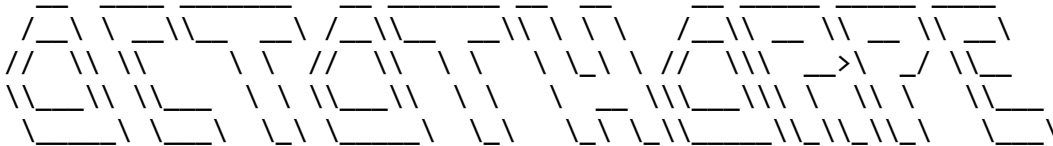


The Telecommunications Collage Vol. I

Miscellaneous Techniques for the Telecommunications Hobbyist

Written exclusively for



P R O D U C T I O N S

By: The Cruiser

The purpose of this text-file is to explain the ethics and purpose of phone phreaking and hacking to the ones that don't know or that think they do but really don't. Also I will report on a few odd developments in the hack and phreak worlds, so this file is by no means just reserved to the newcomers. But most of it, however, is on the basic level. In later volumes I will get into more in-depth subjects. For the beginner, I will not get into basic telephony, switching systems and explaining basics such as loops, divertors, etc., but for those that need that information I highly recommend reading BIOC Agent's gem of a series, "The Basics of Communications". Though the earliest ones date back to 1983, they are very informative and well written. At the end of this file I'll put a little bibliography with a list of text-files and books that are recommended reading. Now on to the rest of the file, which will be roughly divided into sections.

I. Elitism. (This is the only section devoted entirely to newcomers. Others can go ahead to section II).

It's funny listening to some of the new "phreaks" nowadays.

ALL NEW HACKERS/PHREAKS. . .LISTEN!

What hackers/phreaks do is illegal! Sort of like the mafia - if you turn

COLLAGE1.TXT

someone in you can expect to get hurt! So, for all you people out there who cannot handle it, I suggest that you had better stop right away before you get yourself in trouble. There's too many kids out there today who think that they're big shit because they can make long distance calls for free... WHOOPIE! A phreak is not a person that makes long distance calls for nothing. Get that through your heads! A phreak is a person that experiments with the phone company, and tries to manipulate it and see what it can do! It only curtails 20% of long distance calls. That 20% is the final chapter of the phreak, once they crack the Bell system they can make calls for nothing.
HOW CAN ANYONE READ THE LAST CHAPTER AND KNOW WHAT THE BOOK CONTAINS?

Phreaking is illegal and you can get busted for it. No, the FBI won't bust you for sending someone a \$2,000.00 phone bill, the FBI has nothing to do with that at all! And enough about MCI and tracing... 800 numbers always ANI! 950's are routed in a different way, otherwise they're the SAME as other prefixes! ANY number can trace, so there isn't one safe method or long distance company to make free calls. So if you are scared of getting caught, SIMPLY DO NOT DO IT! People who break into computer systems to crash and destroy them or use long distance codes for the mere sake of running up someone's bill should be caught. It's vandalism.

Also, a note about boxing. The blue box is the first and one of the few "boxes" [which is contradictory to the pirates and others that have a rainbow assortment of them], although I would also classify the black box as a "box". Others are just tools of the phone phreak. A beige box is nothing more than a lineman's handset, and a clear box is just a tone dialer. Also, boxing is not completely extinct, like some say. And YES, there ARE ways around ESS! One just has to look for them. Not everything one learns can be attained from a text-file. Phreaking is not a passive activity, one must go places, do things, and experiment. Although I am not saying that boxing is in it's prime, either. [I wasn't a phreak when boxing was in its prime, which was way back in the early 70's]. Phreaks still have blue boxes, some for sentimental reasons, and others still use them. A lot of the "boxes", such as the yellow, urine, lunch, super, cereal, plaid, brown, et. al., don't exist. They were "invented" by intelligent people for the plain idiots and "new breed" of what I call "c0mpyooter kidz" to toy with (and try to build and use!) Oh, and then there's boxes like the red box. The red box exists, but it's just a few of the tones in a blue box. So if you have a blue box, you also have a red box.

What else... Oh, yeah, something about codes. For your own safety, never use codes posted on a BBS. Who knows how many people are using it. And, contradictory to the pirate's favorite little saying, "There's safety in numbers," it's actually more dangerous to use a code posted around the nation. All you have to do it put your code hacker on one night, and if you get about 4 codes, that should last you two months if you use one code every two weeks, and don't give any to anyone.

II. Trashing

Trashing, if done correctly, can be a very profitable and enjoyable part of a phreak's activities. After trashing local Bell and AT&T sites for over two years, I've gained a bit of experience on the subject, and have a few fairly good guidelines for trashing:

1)First of all, you need a place to trash. The best places are your local central office, business office, AT&T service branch, or communications center. To find out where these are located, just open up the good ol' white pages to "American Telephone and Telegraph" or "Bell Systems" and you will find several local addresses. When you pick one out that you think will be profitable, jot down the address and take a few drives out there;one during a weekday business hour, one on a Sunday, and another at night. This will give you an idea of how heavily populated it is at certain times. Don't get out of the car during these surveillance trips, but just make a note of security, etc. Some telco installations keep their trash locked up, others have it guarded, but most of them just have a plain old dumpster. During these trips you also have to watch when the trash is collected, so that you can arrange a day when the trash will be at its peak.

2)Once you have a site picked out, and a good time and date to go, drive out with a friend or two. Sometimes it's better to park your car and walk when it is guarded, so you will have a smaller chance of being detected, but most of the time you can just drive right up. Always do it at night, Fridays, Saturdays and Sundays being the best. Once you are at the dumpster, grab all the bags and put them in the trunk. If you walked, then take them out and leave as soon as possible. Not only is this safer (no worry about getting caught by the cops) than going in the dumpster and sorting the trash there, but it assures you that you don't miss anything. And what's nice about telco trash is that the worst it gets is coffee grounds or an apple core, so you won't have to worry about smelly garbage.

3)Drive off to your house and sort it in your garage, backyard, or whatever. Have some trash bags nearby to put the real trash in. The good trash you can then keep, and dispose of the rest.

There are many good things you can find in telco trash. There are always abundances of printouts, from loop tests to miscellaneous reports. Depending on exactly what kind of building you trashed, you could find broken phones (the parts are very useful) to blank letterheads. I have never found a pad of unused Bell letterheads, but if you find one that is in good condition but written on, take it to your local printer and have them print you out two dozen copies in the same color, but to omit the part that was written on. If the printer questions you, just leave and go somewhere else. At my local printer, this cost me \$2.60. Letterheads and envelopes are very useful for scaring enemies (on occasion, friends too!), or for impressing phellow phreaks

COLLAGE1.TXT

when writing to them. In Bell trash you can also find notebooks and binders with the Bell logo. Once I trashed a computer store and found a binder with the Intel logo on it. It now sits next to my PC and I use it to keep my technical information.

III. Your Phriends at Bell!

There's a lot of phree presents AT&T has for you that's just as easy as a phone call away:

Ever want more than one phone book? Is yours old and tattered? You can get a White Pages, Yellow Pages, Business-to-Business Yellow Pages, or whatever suburb yellow/white pages you want just by asking! It's very simple, and perfectly legal - just open the cover of your current White Pages and get the number to your local Administrative Office. Give 'em a call and ask for whatever phone book you want, and they'll send it free of charge. Don't order more than 3 at a time, however.

A way to get Bell stationary without going trashing is to call Bell and ask for information on, for instance, WATS lines. You'll get a little pamphlet in the mail about WATS lines, plus a Bell memorandum slip saying something like, "George --- here's the information you requested on WATS lines". As before, take it to your printers', and have it copied without the writing.

Those manhole covers that you see on your street with the words "Bell System" on it have more in there than you think. If you can lift one up using a crowbar, go inside. Sometimes you might find a telephone handset, and if you're lucky, a Bell manual or two describing the wires lining the inside. But most of the time, that's just a phreak phairy tale. It's not that easy, but I worked out an easy method to get various manuals that WORKS: Ever see those little black lids on the corner of the block that says "Telephone" on it, and you open it up and there's a long wire in it? It's called a bridging head. Well go to one close to you, either if you have one or try one a few houses away. Take the lid off, and pitch it. Then call up repair service and say, "Hello, this is [insert the name of someone that lives near it, or bullshit a name], and I have a box at the corner of my house that contains phone wires. Well, I just looked outside and the lid is missing. I have a 6 year old daughter, and she plays outside a lot. I don't want her to get electrocuted or hurt, so could you please send someone out to replace the lid? My address is [fill in address here]." And in a while (they'll tell you the time), a bell lineman will drive up, open his truck and get out a replacement lid. When he's doing that, just reach in the truck and swipe something. But you have to be quick and accurate, and you can't be too choosy. While you're at it, you might as well get into a conversation with the guy. BSing with these people can sometimes yield good results.

Many of the Directory Assistance ops can easily be talked to. Although

COLLAGE1.TXT

they get a lot of calls (1000-1300 a day), they still will talk for a few minutes. The problem is that they don't have access to much. They can tell you if a number is unlisted or not, and that's about it. The CN/A operator can give you the name and address of a number. And, if done correctly, you can get some information from her. I hear that most CN/As are going to become a regular customer pay service in the near future, due to all the teens already abusing them. My CN/A (614) doesn't even give you the full address or name on most of the numbers, they just tell you the major city it's in (like for a 614 number they'll say "that's in Columbus", and for a 216 number they'll say "that's in Cleveland"), which doesn't help at all. For unlisted numbers they'll tell you that they have no record. Some CN/As are on Microfische (like mine), and that's what happens when you call them. The others are computerized but they ask for a pass code (two letters and two numerals). It won't be long before this once-valuable operator becomes useless.

IV. Exchange Scanning

The best way to find pbxes, loops, and other goodies is to manually scan for them. In the NPA-NXX-99XX numbers, there's a lot of Bell goodies, just waiting for you to explore them. Get a notebook for phreaking and make a chart for each prefix like this (thanks to BIOC Agent 003 for this method):

NPA-NXX-99XX Scan

99x	x>	0	1	2	3	4	5	6	7	8	9
990											
991											
992											
993											
994											
995											
996											
997											
998											
999											

[illegible]

```
R = ring [try again later]
B = busy [ " " " "]
R1= recording 1 [make a list of all that you come across, R1, R2, R3, etc.]
D = dial tone
O = intercept operator
S = sweep tone
T = tone [tone at lower number + ignore it's a loop]
I = ignore [dead silence. at higher number, it's a loop]
V = voice number to telco
C = carrier [modem]
Q = strange tone/clicks/buzzing
M = voice mail system
N = SCC / Network port (MCI, Sprint, etc)
```

State	800 Prefix	NPA served
-----	-----	-----
Alabama	633	<205>
Alaska	544	<907>
Arizona	528	<602>
Arkansas	643	<501>
California	227	<415>

COLLAGE1.TXT

	421	<213>	
	423	<213>	
	854	<714>	
	824	<916>	
	538	<408>	
	235	<805>	
	344	<209>	
	358	<707>	
Colorado	525	<303>	
	255	<303>	
Connecticut	243	<203>	
Delaware	441	<302>	
District of Columbia	424	<202>	
	368	<202>	For high volume traffic
Florida	327	<305>	
	237	<813>	
	874	<904>	
Georgia	841	<912>	
	*241	<404>	
	554	<404>	
Hawaii	367	<808>	
Idaho	*635	<208>	
Illinois	621	<312>	
	323	<312>	
	637	<217>	
	435	<815>	
	447	<309>	
	851	<618>	
Indiana	428	<317>	
	457	<812>	
	348	<219>	
Iowa	553	<319>	
	*247	<515>	
	831	<712>	
Kansas	835	<316>	
	255	<913>	
Kentucky	626	<502>	
	354	<606>	
Louisiana	535	<504>	
	551	<318>	
Maine	341	<207>	
Maryland	368	<301>	
Massachusetts	343	<617>	
	225	<617>	
	628	<413>	
Michigan	253	<616>	
	521	<313>	
	338	<906>	

COLLAGE1.TXT

	517	<248>	
Minnesota	328	<612>	
	533	<507>	
	*346	<218>	
Mississippi	647	<601>	
Missouri	821	<816>	
	325	<314>	
	641	<417>	
Montana	*548*	<406>	
Nebraska	228	<402>	
	445	<308>	
Nevada	*634	<702>	Las Vegas
	648	<702>	Reno
New Hampshire	258	<603>	
New Jersey	257	<609>	
New Mexico	545	<505>	
New York	223	<212>	
	847	<607>	
	221	<212>	
	431	<914>	
	828	<716>	
	645	<516>	
	448	<315>	
	833	<518>	
North Carolina	334	<919>	
	438	<704>	
North Dakota	*437	<701>	
Ohio	321	<216>	
	543	<513>	
	537	<419>	
	848	<614>	
Oklahoma	654	<405>	
	331	<918>	
Oregon	*547*	<503>	
Pennsylvania	523	<215>	
	345	<215>	
	458	<814>	
	245	<412>	
	233	<717>	
Puerto Rico	468	<809>	
Rhode Island	556	<401>	
South Carolina	*845*	<803>	
South Dakota	*843*	<605>	
Tennessee	251	<615>	
	238	<901>	
Texas	527	<214>	
	433	<817>	
	531	<512>	

COLLAGE1.TXT

	231	<713>
	351	<915>
	858	<806>
Utah	453	<801>
Vermont	*451	<802>
Virginia	446	<804>
	368	Arlington - (for D.C.)
	336	<703>
Virgin Islands	524	<809>
Washington	426	<206>
	541	<509>
West Virginia	624	<304>
Wisconsin	*356	<608>
	558	<414>
Wyoming	443	<307>

Another area to scan are the <NPA>/NXX-4499 numbers. These will connect you to a loud annoying busy signal. But the neat part about it is that if anyone else calls it while you're on, you can talk. Many people (I've seen it where they've gotten 20) can be on it at the same time. And the more people on the line, the quieter the busy signal gets. Although the busy signal is annoying, it's good because you don't get charged for busy signals so you can call it direct. Two working numbers are <603>/353-4499 and <205>/356-4499. There are a lot of these, at least one in every area code.

V. Closing Notes

This ends the first in a series, "The Telecommunications Collage". This one was aimed more at the newer phreaks, but more information will be in issue number two, including Bell computers, answering machine/VRS hacking, radio hacking, and other topics. This file was written on various dates between March 17th, 1987 to April 26th, 1987 [as if you really cared, huh?]. Here I'm listing some suggested reading like I promised you at the beginning of the publication. Use this material well, and remember, knowledge is power! [as I quote Scan Man]

Suggested Reading
--

BIOG Agent 003's Basics of Communications Series (old, somewhat outdated, but
 still good for beginners.)
 Illustrated Encyclopedic Dictionary of Electronics, by John Douglas-Young

COLLAGE1.TXT

Phrack Publications

The Legion of Doom/Hackers Technical Journal

The Shockwave Rider, by John Brunner

Understanding Telephone Electronics, Radio Shack Manual 62-1388

Downloaded From P-80 Systems 304-744-2253