what a white box can do

This article describes how to take a standard touch tone keypad and convert it to a portable unit. This information is essentially public domain and was originally downloaded from the old GSNY BBS. It is also available on Sherwood Stenotype and undoubtedly other BBS's around the world. It is being reprinted and explained here for those who are not able to get this type of information from BBS's and for those who are just starting out in the phone phreak business.

If you convert a touch tone keypad in the manner described below you will become one familiar with the inner workings of your telephone and telephone system. You will also be able to use rotary phones to call extenders or phone services that respond to touch tones, because you now will be able to generate touch tones yourself without having to depend on the phone. You will now be able to use payphones that turn off their touch tones after you dial your number. In addition, there are often phones in airports, hotels, and at bank machines which have no dial on them and automatically dial a pre-programmed number (usually a service number), which can be used to generate touch tones. To connect the keypad to your phone, you will need a line cord. The power required by a wired keypad is about 25 volts, but they will work with as little as 15, thereby allowing you to use two 9 volt radio batteries. As you may have expected, they are also designed to operate with a telephone line speaker (and phone line), and not the standard B-ohm speaker which needs to be used for adequate volume. To accomplish this, we use a matching transformer, this is one of those miniature ones available at Radio Shack. Enough of the theory, now for the circuit.

You will need:

A touch tone keypad
A miniature 100k to 1k ohm transformer
(Radio Shack # 273-590)
A standard 8-ohm speaker
Two 9 volt radio batteries
Two 9-volt battery clips
A case to put it all in (optional)

A few construction notes, it is suggested that you solder and tape all connections. It is also important to read the entire article before attempting to construct this.

First connect the RED wire of the transformer to either terminal on the speaker. Now connect the WHITE wire from the transformer to the other terminal on the speaker. Next, connect the RED (positive) wire of one battery clip to the black wire of the other battery clip. Now connect the remaining RED wire on the second battery clip to the GREEN wire from the touch tone pad. Connect the BLUE wire from the touch tone pad to the ORANGE and BLACK striped wire from the touch tone pad. To these two wires, now connect the remaining lead from first battery clip. You have now finished the power connection to the keypad. Connect the BLACK wire from the keypad to the BLUE wire on the transformer. Next connect the RED and GREEN striped wire from the keypad to the GREEN wire on the transformer. The BLACK wire on the transformer should be connected to anything, along with quite a few wires from the keypad. The connection of the keypad is now complete. All you have to do is connect two nine volt batteries to the battery clips, and you'll be ready to go. You may want to mount it in a case for easy portability. Note that the silver box modification CAN be used with this unit, allowing complete remote phreaking. This is a bit more complex than the conversion you have accomplished above. When none of the buttons are pressed, this unit uses no power, thereby eliminating the need for a power switch, and extending the life of the batteries.

A phone phreak scores

This is another story to add to the annals of social engineering, one which we all can learn from...

A few months ago my Mom had some people revisit and blacklist our driveway. So she called some companies in the phone book, and she chose the cheapest one. They came and did most of the work, and Mom paid them, providing they case back soon to finish the blacktopping job. This all sounded, but after several weeks of the company calling up and postponing the final work, Mom wanted it done. She decided to visit the company at the address listed in the phone book, because she would always get an answering machine when she called them, but when she called she found it was just the back room of a storefront and that the company had vacated it a few months earlier. When she tried calling them their number had been changed. So I did a CNA on their new number for Mom, and she visited the new address that I got. When Mom got there she found a vacant lot. It was at this point that it started to sound pretty fishy to Mom and I. But how could we find out where they were, if they gave a fake address to the phone company?

That's when it occurred to me to call the business office that handles that company's telephone. I called and they answered, "Your number, please." So I gave them the company's number, and I proceeded to tell them how I did not get my last phone bill, and how I wanted to make sure they were sending it to the right address. They told me the real name and address (not the one at CNA or Directory Assistance, which was the one it was listed under), there is a difference, you know, they asked if I was "Mr. So and So", to which I responded "Yes." Then they asked if I wanted to change the mailing address. I said, "No, that's my partner's address. No need to change it. Thank you.

And that was it. I found their address. Mom visited their new location, which happened to be a trailer in the middle of a big field with a telephone and a power cable going into it. When she found the people at the company, they were quite startled, because it seemed that they did not have a license to do the work that they were doing and other customers and some government agencies looking for them. Since Mom had the goods on them, they were obliged to finish 2-19 our driveway, and that's all Mom wanted after all.
HACKING PACKARD

by BioC Agent 003

Available in full on Sherwood Forest II (9143591517) - 2/20

PREFACE

The purpose of this tutorial is to give potential hackers useful information about Hewlett-Packard's HP2000 systems. The following tutorial is in a CR character set. CR - carriage return, RETURN, ENTER, etc.

CAPITAL LETTERS - for user input.

SYSTEM INFORMATION

Each HP2000 system can support up to 32 users in a TimeShared Basic (TSB) environment. HP-POSIX is an add-on UNIX "look alike" version of TSB. HP-POSIX is run on a version of TSB called 

\text{LODEN PROCEDURE}

Once connected to the HP2000, you can enter a menu followed by a CR. The system then responds with: PLEASE LOG IN. If it does not immediately respond on try this procedure until it does (they tend to be slow to respond). User ID: The user ID consists of a letter followed by 3 digits, e.g., H241.

Password: The passwords are from 1 to 20 printing and/or non-printing (control) characters. The following characters will not be found in any passwords so don't bother trying them: line delete ('\x01'), null ('\x00'), return ('\r'), line feed ('\n'), delete ('\x15'), space ('\x20'), back arrow ('\x08'), underscore ('\_'). HP also suggests that 'E' is not used in passwords (but I have seen it done).

The login format is: HELLO-AI23-PASSWD. Where: HELLO is the login prompt, it may be abbreviated to HEL. AI23 is user ID: PASSWD is the password.

The system will respond with either an ILLEGAL FORMAT or ILLEGAL ADDRESS. If you screw up the syntax or it is an invalid user ID or password. The messages: PLEASE LOG IN, ILLEGAL FORMAT, & ILLEGAL ACCESS also help you identify HP2000 syntax.

The system may also respond with ALL PORTS ARE BUSY NOW - PLEASE TRY AGAIN LATER or a similar message. One other possibility is NO TIME LEFT which means that you have used up your time limit without paying.

Unlike other systems where you have a certain amount of tries to login, HP users get a certain amount of time to login before it dumps you. The system default is 120 seconds (2 minutes). The swap can change it to be anywhere between 1 and 120 seconds. The 120 seconds is sufficient time for trying between 40-50 login attempts while hand-hacking a much higher amount when using a hacking program.

USERS

The various users are identified by their user id (AI23) 

password. User names are also identified by their group. Each group consists of 100 users; for example, A000 through A999 is group A000. A100 through A199 is another group. A200 through A299 is the last possible group. The first user is in each group is designated as the Group Master and he has certain privileges. For example, A000, A100, A900, A990 are all Group Masters. The user id A000 is known as the System Master and he has the most privileges besides the hardswp terminal. The library associated with user 2999 can be used to store a HELLO program which is executed each time someone logs on. The system master can hook up to the System Master (A000) but it is the only user id that must be logged on by typing HELP-HELLO-PASSWD. You just have to hook up his password. If you decide to hack 2999, you can create your own personal library. For example, login HELLO and every time you login you have your own personal library. Every time you login, this is about all you can do with 2999, though it is otherwise a non-privileged account.

LIBRARY ORGANIZATION

Each user has access to 3 levels of libraries: his own private library, a group library, and the system library. To see what is in these libraries you would type: CATALOG. GROUP Library: Library libraries (or all commands that can be abbreviated to the first 3 letters) are the library responsible for his own library and maintaining all files. If a program is in your CATALOG, then you can change it.

Group Masters (GM) are responsible for controlling all programs in the Group library. Only members of the group can use these programs (i.e., a type of GROUP). For example, User A000 can control all programs in the Group library of all users beginning with id S5xx. Other users in the group can modify these programs. All programs in the group library are also private, i.e., they are PROTECT & UMPROTECT. With the exceptions of GROUP commands, a command is PROT. If a program is moved, it must be UNPROT.

The Group Master also has access to all privileged commands. They are: PROTECT & UMPROTECT. With the exceptions of GROUP commands, a command is PROT. If a program is moved, it must be UNPROT.

There are 3 primary libraries: User, Group, and the System. The System has the most privileges.

The System has a VALUABLE card to help guide counselors help students to select colleges, jobs, financial aid, etc. GIS is the University's card to help guide counselors help students to select colleges, jobs, financial aid, etc.

HP-POSIX is an add-on UNIX "look alike" version of TSB. HP-POSIX is run on a version of TSB called 

\text{SUPPORTIBRARY}

All users have access to these files by typing LIBRARY to view them. Only the System Master can modify these files since he owns the library & owns the PROTECT command. The GM also has access to other privileged commands such as DIRECTORY: this command will print out all files and program names stored on the system. The GM can print out the entire directory. DIR-S500 will start listing the directory with user S500. Example:

```
DIR-S500 0155/84 1247
A000 0563/84 LENGTH 3156 DRUM
```

The.advantage of hacking the 4000 password is that you can use the privileged commands to see which user id's exist and what programs are stored where so that you can further penetrate the system.

NOTE: There are different levels (versions) of TSB/2000. This article is based primarily on Level F. Most of the levels are similar in their commands so the differences should not be too much of a hacker. Also, the HP usually used its own personal library every time you login. This is about all you can do with 2999, though it is otherwise a non-privileged account.

PROGRAMS

Hewlett-Packard often provides programs from their TSB Library for the systems. Utilities such as ASCII, PRINT, & others are almost inevitably found on every system. Standard games such as MUPUS, TUCK, LUNAR, & many others are also a must. Other companies offer very large programs for the HP2000 also. BIS (Guidance Information System) is a database to help guidance counselors help students to select colleges, jobs, financial aid, etc. BIS is usually found in the S5xx group library (anyone with an S5xx password can use it). Unfortunately, sometimes these programs are set so that a certain command will automatically run them. In some cases you can abort by pressing the BREAK key. There is a function that disables the BREAK key. In this case, only the System or the program can throw you into BASIC. There are many built-ins that the HP2000 that allow users to do all sorts of things. If you run across any of these be sure to let us know.

Most of the HP2000 systems are used by schools, school districts, BOCES, and various businesses. This was an ideal system for schools before micro-computers existed. The HP2000 systems have been in existence since 1973. A400/2000 was replaced by the HP3000 but there are still many HP2000 systems in existence and believe that they will stay there for awhile. Here are the major HP systems getting you to set up for: 203/622-1531, 312/777-7601, 312/958-8170, 312/455-2283, 718/327-7540)

1. AN: belongs to NYU. Type 'HP' at the prompt. Then hit the BREAK key slowly until you see the backslash (\) prompt. You are then in.
At the Last Stroke...

Associated Press

At precisely 11 am on April 2nd a man's voice was heard on Britain's telephone talking clock for the first time. The smooth baritone voice of part-time actor Brian Cobby, 55 years old, replaced the modulated contralto of Pat Simmons, whose voice was retired after 21 years at precisely 10:59 and 50 seconds. Last December Mr. Cobby was chosen from among 5,000 competitors to tell the nation the precise time every 10 seconds in a recorded telephone message that is expected to receive 300 million calls this year.

Only two other voices have been heard on the telephone clock since it was devised in 1939. Both were women's. Mr. Cobby, an assistant supervisor at a telephone exchange in Brightling in southern England, said it was "a great honor to be Britain's watchman." He was paid the equivalent of $6,000 to record the 8,640 time announcements in one 24-hour period.

Good Apples for the Soviets

The New York Times

The Reagan Administration appears to be prepared to cooperate with Soviet efforts to put personal computers in secondary schools, according to industry officials negotiating export licenses.

"We expected it would be more difficult, so I was quite pleasantly surprised," said Albert Eisenstadt, a vice president of Apple Computer who was in Washington to discuss computer exports with Commerce and Defense Department officials. "They just want to make sure we do it right.

The Soviets are already producing their own "Agat"--a Soviet knockoff of an Apple II, but are not able to produce enough. That is why IBM, Commodore, Sinclair Research Ltd., and Apple are all competing for the Soviet market. The Commerce Department has argued that it makes no sense to bar American companies from selling computers the Russians could easily obtain in Japan and Britain. The Defense Department, which has taken a harder line, seems unperturbed by the thought of exporting thousands of machines, provided they are used for education. By law the sale of "hardened" machines that are designed to withstand battlefield conditions are barred.

Hackers Go Free

The New York Times

Four teenagers who used home computers to tap into a space agency computer at the Marshall Space Flight Center will not be prosecuted, United States Attorney Frank Donaldson announced.

The FBI seized the youths' computer equipment at their homes in Huntsville, Alabama, last July 16 after tracing the phone calls used to enter the computer. Unauthorized access to a computer is not permitted.

One of the youths, Robert Grumbles, 17 years old, said he wished the FBI would return his $5,000 computer because "I don't see any reason for them to keep it."

[Keep up the spirit, Rob.]

Robots Kills Man

The New York Times

Last summer, a Michigan man was the first worker killed by a robot in this country. The 34-year-old victim, working with automated die-casting machinery last July, was pinned between the back of a robot and a steel pole, the National Center for Disease Control reported. The worker suffered a heart attack, lapsed into a coma and died five days later.

There are more than 5,000 robots in use nationwide.

'Santa Fraud'

Associated Press

Randy Grimm didn't know it cost 55 cents every time he called a sports trivia game, so he didn't quite pleasantly surprised, "I was quite pleasantly surprised," said Albert Eisenstadt, a vice president of Apple Computer who was in Washington to discuss computer exports with Commerce and Defense Department officials. "They just want to make sure we do it right.

The Soviets are already producing their own "Agat"--a Soviet knockoff of an Apple II, but are not able to produce enough. That is why IBM, Commodore, Sinclair Research Ltd., and Apple are all competing for the Soviet market. The Commerce Department has argued that it makes no sense to bar American companies from selling computers the Russians could easily obtain in Japan and Britain. The Defense Department, which has taken a harder line, seems unperturbed by the thought of exporting thousands of machines, provided they are used for education. By law the sale of "hardened" machines that are designed to withstand battlefield conditions are barred.

Hackers Go Free

The New York Times

Four teenagers who used home computers to tap into a space agency computer at the Marshall Space Flight Center will not be prosecuted, United States Attorney Frank Donaldson announced.

The FBI seized the youths' computer equipment at their homes in Huntsville, Alabama, last July 16 after tracing the phone calls used to enter the computer. Unauthorized access to a computer is not permitted.

One of the youths, Robert Grumbles, 17 years old, said he wished the FBI would return his $5,000 computer because "I don't see any reason for them to keep it."

[Keep up the spirit, Rob.]

Robot Kills Man

The New York Times

Last summer, a Michigan man was the first worker killed by a robot in this country. The 34-year-old victim, working with automated die-casting machinery last July, was pinned between the back of a robot and a steel pole, the National Center for Disease Control reported. The worker suffered a heart attack, lapsed into a coma and died five days later.

There are more than 5,000 robots in use nationwide.

'Santa Fraud'

Associated Press

Randy Grimm didn't know it cost 55 cents every time he called a sports trivia game, so he didn't quite pleasantly surprised, "I was quite pleasantly surprised," said Albert Eisenstadt, a vice president of Apple Computer who was in Washington to discuss computer exports with Commerce and Defense Department officials. "They just want to make sure we do it right.

The Soviets are already producing their own "Agat"--a Soviet knockoff of an Apple II, but are not able to produce enough. That is why IBM, Commodore, Sinclair Research Ltd., and Apple are all competing for the Soviet market. The Commerce Department has argued that it makes no sense to bar American companies from selling computers the Russians could easily obtain in Japan and Britain. The Defense Department, which has taken a harder line, seems unperturbed by the thought of exporting thousands of machines, provided they are used for education. By law the sale of "hardened" machines that are designed to withstand battlefield conditions are barred.

Hackers Go Free

The New York Times

Four teenagers who used home computers to tap into a space agency computer at the Marshall Space Flight Center will not be prosecuted, United States Attorney Frank Donaldson announced.

The FBI seized the youths' computer equipment at their homes in Huntsville, Alabama, last July 16 after tracing the phone calls used to enter the computer. Unauthorized access to a computer is not permitted.

One of the youths, Robert Grumbles, 17 years old, said he wished the FBI would return his $5,000 computer because "I don't see any reason for them to keep it."

[Keep up the spirit, Rob.]

Robot Kills Man

The New York Times

Last summer, a Michigan man was the first worker killed by a robot in this country. The 34-year-old victim, working with automated die-casting machinery last July, was pinned between the back of a robot and a steel pole, the National Center for Disease Control reported. The worker suffered a heart attack, lapsed into a coma and died five days later.

There are more than 5,000 robots in use nationwide.

'Santa Fraud'

Associated Press

Randy Grimm didn't know it cost 55 cents every time he called a sports trivia game, so he didn't quite pleasantly surprised, "I was quite pleasantly surprised," said Albert Eisenstadt, a vice president of Apple Computer who was in Washington to discuss computer exports with Commerce and Defense Department officials. "They just want to make sure we do it right.

The Soviets are already producing their own "Agat"--a Soviet knockoff of an Apple II, but are not able to produce enough. That is why IBM, Commodore, Sinclair Research Ltd., and Apple are all competing for the Soviet market. The Commerce Department has argued that it makes no sense to bar American companies from selling computers the Russians could easily obtain in Japan and Britain. The Defense Department, which has taken a harder line, seems unperturbed by the thought of exporting thousands of machines, provided they are used for education. By law the sale of "hardened" machines that are designed to withstand battlefield conditions are barred.

Hackers Go Free

The New York Times

Four teenagers who used home computers to tap into a space agency computer at the Marshall Space Flight Center will not be prosecuted, United States Attorney Frank Donaldson announced.

The FBI seized the youths' computer equipment at their homes in Huntsville, Alabama, last July 16 after tracing the phone calls used to enter the computer. Unauthorized access to a computer is not permitted.

One of the youths, Robert Grumbles, 17 years old, said he wished the FBI would return his $5,000 computer because "I don't see any reason for them to keep it."

[Keep up the spirit, Rob.]

Robot Kills Man

The New York Times

Last summer, a Michigan man was the first worker killed by a robot in this country. The 34-year-old victim, working with automated die-casting machinery last July, was pinned between the back of a robot and a steel pole, the National Center for Disease Control reported. The worker suffered a heart attack, lapsed into a coma and died five days later.

There are more than 5,000 robots in use nationwide.

'Santa Fraud'

Associated Press

Randy Grimm didn't know it cost 55 cents every time he called a sports trivia game, so he didn't quite pleasantly surprised, "I was quite pleasantly surprised," said Albert Eisenstadt, a vice president of Apple Computer who was in Washington to discuss computer exports with Commerce and Defense Department officials. "They just want to make sure we do it right.

The Soviets are already producing their own "Agat"--a Soviet knockoff of an Apple II, but are not able to produce enough. That is why IBM, Commodore, Sinclair Research Ltd., and Apple are all competing for the Soviet market. The Commerce Department has argued that it makes no sense to bar American companies from selling computers the Russians could easily obtain in Japan and Britain. The Defense Department, which has taken a harder line, seems unperturbed by the thought of exporting thousands of machines, provided they are used for education. By law the sale of "hardened" machines that are designed to withstand battlefield conditions are barred.

Hackers Go Free

The New York Times

Four teenagers who used home computers to tap into a space agency computer at the Marshall Space Flight Center will not be prosecuted, United States Attorney Frank Donaldson announced.

The FBI seized the youths' computer equipment at their homes in Huntsville, Alabama, last July 16 after tracing the phone calls used to enter the computer. Unauthorized access to a computer is not permitted.

One of the youths, Robert Grumbles, 17 years old, said he wished the FBI would return his $5,000 computer because "I don't see any reason for them to keep it."

[Keep up the spirit, Rob.]

Robot Kills Man

The New York Times

Last summer, a Michigan man was the first worker killed by a robot in this country. The 34-year-old victim, working with automated die-casting machinery last July, was pinned between the back of a robot and a steel pole, the National Center for Disease Control reported. The worker suffered a heart attack, lapsed into a coma and died five days later.

There are more than 5,000 robots in use nationwide.
DEAR 2600:

When will it almost be impossible to use Long Distance Services? It is so easy to Phreak off these and they never catch the majority of us, but when will it stop?

JUSt REALIZED THAT THERE WAS JUST NOT ENOUGH EVIDENCE TO PROVE ANYTHING, BUT CALIFORNIA STILL HAS HORRIBLE TOUGH LAWS... EVEN DISCLOSE A PHONE NUMBER OR A PASSWORD FOR A TEL/EVEN A WHOLE PASSWORD THERE... WE ARE GLAD HE GOT HIS COMPUTER BACK

DEAR 2600: Have you been reading about those new high tech secure telephones? I've been thinking about what must be inside them. The closest thing I've heard to that kind of technology would be something like digital audio processing, but after the voice is turned into bits, they scramble them up and then send them off. The other side then decrypts the bits and transforms the encrypted signal back into voice. The stuff I've read (in Popular Communications Magazine, around a year ago) said that a lot of law enforcement agencies use it to intercept phone calls... I'd rather tape audio than video. (I believe they mentioned were the DEI and the Treasury Police. I'm not sure if they actually discuss it.)

OPEN LETTER:

ALL THIS HAPPENS AFTER THE VOICE IS TURNED INTO BITS. I SERIOUSLY DOUBT THAT ANYTHING CAN STOP THIS. I have no idea how sophisticated this is, but it seems to me that it could be a potential security risk...

DEAR 2600: You have been reading about those new high tech secure telephones? I've been thinking about what must be inside them. The closest thing I've heard to that kind of technology would be something like digital audio processing, but after the voice is turned into bits, they scramble them up and then send them off. The other side then decrypts the bits and transforms the encrypted signal back into voice. The stuff I've read (in Popular Communications Magazine, around a year ago) said that a lot of law enforcement agencies use it to intercept phone calls... I'd rather tape audio than video. (I believe they mentioned were the DEI and the Treasury Police. I'm not sure if they actually discuss it.)

DEAR 2600:

When will it almost be impossible to use Long Distance Services? It is so easy to Phreak off these and they never catch the majority of us, but when will it stop?

JUSt REALIZED THAT THERE WAS JUST NOT ENOUGH EVIDENCE TO PROVE ANYTHING, BUT CALIFORNIA STILL HAS HORRIBLE TOUGH LAWS... EVEN DISCLOSE A PHONE NUMBER OR A PASSWORD FOR A TEL/EVEN A WHOLE PASSWORD THERE... WE ARE GLAD HE GOT HIS COMPUTER BACK

DEAR 2600: Have you been reading about those new high tech secure telephones? I've been thinking about what must be inside them. The closest thing I've heard to that kind of technology would be something like digital audio processing, but after the voice is turned into bits, they scramble them up and then send them off. The other side then decrypts the bits and transforms the encrypted signal back into voice. The stuff I've read (in Popular Communications Magazine, around a year ago) said that a lot of law enforcement agencies use it to intercept phone calls... I'd rather tape audio than video. (I believe they mentioned were the DEI and the Treasury Police. I'm not sure if they actually discuss it.)

OPEN LETTER:

ALL THIS HAPPENS AFTER THE VOICE IS TURNED INTO BITS. I SERIOUSLY DOUBT THAT ANYTHING CAN STOP THIS. I have no idea how sophisticated this is, but it seems to me that it could be a potential security risk...

DEAR 2600:

When will it almost be impossible to use Long Distance Services? It is so easy to Phreak off these and they never catch the majority of us, but when will it stop?

JUSt REALIZED THAT THERE WAS JUST NOT ENOUGH EVIDENCE TO PROVE ANYTHING, BUT CALIFORNIA STILL HAS HORRIBLE TOUGH LAWS... EVEN DISCLOSE A PHONE NUMBER OR A PASSWORD FOR A TEL/EVEN A WHOLE PASSWORD THERE... WE ARE GLAD HE GOT HIS COMPUTER BACK

DEAR 2600: Have you been reading about those new high tech secure telephones? I've been thinking about what must be inside them. The closest thing I've heard to that kind of technology would be something like digital audio processing, but after the voice is turned into bits, they scramble them up and then send them off. The other side then decrypts the bits and transforms the encrypted signal back into voice. The stuff I've read (in Popular Communications Magazine, around a year ago) said that a lot of law enforcement agencies use it to intercept phone calls... I'd rather tape audio than video. (I believe they mentioned were the DEI and the Treasury Police. I'm not sure if they actually discuss it.)

OPEN LETTER:

ALL THIS HAPPENS AFTER THE VOICE IS TURNED INTO BITS. I SERIOUSLY DOUBT THAT ANYTHING CAN STOP THIS. I have no idea how sophisticated this is, but it seems to me that it could be a potential security risk...

DEAR 2600:

When will it almost be impossible to use Long Distance Services? It is so easy to Phreak off these and they never catch the majority of us, but when will it stop?

JUSt REALIZED THAT THERE WAS JUST NOT ENOUGH EVIDENCE TO PROVE ANYTHING, BUT CALIFORNIA STILL HAS HORRIBLE TOUGH LAWS... EVEN DISCLOSE A PHONE NUMBER OR A PASSWORD FOR A TEL/EVEN A WHOLE PASSWORD THERE... WE ARE GLAD HE GOT HIS COMPUTER BACK

DEAR 2600: Have you been reading about those new high tech secure telephones? I've been thinking about what must be inside them. The closest thing I've heard to that kind of technology would be something like digital audio processing, but after the voice is turned into bits, they scramble them up and then send them off. The other side then decrypts the bits and transforms the encrypted signal back into voice. The stuff I've read (in Popular Communications Magazine, around a year ago) said that a lot of law enforcement agencies use it to intercept phone calls... I'd rather tape audio than video. (I believe they mentioned were the DEI and the Treasury Police. I'm not sure if they actually discuss it.)
<table>
<thead>
<tr>
<th>State</th>
<th>Institution</th>
<th>Domain</th>
<th>Address</th>
<th>Location Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>OH</td>
<td>The Ohio State University</td>
<td>OSU</td>
<td>Columbus, OH</td>
<td>Columbus</td>
</tr>
<tr>
<td>NC</td>
<td>University of North Carolina</td>
<td>UNCCD</td>
<td>Charlotte, NC</td>
<td>Charlotte</td>
</tr>
<tr>
<td>SC</td>
<td>Clemson University</td>
<td>CLEM</td>
<td>Clemson, SC</td>
<td>Clemson</td>
</tr>
<tr>
<td>AR</td>
<td>University of Arkansas</td>
<td>AR</td>
<td>Fayetteville, AR</td>
<td>Fayetteville</td>
</tr>
<tr>
<td>TX</td>
<td>The University of Texas</td>
<td>UT</td>
<td>Austin, TX</td>
<td>Austin</td>
</tr>
<tr>
<td>CA</td>
<td>University of California</td>
<td>UC</td>
<td>Los Angeles, CA</td>
<td>Los Angeles</td>
</tr>
<tr>
<td>WA</td>
<td>University of Washington</td>
<td>UW</td>
<td>Seattle, WA</td>
<td>Seattle</td>
</tr>
<tr>
<td>CO</td>
<td>Colorado State University</td>
<td>CSU</td>
<td>Boulder, CO</td>
<td>Boulder</td>
</tr>
<tr>
<td>IL</td>
<td>Illinois State University</td>
<td>ISU</td>
<td>Urbana, IL</td>
<td>Urbana</td>
</tr>
<tr>
<td>MN</td>
<td>University of Minnesota</td>
<td>UMN</td>
<td>Minneapolis, MN</td>
<td>Minneapolis</td>
</tr>
<tr>
<td>WI</td>
<td>University of Wisconsin</td>
<td>UW</td>
<td>Madison, WI</td>
<td>Madison</td>
</tr>
<tr>
<td>MO</td>
<td>University of Missouri</td>
<td>MU</td>
<td>Columbia, MO</td>
<td>Columbia</td>
</tr>
<tr>
<td>AR</td>
<td>University of Arkansas</td>
<td>AR</td>
<td>Fayetteville, AR</td>
<td>Fayetteville</td>
</tr>
<tr>
<td>TX</td>
<td>The University of Texas</td>
<td>UT</td>
<td>Austin, TX</td>
<td>Austin</td>
</tr>
<tr>
<td>CA</td>
<td>University of California</td>
<td>UC</td>
<td>Los Angeles, CA</td>
<td>Los Angeles</td>
</tr>
<tr>
<td>WA</td>
<td>University of Washington</td>
<td>UW</td>
<td>Seattle, WA</td>
<td>Seattle</td>
</tr>
<tr>
<td>CO</td>
<td>Colorado State University</td>
<td>CSU</td>
<td>Boulder, CO</td>
<td>Boulder</td>
</tr>
<tr>
<td>IL</td>
<td>Illinois State University</td>
<td>ISU</td>
<td>Urbana, IL</td>
<td>Urbana</td>
</tr>
<tr>
<td>MN</td>
<td>University of Minnesota</td>
<td>UMN</td>
<td>Minneapolis, MN</td>
<td>Minneapolis</td>
</tr>
<tr>
<td>WI</td>
<td>University of Wisconsin</td>
<td>UW</td>
<td>Madison, WI</td>
<td>Madison</td>
</tr>
<tr>
<td>MO</td>
<td>University of Missouri</td>
<td>MU</td>
<td>Columbia, MO</td>
<td>Columbia</td>
</tr>
<tr>
<td>AR</td>
<td>University of Arkansas</td>
<td>AR</td>
<td>Fayetteville, AR</td>
<td>Fayetteville</td>
</tr>
<tr>
<td>TX</td>
<td>The University of Texas</td>
<td>UT</td>
<td>Austin, TX</td>
<td>Austin</td>
</tr>
<tr>
<td>CA</td>
<td>University of California</td>
<td>UC</td>
<td>Los Angeles, CA</td>
<td>Los Angeles</td>
</tr>
<tr>
<td>WA</td>
<td>University of Washington</td>
<td>UW</td>
<td>Seattle, WA</td>
<td>Seattle</td>
</tr>
<tr>
<td>CO</td>
<td>Colorado State University</td>
<td>CSU</td>
<td>Boulder, CO</td>
<td>Boulder</td>
</tr>
<tr>
<td>IL</td>
<td>Illinois State University</td>
<td>ISU</td>
<td>Urbana, IL</td>
<td>Urbana</td>
</tr>
<tr>
<td>MN</td>
<td>University of Minnesota</td>
<td>UMN</td>
<td>Minneapolis, MN</td>
<td>Minneapolis</td>
</tr>
<tr>
<td>WI</td>
<td>University of Wisconsin</td>
<td>UW</td>
<td>Madison, WI</td>
<td>Madison</td>
</tr>
<tr>
<td>MO</td>
<td>University of Missouri</td>
<td>MU</td>
<td>Columbia, MO</td>
<td>Columbia</td>
</tr>
</tbody>
</table>

See page 1-31 for details on how to use this data.