TAP
Room 603
147 W. 42 St.
New York 10036

11th ANNIVERSARY ISSUE No. 75

MAY – JUNE 1982

WATS EXTENDERS

By: The Magician

Many people think of phone phreaks as slime, out to rip off Bell for all she is worth. Nothing could be further from the truth ! Granted, there are some who get their kicks just by making free calls, however they are not true phone phreaks. Real phone phreaks are "telecommunications hobbyists" who experiment, play with and learn from the phone system. Occasionally this experimenting, and a need to communicate with other phreaks (without going broke), leads to free calls. The free calls are but a small subset of a TRUE phone phreaks activities.

Until several years ago, The phreaks main tool for free calls was the Blue Box. In recent years however, Bell has made GREAT strides in their security and detection of Blue Box's. While Box's still work, their use is becoming EXTREMELY dangerous. With the advent of CCIS, the places where a Blue Box will work are rapidly decreasing, and within several years the Box will be totally obsolete.

Thus for their communications needs, phreaks have turned to other methods, one being: WATS EXTENDERS.

Many companies throughout the United States have salesman in the field that must contact a large amount of customers long distance by phone. To pay for these calls, generally the salesman use the companies Bell credit card (Now called a "Calling Card") this is quite expensive to the company.

Several years ago, someone came up with a neat money saving idea. Since the company already has an INWATS (800) number for salesman to call in orders to the main plant, and since the compnay had a flat rate OUTWATS line to call customers during the day. Why not couple them together after hou s so that the salesman calls the companies INWATS 800 number, then gets connected up to OUTWATS. This would mean he could call anywhere in the United States, from anywhere at no charge to him! This arrangement would save the company tremendous amounts of long distance charges since they had the WATS lines anyway, and the WATS was a lot more cost efficient than Credit Cards.

This arrangement was exactly how early "WATS EXTENDERS" worked.

During WATS (800) scanning (For how to do this, read "Napolean Solo's" EXCELLENT article in issue 55) phreaks discovered these WATS EXTENDERS, and found they could call anywhere in the country just by calling the extenders 800 number, then (Using Touch Tone of course) dial the number the wanted.

The companies soon realized that their extenders were being messed with and decided to add some security to prevent tampering.

It was set up so that when a salesman dialed the WATS EXTENDER, he would here what sounds like a dial tone. The salesman then keyed in a four digit Touch Tone secret access code. If the code was incorrect a high-low tone would result, and the extender would have to be re-dialed. If the code was correct, a second internal PBX dial tone would result. The salesman would then access the companies OUTWATS line by hitting an 8 or 9 (usually) and dial wherever he wanted.

The four digit access code posed a problem to phreaks since only 1 out of 9999 possible codes worked, and the 800 number had to be re-dialed each time to try another.

Many a Phone Phreak spent long nights breaking the four digit codes and then using the extenders themselves! Most companies change the code every few months so the phreaks would have to start over again. (Also company employees that were not authorized to know, but found out from "leaks").

Many of you have probably heard of the infamous computer "Charlie". For those who haven't, several years ago Charlie was brought to life by Capn Crunch (Now retired from the communications service) Charlie was an APPLE II computer with a special board which allowed it to Touch Tone dial numbers extremely rapidly (D/A) then "listen" to the results (A/D).

Charlie was put to use calling a given WATS EXTENDER, trying an access code, if the high-low tone was heard (meaning an incorrect code), Charlie hung up and dialed again, trying the next sequential code. Charlie would sit working for hours, and when it found the code, it would print it on it's display screen. VERY Effective !

Unfortunately the only problem with Charlie was that he was very noticeable to Bell. Every time an 800 number is called, an AMA record is punched at the C.O. thus it looks real phunny to Bell to see that you have called Dry dock orange shippers 800 number in Florida 3,750 times at 2:00 AM with each call lasting 1 second ! Since Charlie was not very easily portable to pay. phones this was a real problem.

There are many WATS EXTENDERS reportedly presently in service. Most working as described, with some taking more then a four digit code, and some even responding to voice input !

It should be pointed out however, that should any of you crack any WATS EXTENDER access codes and attempt to use them, you are guilty of Theft of communications services from the company who owns it, and Bell is very willing and able to help them nail you ! WATS EXTENDERS can get you in every bit as much trouble as a Blue Box should you be caught.

Most WATS EXTENDERS also record all numbers called from them on OUTWATS. If the company detects the extender being mis-used, they will usually first try to change the access code. If the abuse continues and they get mad enough they will contact Bell who will help them investigate all the numbers you called !

Thus, as in most things those of you who are determined to play with WATS EXTENDERS, do so from a pay phone and only to institutional switchboards, or people with short memories. By the way, on some "Money First" payphones (as opposed to "Dial Tone First") the Touch Tone pad is cut off after the WATS call is complete. (Because of polarity reversal) It can be re-activated by depositing a dime after the connection is made, which you will get back after you hang up.

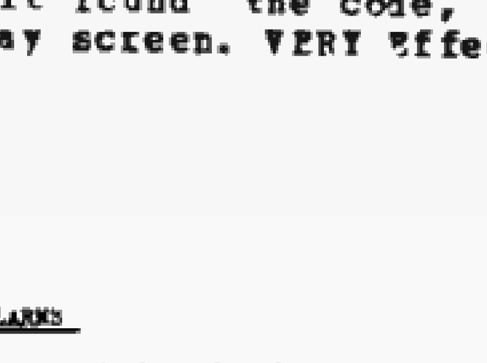
Also please remember the opening of this article. DO NOT use WATS EXTENDERS just to make free calls all the time!, experiment with them and learn what they can do and how they work. I think you will learn a lot !!

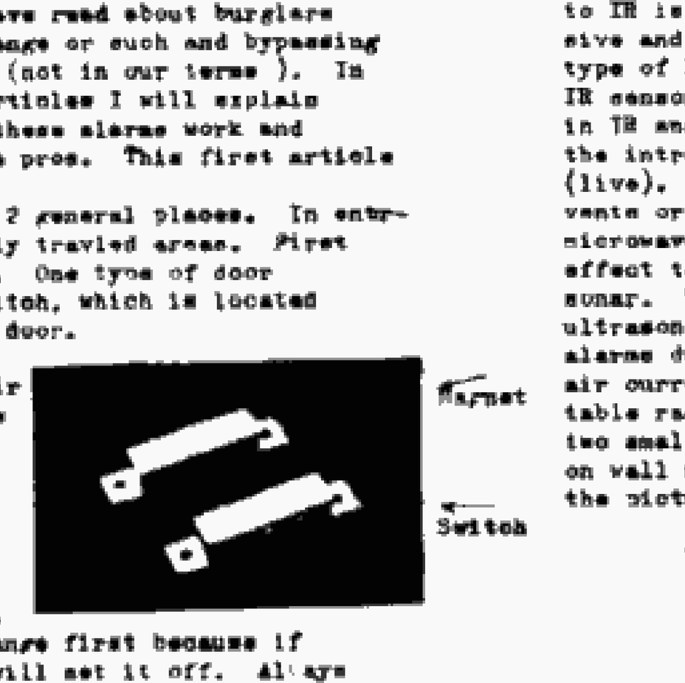
Send any comments etc. to: TAP c/o The Magician

ALARMS

I'm sure many of you have read about burglers ripping off a jewlry exchange or such and bypassing the alarm with a blackbox (not in our terms). In the following series of articles I will explain how (to the last detail) these alarms work and how they are fucked by the pros. This first article is about sensors.

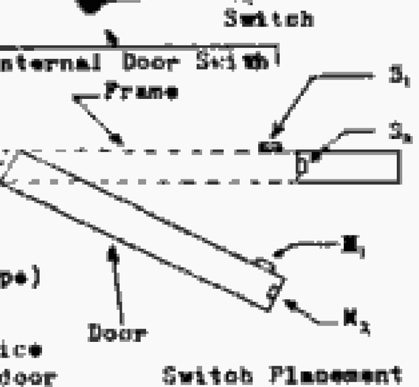
Sensors are located in 2 general places. In entrance ways and in frequently travled areas. First lets take a look at doors. One type of door sensor is the magnetic switch, which is located on the side or top of the door. The illustrations show two basic swithes and their placement. To bypass them you must determine wether it is a closed or open circuit. Take a VOM and test the terminals for a current flow. If you don't get a reading then test for an closed circut. Never test with an ohms range first because if it is on open circut you will set it off. Always use a voltage range first. If it is normally open just cut one wire. If it's normaly closed short the wires. Never attempt to bypass them with a magnet as some of them are magnetically biased and you will set them off. Magnetics are also placed inside door frames and on the inside of garage doors. The best way to check for magnetic swithes is a modified metal detector.





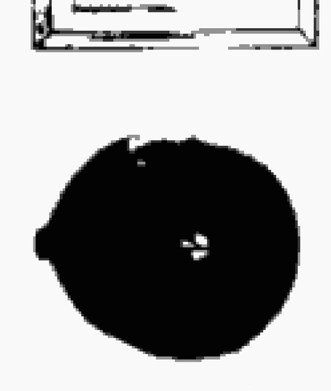
The second type of switch is a push button located in the frame of the door. To bypass them a stiff peice of metal is slid between the frame and door and is used to hold the swith down as the door is opened. By the way, this is also used in lavatories to automatically flush the urinals.

Windows are the next topic. They are usually protected against breakers only. This is done by placing a loop of thin metallic foil on the window. If it's smashed the foil is broken and the alarm is sounded. (To fuck it up take a razor blade and cut a line across it. It is invisible and the alarm sounds as soon as it's turned on.) Just use a glass cutter and cut a section out of the glass. Then reach in and short the contacts. An interesting way to break windows is to cover the glass with tape. Then the window is gently tapped with a hammer until all the glass is broken. Then pull the tape off in a single sheet and the broken glass will remain stuck to it. The latest in window and wall protection is the vibration sensor. There is no fool prufe way to fool them (yet). Vibration sensors are also used on fences to detect climbing. If possible it is always best to simply avoid the sensor than to try to bypass it. Another type of device is the old pressure mat. They are used under carpets or as door mats. Placement is in halls, stairways, under windows and in front of doors. The only way to avoid them is to walk along the edge of a suspected hall and avoid all welcum mats. Light beam detectors use a beam of light that sets an alarm off if the beam is broken. They use IR, UV and visible light. Look for small boxes with windows at about thigh level. They are now mounted in other fixtures such as sockets and books. The best way to locate a visible light beam is to get a can of dry powder deoderant and spray it in the direction you are going. The beam will show up, just like a flashlight in a dusty room. For UV get a "empty" spray can (a can that can be filled with any substance you choose) and fill it with flourescent paint (at any novelty store or Edmund Scientific).



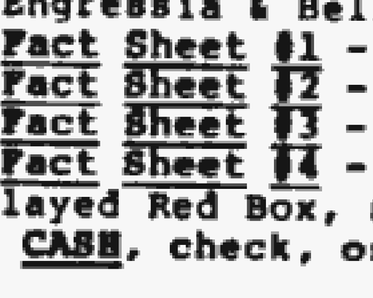
Vibration Sensor

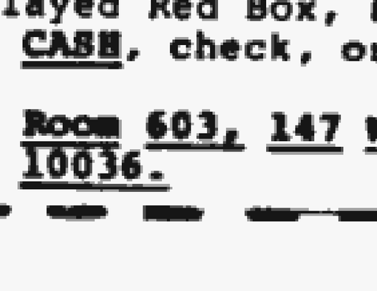
Vibration Detector. . .
Protects Walls & Ceilings



Most places use IR. The only way to IR is a IR scope which is expensive and bulky. There is another type of IR sensor called passive IR sensor. It notices a increase in IR energy in an area ,such as the introduction of a human body (live). They are disguised as wall vents or sockets. Ultrasonic and microwave detectors use the doppler effect to detect motion, just like sonar. The only difference is that ultrasonics are more prone to false alarms due to changes in weather and air currents. They look like small table radios with a large vent or two small holes. They are also put on wall mounting brackets as shown in the picture.

Bispy Passive Infrared Disappears Into Woodword
• Virtually Undetectable as Burglar Alarm





The Stainless Steal Rat

IBM TIME SHARING OPTION (TSO)

– Nick Haflinger

I have seen articles about computer access but I almost never see anything about the GIANT of computing. IBM mainframe computers allow the knowledgeable user to do almost anything he desires. These huge machines are used by most major corporations and nearly all utilities, insurance companies, and newer Social Security offices. Almost every computer has at least 1 dial-in port which can be called by anyone that knows the number. Some even have an Inwats line. CAPITALIZED words are keywords keyed in by the user. that's you. All system responses will be capitalized and enclosed in quotes. A dataset name on IBM systems must be enclosed in single apostophes (') or belong to the user. Get a note pad ready and let's go.

IBM systems have a monitor program called TSO. This is what we will be accessing. After your terminal (110-300 baud) has made its connection type in LOGON or //LOGON. You should be prompted for USERID, PASSWORD, and maybe ACCOUNT NUMBER. If you know all the info just type LOGON USERID/PASSWORD ACCOUNT NO. Some installations allow the use of nonsense like LASTNAME/FIRSTNAME or similar constructs for USERID/PASSWORD. Try calling the company and obtaining the names of some programmers under some pretext. Try these names or use more sophisticated wiretap procedures to obtain actual userid's.

Let's assume that you have gotten logged on. The system will reply with some messages and eventually say "READY". You are in! Here are a few commands that you can use to get your bearings. Copy down the reply to every command you try. If you have no experience with IBM command syntax the HELP command will be useful. You may want to route this output to a printer. Enter HELP HELP to get more information on the help command. Enter HELP by itself to get a list of available commands. Enter HELP COMMANDNAME to get specific info for a command, eg. HELP EDIT will tell you about the edit command.

Now on to the real goodies. When you get logged on the system may have listed some datasets that belong to your userid. We want to use these as a tool for breaking the system. Study the commands below and then we will discuss a general strategy for using the information that they will give us.

LISTCAT – Lists all the datasets owned by your userid. The system will also tell you what catalog the datasets are in.

LISTDS 'dsname' – Get the dsname from the above command and this will tell you the characteristics of the dataset.

LISTALC ST – This is a good one. When you logged on the system allocated several datasets to your terminal. They may contain anything so they are the starting point. Copy down all of this. If you see "SYS1.UADS" in your list you hit the jackpot. SYS1. anything is a system dataset and usually valuable.

STATUS – This will list any jobs that may be executing under your userid. Follow with a "?" for more info.

PROFILE – This will display the characteristics of your userid. These can be changed during your logon session but should be changed back before you logoff. It will be helpful to have the options PROMPT and MSGID. If you don't have them just set them up by entering PROFILE PROMPT, etc.

That's all for this month. Try out these commands and if you can, get a listing of the command syntax via the HELP command. In future issues I will introduce more commands and teach you how to enter programs into the system. Our eventual goal will be to gain access to the password dataset and other goodies.

New Economic Policy

Tired of all that bullshit the government has been giving about how to reduce inflation? Well here is the real way to cut your bills.

I Super-Markets

The next time you visit your local food rippoff center that claims to have the lowest prices in town, you can make sure that they keep their promise. When you catch an employee loafing on the job borrow (permanently) his or her little price tag gun. After several minuets of examination and trial you can stamp your own prices just like the pro. Need I go further? Of course. Just for good relations take all those funny little rolls of stickers that are used to show when there ise special and all the blank rolls for the tag gun. Beware. Make sure that the product you stamp with your gun is the same as the tag is. Some tags are pre labled: Grocery, candy, milk item, etc. Make sure the tag matches the item. Never remark items that are common. Many times the cashiers know the price. Also, with your "special" stikers be careful. Many times they are distributed by the manufacturer of the product. If you are in a hurry just take the price tag off the cheapest bargin brand and put it on the best quality brand. This can be tricky if not impossible because some places have price tags that are pre-cut, so they fall apart if you try this.

II Counter Espionage and Other Tricks

For all you that shoplift (or about to begin) here are some tips.

– stay away from large Malls and Shopping Centers it's like narc city. The narcs like it there because they can bust little kids for shoplifting candy.
– keep your eyes open for mirrors, two way mirrors, cameras and nosey clerks.
– if you are with a partner keep your mouth shut They have hidden mics in those tall columns that seem to hold up the roof.
– Avoid all large silvered objects. In one place I know they put small cameras in large silver Christmas balls (Merry Christmas, huh?)
– Look for people that you always see in the same store and for people who walk around like zombies and pay more attention to the people in the store than the products.
– avoid all people with 2-way radios. They are most definitly not hams with their 2 meter.

If you decide to shoplift (naughty you), remember all you have to do is remove the item from its package and take off all store markings and tags and they cannot prove the item is yours. Use display models if possible, because you can fiddle with them without suspicion. If you think the risk of getting caught is too great or you cannot get it because of its size (I know a guy who shoplifted a 20" crock pot) you can still get it at a greatly reduced price. Many places use felt tip markers or pens to show reductions. When a store has a clearance sale just cum on in and make your own reductions (not too outrageous please). Sometime the cashier will be suspicious and go and chek your items price against one on the shelf. The only way to beat this is to mark all the items down. This way you can also buy several and you do a publik service for their regular customers. My last trick is to use a high quality eraser and erase the first digit of the price. I have done this one several times with chips and other expensive parts. Some of those clerks are as blind as riveted bulkheads. The real price was stamped on the package right next to the erased price tag. I still saved 10 Amirikan (worthless) dollars.

Happy budget cutting !

The Stainless Steal Rat

ATTENTION ---- ATTENTION ---- ATTENTION

The 8BBS dial-up system mentioned in TAP #72 is no longer in operation. Last summer while the SYSOP was away on vacation his place was raided by the FBI, police, Telco security and others. The 8BBS disk packs, user log printouts and a modem that some Philadelphia area users had sent out were seized as evidence and are being used to prosecute some people in the Los Angeles and Philadelphia area.

In issue #71, I talked about the four major alternate nets serving the country. I recieved some letters from readers with info and comments. I'd like to thank Mt. Bill and you others for writing to me. You were all helpful. SP Sprint, MCI, ITT citicall, and Western Union aren't the only nets, there are a lot of others. But they are the four major ones that serve the public. Since they serve the public, they are much easier for the average phreak to get access numbers and codes for. But there are many other nets, as was pointed out to me in a letter. If you have info on another net, send it in!

Also, I was told that I gave the impression that Sprint covered most areas. All the alt. nets are the same, in that they only cover the large metropolitan cities, and sometimes local suburbs. Thats where all the money is, and thats why they can sell line time cheaper than Ma Bell. Ma Bell has to charge higher rates in the cities to subsidize all the rural places where there is only one phone in 10 square miles. The alt. nets only serve the high volume areas, that is, large cities. Still, Sprint covers more cities than anyone else.

I have spent time since my last article breaking into various nets, and can report that MCI is by far the easiest. In fact, I was able to crack 3 codes in 30 minutes by hand, while talking to my roommate and listening to Pink Floyd. I had very little luck with Sprint, getting only one code. ITT is a little easier than Sprint, but I didn't get much there either. Western Union covers so few cities, its hardly worth breaking into.

If you have a computer with an autodial modem, you can program the computer to break codes. But there is no modem that I know of that can tell whether a phone is ringing or not, that is, whether the call went through or got stopped. But I got a great idea from a friend. Instead of sitting by your phone and listening as your computer runs through possible codes, program it to dial other computers through the net, and let it wait about 15 seconds after it finishes dialing each time, and see if it gets a carrier. Then the computer can tell by itself whether or not it has hit a good code, and you can go drop acid or whatever you do in your spare time.

But whenever you are breaking codes, make sure that the number you put in is a recording or a big company computer (like TELENET), not your girlfirends house, as the nets may wonder what all this activity is and try to call the number you are using, to see who lives there, who would be calling them illegally, and generally hassle them.

I also wouldn't worry too much about the nets tracing you, unless you are in their exchange. I call in from home sometimes. What I would worry about is them paying a little visit to the person you have called, and asking who they know that would be calling them at a large discount. So only call instant amnesiacs, and not your grandmother. If you really want to be safe, call through one net to another net in the city you want, then go through the second net to make a local call to your friend. The second net will only be making a local call, and so won't worry much about it. The first net will only be able to trace to the second net. Make the pigs work to find out who's screwing them over! But be sure not to use the same net twice in a row. Setting up various links of the call through various nets, sort of in series, is a great way to make alt nets safer. Unfortunately, it seriously degrades the quality of the final line you have to talk over.

To change the subject, I have noticed that some fire engines have big strobe lights mounted in the front, near the cherry lights. I found out that this is so that they can turn stop lights green. Many stop lights have photocells that sense incoming light to see if it is flashing at the proper frequency. If it is, then all lights on the side the strobe is coming from are turned green and all others are turned red. Anywhite strobe light should work, its the frequncy of the flashes that matter. I don't know what they are. But I do know that you need an awfully big strobe light, about the size of an airplane landing light it seemed to me. They are probatly expensive, although you may be able to get them cheap in a surplus store. I've seen this system in Anchorage, San Jose, and San Diego. I'm sure that many other cities have installed it on their major lights too, but check to make sure your city has it before buying a light.

Have phun phreaking and F.T.B.S!

COMPUTER SECURITY

and the breaking thereof

By Simon Jester

FLASH!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

There is a new method to break into computers, and it has professional security consultants shitting in their pants! In september 81, some students at UC Berkeley discovered a way to break into UNIX systems. One of them must have been a real asshole, because he told the system operator who told the system manager, who hired SRI to look into it. SRI is Stanford Research Institure Inter-national, and among other things they specialize in computer security. At SRI Donn Parker looked into the matter. Donn Parker is one of the top security experts in the world. He looked into the matter, and promptly realized that it compromized all security on the UNIX. He also speculated that the method could be adapted to work on other systems, as well.

UNIX is an operating system for DEC computers. I'm not sure if it works on other machines, but I have heard that Ma Bell uses a lot of UNIX systems. The scam goes like this. On large computers, they use a technique called time-sharing to let a lot of people use terminals all hooked up to one central computer all at the same time. Each person is assigned a portion of on-line memory (as opposed to disk memory), which is called his work space. The system saves a work space for itself, too. The students discovered a way of having one terminal take over control of another terminal and the workspace that goes along with the second terminal. The good part comes in here. Most students and hackers have low security accounts. But when you take over another workspace, the person logged on may have a high security account. If so, you could go through his account and access all the high security stuff he has access to that you're not supposed to have access to.

Only a few technical details on how to do this are known. It is known that you somehow send control and/or escape characters from your terminal through to the other persons terminal and/or workspace to take over control. This will work on UNIX systems, and there is some very similair method that may work on many other systems. Parker has said that the only effective ways of fighting this scam are to either remove the control/escape keys from all terminals or to insert software filters to filter out control/escape keys before they reach the OS. These are pretty lame solutions.

As Parker points out, removing the control/escape keys from every terminal is about as practical as installing MX missiles on underground railroads under Nevada. It won't work, because there are already over 3 million terminals in America, each with an escape and control key. And installing a software filter for control/escpae characters is a cheap fix too. Parker points out (and so do I) that operating systems are so complex that there will always be some way of slipping the characters around the filter and getting them to their destination. The proper way to fix this problem (from a cops point of view) would be to fix whatever aspect of the UNIX system allows the characters to let one workspace take over control of another. Since this idea seems to have been abandoned by Parker, and since he also points out that it would be possible to use this method on other operating systems, I come to the conclusion that the flaw is not in the UNIX code itself, but in the concept of time-sharing itself. I've read some of Parker's work, he isn't stupid. If there were a foolproof way of fixing this problem he would have found it by now.

So what does this mean? That we may be onto the biggest security system break in history! Almost any large computer is potentially vulnerable. But we need more information on how to do this. My information came from the LA Times. Tom has a copy of the article, and I'm sure he would send a copy to anyone who is interested, but it doesn't get too technical. It does mention two sources of more technical data about this. First of all, there was an article in InfoWorld during January about this (InfoWorld comes out weekly). So far I haven't been able to get a copy of this issue. If you have or can get a copy of it, PLEASE send it to me c/o TAP. The second source is from Parker at SRI. If you write to him on company stationary, and convince him that you are a security analyst or something similair, and give him a legitimate sounding address, he will send you a copy of his report on the subject, which tells every detail. His address is Donn Parker, SRI International, Menlo Park CA, 94025. Please don't write to him unless you have stationary and a business sounding address, and are sure you can convince him that you have a need to know. If he is deluged with requests for the report from phreaks, he will stop sending them out. I don't have either so I haven't been able to get the report. If you manage to get a copy, please PLEASE send a copy to me c/o TAP. Also, if you have any knowledge of UNIX systems, please write down whatever you know, system structure, security formats, whatever, and send it to me, as I don't know too much about UNIX. As soon as I know how to do this I will tell everyone in TAP, but I doubt I'll be able to find out unless you all help me by sending me whatever you do know.

Con game in the cards?

A New Jersey man was indicted yesterday on charges of spending more than $22,000 for goods and services through illegal use of credit cards obtained while in jail. The indictment by a federal grand jury in Newark charged Robert Lee Johnson with four counts of mail fraud and two counts of interstate use of fraudulently obtained credit cards.

The government charged that Johnson had 54 credit cards from 22 companies between Oct. 14, 1974, and March 6, 1978, while in jail.

The applications falsely stated that the defendant was employed by certain companies, making a substanial salary and receiving credit from several other sources, the indictment charged. The defendant gave the addresses of the Mercer and Union county jails, but claimed ownership of the buildings on several credit card applications, according to the indictment.

A Taxpayer Invents Ripoff

Hayward, Calif. — Bob Wister figures he can lower his property taxes by razing his house. He said that he is going to begin ripping his house apart board by board until it's worth $28,000 — what he paid for it in 1973. The latest assessment is for $38,000.

"I will rip down what is sufficient to get it down to the 1973 assessed value when I bought it," he said, vowing to stop only when a real-estate appraiser tells him he has reached the right value.

"That's what I can afford," he said. "I can't afford what it is now and I'm not going to stand for it. It practically doubles my taxes from what they were in 1973."

TAP, Room 603, 147 W. 42 St., NY 10036

75

Bulk Rate
US POSTAGE
PAID
Permit No. 3
Keasbey, N. J.

"We have a serious oil glut on our hands, gentlemen ... we'd better declare another shortage."