bugs in them that allow you to use a 1 or a 0 as the 4th digit when dialing. (This tends to happen mostly in crossbars and it doesn't work consistently.) This enables a caller to call special operators and other internal telco numbers without having to use a blue box. For example, 415-121-1111 would get you a San Francisco-Oakland INWARD Operator.

(The above was taken from Basic Telecommunications Part IV, written by BIOC Agent 003.)



FLASH

NSA Wants Better Phones

The New York Times

The National Security Agency is proposing that the Government and industry be equipped with as many as 500,000 telephones that can be secured against interception.

The agency is convinced that the Soviet Union and the other nations are obtaining important intelligence from United States telephones.

Although cloaked in secrecy, a program like the one the agency proposes could cost hundreds of millions of dollars. Under the proposal, production of the secure phones would begin in two years.

The number of secure telephones currently used by Government agencies is classified information. But the Carter Administration said there were 100 such phones in the Government and it planned to buy 150 more. The cost of each phone then was \$35,000. The Reagan Administration has bought an unknown number of additional secure phones.

"Anyone making a phone call to the West Coast or Boston from the Washington area has no idea how the conversation will be transmitted," an NSA spokesperson said. "It might go via fiber optics, conventional cable, microwave towers or one of the 19 domestic satellites. If it is going via satellite you can presume the other guy is listening to it."

Oh No, Not Again!

Associated Press

The House passed a bill on September 17 by voice vote that would make it a Federal crime to gain unauthorized access to or tamper with computerized medical records.

Victimized by Crime Computers

The New York Times

Police officers went to an apartment in New Orleans looking for a woman named Vera Davis, who was wanted for theft and forgery. Although the woman who answered the door identified herself as Shirley Jones, they arrested her anyway. A police computer listed Shirley Jones as an alias used by the forgery suspect. That was two and a half years ago.

According to her attorney, Mrs. Jones, who was once advised by a sheriff's deputy to change her name to avoid future arrests, is one of a growing number of people in New Orleans who have gotten in trouble with the law because of inaccurate, outdated, or misused information in police computers.

The New Orleans computers are part of a national network. From a local terminal, a computer check can be run through the National Crime Information Center in Washington, operated by the FBI, in less than a minute.

The New Orleans case, said Robert Ellis Smith, publisher of *Privacy Journal*, a newsletter that reports on privacy cases from Washington, DC, is "symbolic of a larger national problem, an incredibly high rate of inaccuracy" in criminal records and "an inordinate amount of mistaken identity cases in the criminal justice information systems."

Sears Satellite Network

Associated Press

The American Satellite Company has signed a contract with Sears, Roebuck and Company to construct and operate a

private communications system linking corporate offices of Sears and its subsidiaries in 26 United States cities. This would be the largest private system ever developed capable of offering full-motion video teleconferencing.

Loopholes Around Wiretap Laws

The New York Times (again)

Senator Patrick J. Leahy, Democrat of Vermont, has said that he will seek legislation to improve protection of privacy by closing gaps in Federal wiretapping laws.

He and several experts said at a Senate Judiciary subcommittee hearing that it was unclear, for example, whether existing laws permitted Government officials or others to intercept electronic mail, or even ordinary telephone calls sent by computer or microwave technology, without a warrant.

"There are tremendous holes in communications privacy today," testified Ronald L. Plesser, a Washington lawyer who has long specialized in information privacy issues.

The experts at this hearing testified that private interception of electronic mail and other messages carried through telephone networks may not violate Federal law.

IBM is Buying Rolm!

The New York Times (yet again)

IBM has said that it will buy the Rolm Corporation, in a move that will heighten the competition between the world's largest computer company and AT&T. The price? \$1.25 billion.

"IBM wants it all, it needs it all," said Esther Dyson, editor of Release 1.0, an industry newsletter. "They have a biological urge to grow."

Most analysts, however, said that IBM had realized—perhaps belatedly—that it greatly needs to strengthen its offerings in telecommunications switching equipment.

Rolm, founded in 1969 as a maker of military computers is now a leading maker of private branch exchanges, systems that control both voice and data communications over the telephone.

911 Suspect Hung Up

The New York Post

A notorious hoax caller who has plagued 911 switchboards for three years has been nabbed reporting another bogus crime, police say.

Cops say the suspect—who they have been unable to identify—made more than 500 false reports ranging from strangulations in progress to rapes and shootings of police officers.

He was arrested at a Penn Station pay phone while telling a 911 operator he had just raped and strangled his girlfriend with her pantyhose. That was the fabricated crime he reported most frequently, according to police.

"He called every day of the week at all hours," said Sgt. Stephen McDonald.

"He was causing a lot of problems and the 911 people were really looking for him," said Officer James Lapidra who collared the hoaxter.

According to McDonald, news of the hoaxter's capture was jubilantly received by 911 operators: "There was a lot of cheering."

In the words of Lapidra, "He was surprised he was caught."

LETTERS FROM THE OUTSIDE WORLD

Dear 2600:

I am currently involved with the Crystal Palace BBS, formerly OSUNY (hopefully you have heard of it). The system is down now for some software modifications, and many people have tried to persuade me into changing the purpose of the board, which is telecommunications and other related fields. The crackdown on this type of BBS is starting to become overwhelming. This is what my inquiry is about. After reading my first copy of your newsletter, I was elated with the quality and content of information it had! Referring to the front page article (July 1984, page 1-37), "Look Out, He's Got a Computer!" I agree that the anti-computer hysteria has gone and is going to go too far! I am interested to know what exactly is an illegal BBS message and what is not. Do I have to monitor the system 24 hours a day, 7 days a week? Am I responsible for every message posted on the board? I know that these are questions that everyone wants answers to and can't find. As I see it the BBS is just another form of newsletter, so why are they picking on us? I do, however, realize that some messages are quite illegal like: credit card #'s and the like, but the information on how to get those #'s is not illegal (right?). Any information on this subject would be greatly appreciated.

Crystal Palace

Dear CP:

What is a BBS? You know the answer, we do, and a good many of our readers also do. The problem is that the people who go around passing laws and raiding homes don't have the slightest idea what a BBS really is. All they care about is the fact that a computer is involved somewhere along the line. And computers, they say, can do anything in the world. But what's so ironic in the case of a BBS is the fact that the computer is just storing messages!! The exact same effect could be accomplished on a physical bulletin board, inside an auditorium, or in everyday conversation. But you don't see these things being outlawed because people would never stand for that kind of repression (we hope). Computers are easy targets because the average person doesn't understand them at all. By making people think that it's actually illegal to write something down and pass it along to others, the authorities are taking one great big step towards total control.

We agree that a BBS is really another form of newsletter. We don't agree that messages containing credit card #'s are illegal in any sense. (They are boring, though, and practically useless to anyone except fraud investigators.) It's the actual use of these numbers that constitutes fraud, not the simple act of passing them around. If a cop on the street overheard you giving numbers to a friend, could he arrest you? Let's hope it hasn't reached this stage.

We're currently working on getting some more legal information concerning this subject so that we can address your questions better. In the meantime, though, we hope your board and the many others like it around the world won't be intimidated by these scare tactics. You can talk about whatever the hell you want. But it's still illegal to commit the crimes you're talking about.

If enough of you guys stood up for your rights out in the open, this wouldn't be such a problem. You might actually wind up saving an important part of democracy for a few more years.

By the way, readers, if you're running a BBS that talks about these things or know of one that does, send in the name and phone number for our Hot 100 list which will be published soon. Make sure the BBS you're sending wants to be publicized and try to include a reason or two why your BBS is better than most. Check the front page for our addresses.

Dear 2600:

Received your August issue, and enjoyed it. A number of comments...

- 1) Does anyone know what happened to TAP?
- 2) There is a newsletter called the *Comsec Letter*, available for free from Ross Engineering Assoc., 7906 Hope Valley Court, Adamstown, MD 21710. Lots of good information, but they want a letter requesting the newsletter on letterhead and identifying your interest in communications security (one can't be too careful these days!). It's always interesting to know

what's happening on the other side...

3) What works against an ESS switch? Black boxes are ok, but more modern equipment seems to be coming in rapidly, blowing our older techniques off the air!

The Animal

Dear Animal:

For info on TAP, consult our September issue, page 1-52. We hate repeating ourselves all the time.

Thanks for the sample copy of *Comsec Letter*. It looks interesting and we're looking into reprinting some of the good stuff. Readers: feel free to send us anything that looks like it might be interesting to us. It usually is.

ESS switches and black boxes are dealt with extensively on page 1-43 of our August issue, as you probably know. The only thing we can suggest to counter an ESS is ingenuity. There's always a way to get around anything.

Dear 2600:

I really enjoy your publication! It seems you guys are not a bunch of wimps who are so damn paranoid that the feds are going to catch you. Anyway, what types of back issues do you have? I received my first issue, which is Volume 1, Number 9. What are the context of the back issues? I'm looking for one having to do with loops, sprinting, hacking out sprint/mci's, or anything similar. Also, any arpanet/archnet stuff?

kd

Dear kd:

We'll be publishing a guide to our back issues that should be out right in time for the Christmas rush. Just about all of the topics you mentioned have already been covered and they all will be covered in the future. We accept articles and information from anyone.

You're quite correct in saying that we're not paranoid. We have nothing to be paranoid about because we're not doing anything wrong.

Dear 2600:

Though it may seem like only yesterday that computer crime first caught the nation's fancy, it has been on the mind of state legislators for quite some time. With the recent passage of computer crime laws in Maryland, Iowa, Connecticut, and Hawaii, the number of states locking computer crime laws has fallen to seventeen. The laws of the other 33 have been collected in a new reference work published by the National Center for Computer Crime Data, and called *The Computer Crime Law Reporter*. In the course of compiling the texts of all the state computer crime laws on the books, editor Jay Bloom/Becker found that a number of states had bills on the books for years without anyone noticing them.

The book, 200 pages plus two updates, is available for \$45 from the National Center for Computer Crime Data, 4053 J.F.K. Library, California State University at Los Angeles, 5151 State University Drive, Los Angeles, CA 90032.

In addition, the National Center will begin publishing a newsletter devoted to morals and ethics in computing. Its name is *Conscience in Computing*.

There are schools teaching computer ethics, no matter how many are not. There are professionals questioning their roles as computer scientists and asking about the social impact of their work. There are computer bulletin boards which support ethics discussion groups.

Conscience in Computing will be a monthly newsletter, subscriptions costing \$18 annually. Work exchanges allow readers to become subscribers by convincing others to subscribe, reporting news of conscience in computing, or working out an individual contract with the National Center. Interested people can write to the above address.

The National Center for Computer Crime Data (*The National Center for Computer Crime Data is a nonprofit research organization at California State University at Los Angeles.*)

Whoopsee

In our last issue, we forgot to mention that in our August issue, we forgot to mention that the front page story ("But How Does It Work?") came from the desk of BIOC Agent 003. Better late than never.



CONTACTING THE GESTAPO!

ON...GARB LANGUAGE

(These are editorial comments.)

At the MCI convention, Corp. stockholders meeting in July a woman asked chairman William C. McClellan about a letter he published in the New York Times. He explained that the ad brought in a lot of business and brought in a lot of money. He said that the ad "really paid off." The ad "really paid off" because it brought in a lot of business and brought in a lot of money.

While some in the business world are "really paid off" by the ad, others are not. Some are "really paid off" by the ad, but others are not. Some are "really paid off" by the ad, but others are not.

According to the Oxford English Dictionary, "paid" is to give or to pay. The dictionary suggests that in some cases in the future, the word might mean to pay someone. The dictionary suggests that in some cases in the future, the word might mean to pay someone.

Now, if you are a "paid" person, you are a "paid" person. Now, if you are a "paid" person, you are a "paid" person.

President Lyndon Johnson once told me that the word "paid" is to give or to pay. The president said he was not to give it out too much.

— J. J. Wells

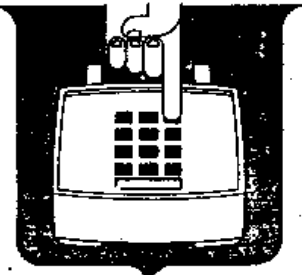
New York Telephone

Felix Houser was that he was "paid" in the month of June, but it is not clear how he could be on the outside paying in.

"Paid off" can be coming into several general uses. It is one very widely used by the armed forces during World War II. The term "paid" has been around since the time of the Old Testament and in Shakespeare's "When did you see that light?"

McClain says he was not "paid" in the month of June, but it is not clear how he could be on the outside paying in.

— J. J. Wells



Security as close as your fingertips

- CORPORATE SECURITY
 - Director Corporate Security
 - J. E. Miller 212-395-0505
- SECURITY STAFF
 - Security Supervisor
 - W. F. McGarley 212-395-0528
 - Security Manager
 - R. F. Johnson 212-395-0552

- NEW YORK CITY REGION
 - Security Manager
 - W. R. Green 212-395-4158
- New York City West
 - Security Office 212-395-0515
 - Security Supervisor
 - J. R. Parr 212-395-0516

- New York City East
 - Security Office 212-291-9617
 - Security Supervisor
 - C. J. Hauswirth 212-523-9953

- STATE REGION
 - Suburban
 - Security Manager
 - J. J. Ferran 914-689-9949
 - Mid-State
 - Security Office 914-699-9985
 - Security Supervisor
 - M. R. Zapf 914-699-9985

- Long Island
 - Security Office 516-294-0210
 - Security Supervisor
 - R. H. Lamberson 516-294-0722

- UPSTATE
 - Security Office 518-449-3250
 - Security Supervisor
 - T. A. Paolucci 518-449-5442
 - Security Manager
 - T. J. Doran 518-449-7224

I-59

C. M. Gorman

- TOLL FRAUD
 - Toll Fraud Office 212-221-1764
 - Security Supervisor
 - H. F. Gallagher 212-221-5644
 - Security Manager
 - J. S. Whitman 212-395-0507

On weekends, holidays and out of hours, call the following telephone numbers to obtain assistance.

- Customer Service Bureau
 - New York City Region 212-395-2571
 - Mid-State 914-390-5600
 - Long Island 516-742-3030
 - Security Office
 - Upstate 518-449-3250

- BUILDING PROTECTION ORGANIZATION
 - Guard Coordinators
 - New York City Region
 - W. J. Blumet 212-394-3400*
 - State Region
 - H. K. Askidson 914-684-8253*

*NOTE: These telephone numbers should be called concerning matters of building protection.

The MCI convention was held at the New York Hilton Hotel in New York City. The convention was held from July 15 to July 17, 1973. The convention was held from July 15 to July 17, 1973.

The MCI convention was held at the New York Hilton Hotel in New York City. The convention was held from July 15 to July 17, 1973. The convention was held from July 15 to July 17, 1973.

The MCI convention was held at the New York Hilton Hotel in New York City. The convention was held from July 15 to July 17, 1973. The convention was held from July 15 to July 17, 1973.

•Humm-mm-mm. That's the
 tone—your "go ahead"
 tone to start dialing. Please
 wait for it.

Answer Promptly


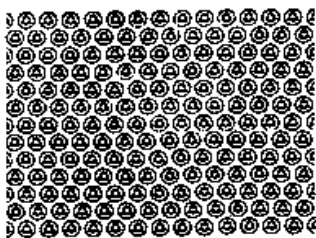


Don't make a friend wait or miss a call by not answering your telephone at once.

Area codes are used to call from one telephone area to another, but not within the same telephone area.

Dial-a-Discount. Dial-it-Yourself.

WHEN ANSWERING THE TELEPHONE. always identify yourself, your firm, or your department.

when to get personal...



Station-to-station rates are always cheaper, so you should use person-to-person only when you want to talk to a particular party.

after you finish your call.....



be sure to replace the receiver

Try One-Plus Dialing.

•Telephone cords and water don't mix. A wet cord can put your telephone out of order. So please keep your telephone cord away from sinks, valves, steam and other places where water might get on it.

DIAL CAREFULLY!
 Avoid wrong numbers by first checking the number and then
DIAL EACH DIGIT CAREFULLY!

The wheel that lets you roll around town without leaving home.



Just spin the dial and you're talking to the pharmacist. Spin it again and reach your insurance man. Or chat with a friend across town. Count on it any time — to save you time and traveling. Saves money, too. What else does so much yet costs so little?

when you're away from your office — who'll answer your phone?



See "Telephone Answering Service" pages in this directory.

IF YOU'RE NEW IN TOWN...




shop the Yellow Pages

•Party-liners—don't forget the other fellow needs the telephone too.

•For better service, don't transfer a call to someone else if you can take care of it yourself.

NOT SURE OF THE NUMBER?

You'll save time and trouble if you look in the directory



Save time... telephone.

When you're on the go... you're as close to home or office as the nearest public telephone booth... try it and see.