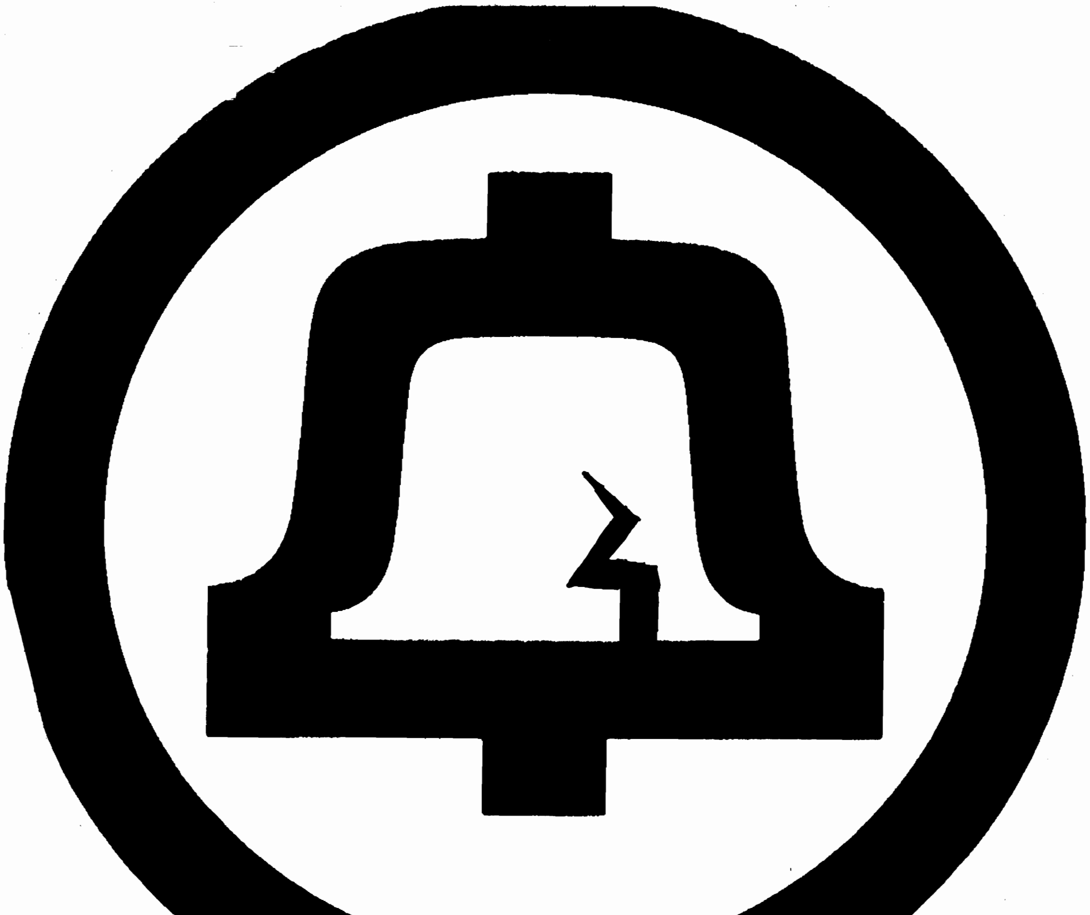
Cyber 'Zine

issue no. seven

Volume two



Need we say more?

A lot of people have been asking about information on the phone companies switch networks and maintenance systems. Information on this stuff is very hard to come by, unless you live in the CO's dumpster after school.

The Packet Switch Network is the computer that controls all the phone numbers in an area. It acts like the old time operators, as you call a number, the computer controls the switches of the number you are calling. Just like the operator connecting a line (the ring and tip, that is were those terms came from). Getting into this system could be very exciting, you could change your phone number (or some one else's), grant youself all of those expensive services like three-way calling. speed dialing, call blocking, etc. The dial-up is usually in the same prefix that the computer controls. If you do get a dial-up, the screen will say this- (this is in the Ameritek RBOC area):

```
AMERITECH ID:W05137B


WARNING!
THIS SYSTEM IS RESTRICTED TO AUTHORIZED USERS (editor note: Not us)
FOR AUTHORIZED BUSINESS PURPOSES. UNAUTHORIZED ACCESS IS A VIOLATION
OF LAW. PROPRIETARY OR CONFIDENTIAL INFORMATION MAY NOT BE DISCLOSED
WITHOUT PRIOR AUTHORIZATION.
```

Most of the time this is guarded by a password, but sometimes you'll just drop right in! The account number that is requested is the phone number of the phone you want to mess up or change. If you are just a beginner we recommend that you stay away form this as you could really mess it up for other hackers. (who cares if 100,000 people lose their phone service).

Also, if you get into a switch network, you will sometimes be able to shoot off into COSMOS. This is a COmputer System for Mainframe OperationS. It is unclear if this is still going or not because they are always up-grading their equipment. What it does is regional maintenance system. It sends out the signals that create or destroy phones. Along with this, is a system called MIZAR. (unclear if it still exsists). The local MIZAR actually does the work. Since COSMOS keeps records, most hacking is done on MIZAR. Of course, you encounter that little password problem again. Social engineering is almost out of the question is these cases. They won't give out their passwords because they have been burned too many times. If you do get in, print out a list of encrypted passwords. It will usually work by typing- % CATA /ETC/PASSWD

Here are some abbreveations you might encounter in COSMOS-
AA - the wire center
% - indicates your online
(if you get AA% -type ISH -then you should get H TN ***-****, the ***-**** is the phone number you used as the account #)
H - means hunt (through database)
TN - means trunk number (telephone number)

This is all for now, if you need more look at a offical COSMOS technical manuel. Obtained from very nice Bell men. We should be getting more information, so hang on.

Counter-Surveillance

Modern day spies are using the most advanced forms of espionage tools these days. There availability is increasing by sales trough spy shops around the world that offer low cost surveillance and counter-surveillance equipment. Here is a list of the most common devices used and how to defeat them.

Telephone Taps

This is probably the most commonly known, and used method in the world. It involves intercepting phone/fax/modem calls as they are made, and then transmitting them to a receiver or tape recorder. They can also be tapped by a method called the hookswitch bypass. After the telephone's hookswitch has been bypassed, it becomes "hot". This means that it will continue to transmit room sounds through telephone lines, even when the phone is hung up. We will show you how to do this later in the issue.

Since some phone taps are hard wired (wired directly to the phone line) measuring the voltage of the phone line will determine if the line is tapped. The phone company goes out of its way to keep the dial tone voltage at 48 volts d.c. Anything less or more than this is probably a tap. (AT&T will do free tap detections on your phone line if you ask them) Description of the hookswitch bypass or "Hot Mics" is on page 2

Wired Microphones

This method is used commonly in movies and by the police department. it involves a microphone and transmitter that is worn by a person, or is concealed inside an object. Since they operate on the standard radio spectrum, and are rarely encrypted, a standard radio frequency scanner set on search can be used to intercept the transmission or find the hidden transmitter. Also, a $100 radio frequency counter at Radio Shack will make a good transmitter detector. It will determine the exact frequency of a transmitter. This will make an inexpensive "bug" detector for any one concerned about their privacy.

Tape Recorders

Todays new, miniature voice-operated tape recorders make eavesdropping even easier. Just buy a small, external microphone and you can set the tape player anywhere you want. The voice-operated feature saves the batteries, and records only when someone is talking. The bad part is that they have to be retrieved after use.

Helpful Hints

- Since most hidden microphones detect sounds from all around, playing music, or a t.v. will defeat them.
-The 1000 Hz test line offered by the phone company can also be used to find taps in the phone line. If you have the right equipment, you can measure the return frequency of the test tone. If it is not 1000 Hz, a tap could be on your line.
- Ultra-violet light can be used to find the small holes pin-hole cameras use. They can also find changes in surface texture that may have been caused by someone installing a hidden transmitter.
- Physical inspection is the best form of counter-surveillance.
- Always check out any suspicious wires you might find.

TYPES OF HOT-MICS

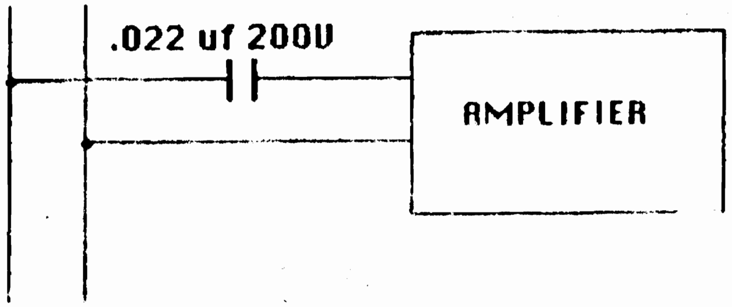


Fig 1

You can listen to Phone Conversations by directly Connecting an audio amplifier (Radio Sthack part # - 277-1008, $11.99) and a .022 uf Capacitor (Radio Shack part 272-1066, $.69) This only works if Some one is talking on the phone. The Capacitor removes any Click your Sister migh hear when you Connect it to the Phone lin

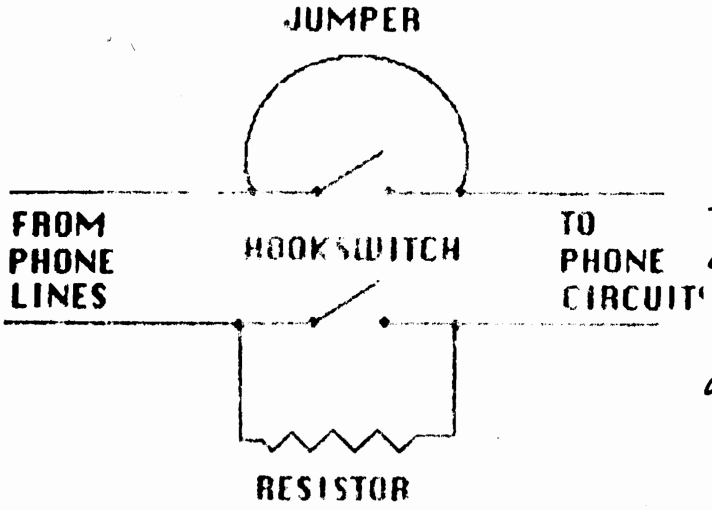


Fig 2

This must be done __INSIDE__ the targets Phone. Thele are two hookSwitches (They make the Clicking noise when you hang up the phone) A resistor of 10KΩ will work. The lower the lesistance the better. To low of lesistance will alter the ring of the phone. This set-up will transmit room sound down the phone line were you can then intercept them with the audio amplifier. (see fig 1)

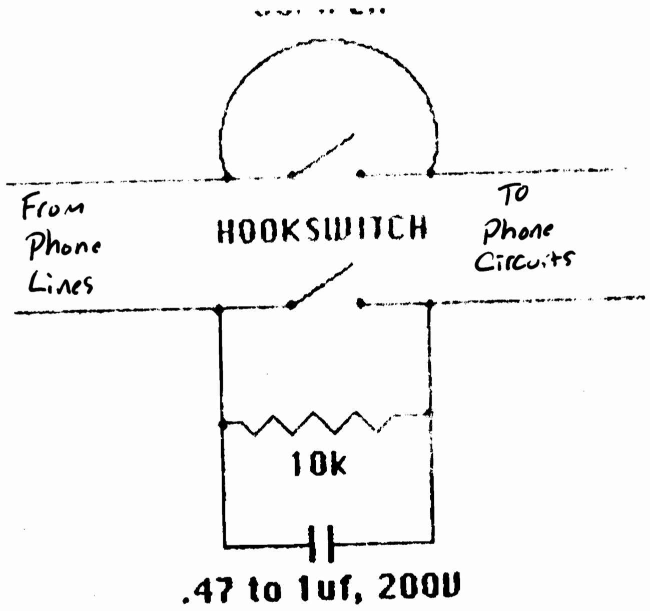


Fig 3

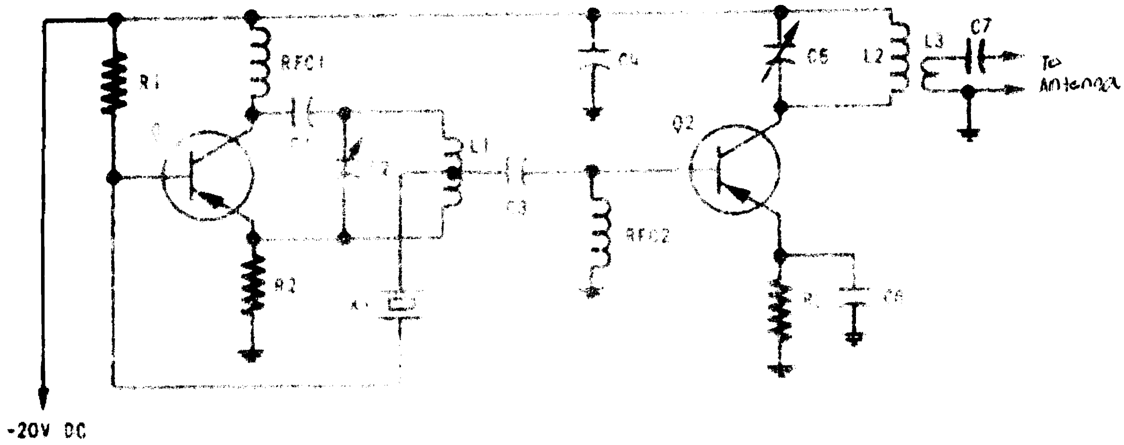
This is the Same basic Set-up as Figure 2, but with better quality output. The Sound can be recovered by doing set-up #1.

Installation Notes

- Make Sure the ring of the phone is not effected.
- Make Sure that room audio can't be heard on extension phones in the house.
- all of these use line voltage so they are easily detectable, but are widely used.

RCUITS - SURVEILLANCE

150 MHZ TRAMSMITTER

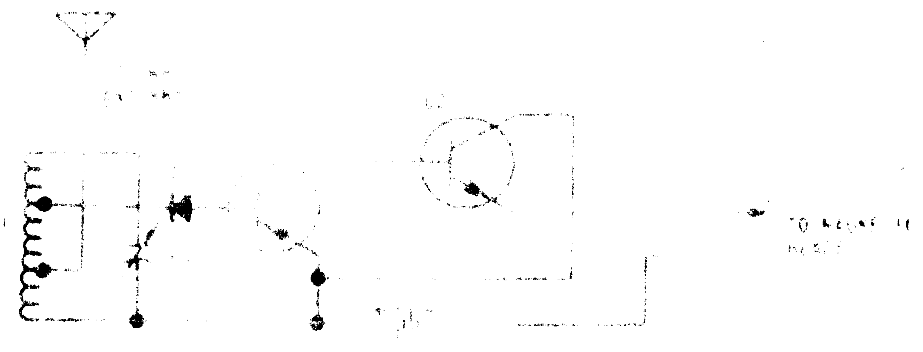


PARTS LIST

Q1 - [illegible] 2N-2[illegible] [illegible] PNP typ[illegible]
Q2 - [illegible] Q1 [illegible] L1- 8 [illegible] #[illegible] tapped 4 [illegible]
C1 - [illegible]
C2 - 51 [illegible] variable [illegible] L2- 8 [illegible] wire, 5/16"
C3 - 51 [illegible]
C4 & C7 [illegible] L3 [illegible] wire, [illegible]
C5 - [illegible] end of L2.
C6 - .[illegible]
R1 - [illegible] [illegible] series for
R2 - 1.[illegible] [illegible] frequency
R3 - [illegible] A[illegible] wire or whip

[illegible] CIRCUITS - CONTINUED

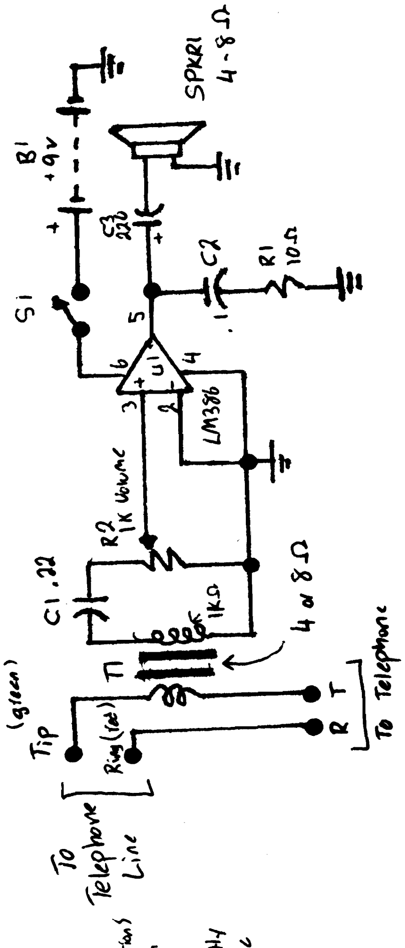
D[illegible] BODY OR
[illegible]



PARTS LIST

Q1 - 2N[illegible] [illegible] or equi[illegible] type
Q2 - [illegible]187, [illegible] equiv. [illegible] type.
D1 - [illegible]
C1 - [illegible] pf variable
L1 - 4 turns #[illegible] [illegible]ed, [illegible] form [illegible] long
Antenna tap [illegible] 1/2 turn from top. [illegible] tap is
2 turns up [illegible]om bottom.
B1 - [illegible] volts DC

[redacted]



This Circuit Will amplify Phone Conversations so every one can hear them. Connected directly to the phone line

PARTS LIST

U1 - LM386 low-Power audio amplifier, intergraded Circuit
R1 - 10 ohm, 1/4 watt, 5% resistor
R2 - 1000 ohm Potentiometer
C1 - 0.22 μF Ceramic-disc Capacitor
C2 - 0.1 μF Ceramic-dis Capacitor
C3 - 220μF, 16 WVDC, electrolytic capacitor
B1 - 9 Volt transistor - radio battery

SPKR1 - 4 to 8 Ω Speaker
S1 - SPST Toggle Switch
T1 - 1000 ohm to 8 ohm Center-tapped audio-output transformer

Test Line Numbers

These are from 1988, but should still be useful. Of course some of them have been changed, this should not effect anyone seriously, Just increase your phone number scan in the 958, 433, 497, and 952 exchanges.

These were given to Wisconsin Bell employees for the ability to test a customer's line without charging them. All ESS (Electronic Switching System)/Digital central offices were equipped with 958 toll free numbers for testing purposes. The type of test and their number are as follows:

Milliwatt (1000 Hz)	958-0010
Loop Around	958-0011
Dry Line	958-0012
Open	958-0013
Short	958-0014
Balance (900 Ohm)	958-0015
1004 Hz Tone	958-0016
Synchronous	958-0017
Coin	958-0018
Silent Termination	958-0019
Ring Back	97 and last 5 digits of ring back number, hang up twice.

These numbers also do the same thing and are used if the others are busy or not working. These are NOT toll free.

Green Bay ONLY (we will print other cities later)

Exchange	Number	Purpose
431	433-0015	Balance Termination
	433-0044	1000 Hz Tone
	433-0098	Synchronous
	433-0004	Transmission Test Line
	433-0014	Short Test
	433-0013	Open Test
	433-0011	Loop Around
	433-0010	Loop Milliwatt
434	434-0011	Balance Termination
	434-0010	1000 Hz Tone
	434-0009	Synchronous
	434-0004	Transmission Test Line
	434-0014	Short Test
	434-0013	Open Test
	434-0011	Loop Around
	434-0010	Loop Milliwatt
435	Use 433 test lines	
436	Use 433 test lines	
437	Use 433 test lines	
455	Use 433 test lines	

Continued on the next page------->>>

BELL RINGER

Exchange	Number	Purpose
465	465-0015	Balance Termination
	468-1097	1000 Hz
	465-0009	Synchronous
	465-0005	Transmission Test Line
	465-0014	Short Test
	465-0013	Open Test
	465-0011	Loop Around
	465-0010	Loop Milliwatt
468	Use 465 test lines	
469	Use 465 test lines	
494	Use 497 test lines	
496	Use 497 test lines	
497	497-0015	Balance Termination
	497-1097	1000 Hz
	497-4965	Synchronous
	497-0004	Transmission Test Line
	497-0014	Short Test
	497-0013	Open Test
	497-0011	Loop Around
	497-0010	Loop Milliwatt
498	Use 497 test lines	
499	Use 497 test lines	
952	952-0015	Balance Termination
	952-0012	1000 Hz Tone
	952-0098	Synchronous
	952-0004	Transmission Test Line
	952-0014	Short Test
	952-0013	Open Test
	952-0011	Loop Around
	952-0010	Loop Milliwatt

Ameritech operator 361 is
the supervisor in Green Bay

This is only a short list. There are a lot more test numbers that we don't have. Keep scanning exchanges (the first three numbers of your phone number) and your bound to find more. Bell doesn't like to give their numbers out so they maybe hard to find. Oh, by the way these numbers are confidential, and are not for use or disclosure outside Wisconsin Bell except under written agreement, heh-heh.

To obtain copies of the AT&T Bell System Technical Journal, write to:

AT&T Bell Laboratories Technical Journal
Room 1H321
101 J. F. Kennedy Parkway
Short Hills, NJ
07078

There are two types of journals, the Bell System Technical Journal, and the AT&T Bell Laboratories Technical Journal. Each issue has a number after the title, and a sub-title consisting of: no. and pt. Then a month followed by a year. For instance, the UNIX journal is- The Bell System Technical Journal 57
no. 6, pt. 2, July/August 1978

They are written by the Bell Laboratories staff, and some are reprinted by Prentice-Hall.

LOCK PICKING

This article will be helpful to any one that is new at the art of lock picking. Picking locks is easy, but it requires lots of practice. As long as you keep trying and practicing, I guarantee you'll have success.

Part one: Tools

Rakes- These come is a wide variety such as balls, half-balls, and diamond. They are used for raking a lock.

Feeler Picks- They come in two varieties half and full hook. They are used to feel and lift one pin at a time.

Tension wrench- A small lever that is used to turn the cylinder inside its shell. You must use the slightest amount of force possible.

Warded picks- Used to pick warded locks. See issue #1.

Lock pick guns- These open locks by forcing all the pins up at once. By turning on the tension wrench at the same time, you can open locks in seconds.

Ace picks- These pick the tubular locks found on most vending machines and parking meters.

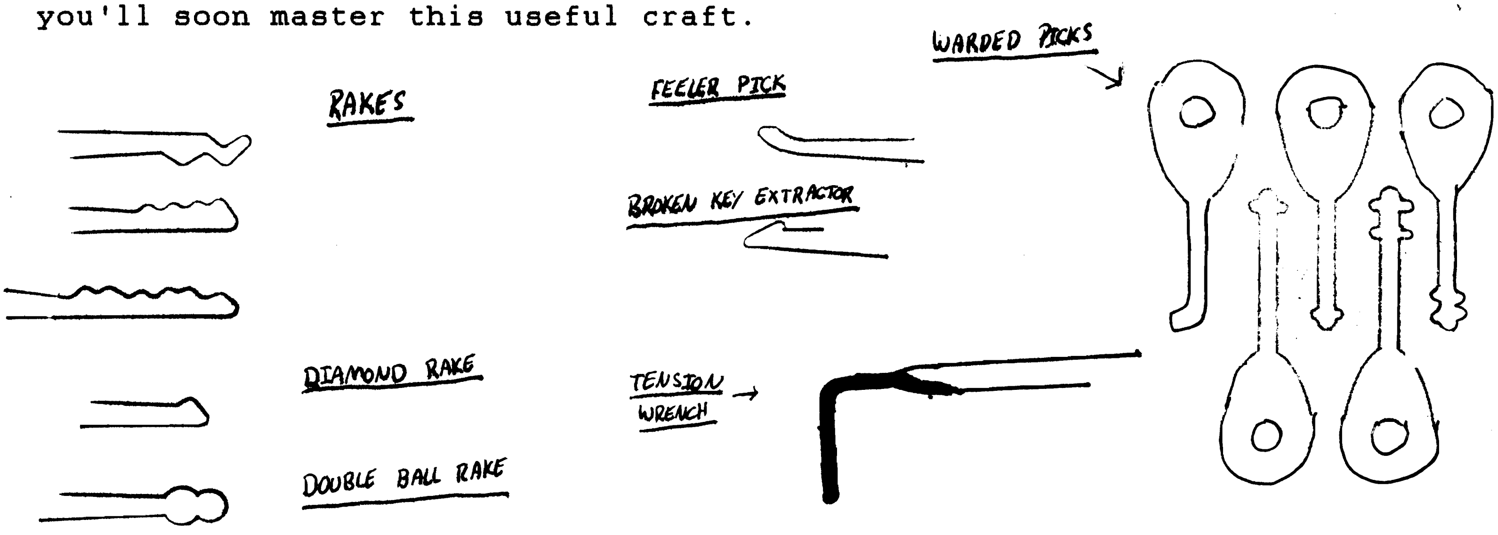
Part two: Picking locks

First off, I can't tell you every thing about locks, and lock picking. The best possible schooling is to just keep on practicing and reading books about locks and lock picking.

Insert your tension wrench in the lower portion of the keyway and insert your rake. Gently slide the rack back and forth with a very light torque on the tension wrench. Make sure that the top knocks of the pick are just barely touching the bottom pins on the lock. As each pin hits its shear line (when all the pins are at this line the lock opens), the tension wrench will turn very slightly. Sooner or later the cylinder will swing around and the lock will open.

A good tip when using the feeler pick is to start from the back. Before adding torque to the tension wrench find the last pin and by slowly applying torque with your tension wrench raise that pin to its shear line. The tension wrench will move ever so slightly, keep doing this to all the pins until the lock opens.

This should be enough until the next issue. Keep practicing and you'll soon master this useful craft.



The following article is how to enter Internet by using Telnet.

What the computer types will be in capitals, while whatever you need to type will be left small.

The dialup is 606-258-2400 (1200-2400 baud)

```
---------------------------------------------------------------------
WELCOME TO UKNET.
>>connect telnet
CONNECTING... (1) TELNET-020 SUCCESS.
YOU MAY NOW ENTER NET/ONE COMMANDS.
>>telnet
TELNET>>
---------------------------------------------------------------------
```

You may now enter the Telnet address that you want to get in.

Note- At TELNET>>, you must type Open to open the Telnet address you want. Example- open 165.113.1.30

EXTRA
^^^^^

-Number 14 washers make perfect dime slugs.

-By soldering wire to a quarter, you'll be able to put the quarter in a machine and pull it out quickly getting what ever you want for free. Also, you can drill a hole in the outside of the quarter and use fishing line for the same purpose.

-By putting a small hole at the end of a dollar bill, and attaching dental floss to it, you'll be able to put it in a change machine and pull it out, getting the change and keeping your dollar.

-If you make your own slugs (fake quarters, dimes, and nickels), make sure they are non-magnetic. This is the first thing machines check for. Also, make sure they are round, and are approximately the same weight.

-Supposedly, by putting a concentrated mixture of salt and water into the bill insert slot, you'll be able to get money out of it. We have never tried this, but it might work. (use a straw)

Free Local Phone Calls
~~~~~~~~~~~~~~~~~~~~~~

For those of you that saw the movie "War Games", you may be suprised to learn that punching pay phones still works (grounding out the tone/pulse that checks for money). It only works in certain areas because they are constantly upgrading their equipment. Here's the procedure:

NAILS?

1. Find a pay phone. Take a small nail and poke a hole in the mouthpiece. (see diagram) If you can't get it yourself, use the pay phone as a hammer to push the nail in. You must break the metal seal of the microphone.

SHOCKS?

2. Next, dial the first six digits of the local phone number. At the same time (Important) you push the seventh digit- push the nail into the hole (at a downward angle, usually) you created, and then pull the nail out. The whole process should last only a second. You may expeience a small shock (100 volts, don't be a wimp). It probably won't work your first time because it takes some getting used to.
~~~~~~~~~~~~~~~~~~~~~~