Basics to know before doing anything, essential to your continuing career as one of the elite in the country... This article, "The introduction to the world of hacking." is meant to help you by telling you how not to get caught, what not to do on a computer system, what type of equipment should I know about now, and just a little on the history, past present future, of the hacker.

Welcome to the world of hacking! We, the people who live outside of the normal rules, and have been scorned and even arrested by those from the 'civilized world', are becoming scarcer every day. This is due to the greater fear of what a good hacker (skill wise, no moral judgments here) can do nowadays, thus causing anti- hacker sentiment in the masses. Also, few hackers seem to actually know about the computer systems they hack, or what equipment they will run into on the front end, or what they could do wrong on a system to alert the 'higher' authorities who monitor the system. This article is intended to tell you about some things not to do, even before you get on the system. I will tell you about the new wave of front end security devices that are beginning to be used on computers. I will attempt to instill in you a second identity, to be brought up at time of great need, to pull you out of trouble. And, by the way, I take no, repeat, no, responsibility for what we say in this and the forthcoming articles.

Enough of the bullshit, on to the fun: after logging on your favorite bbs, you see on the high access board a phone number! It says it's a great system to "fuck around with!" This may be true, but how many other people are going to call the same number? So: try to avoid calling a number given to the public. This is because there are at least every other user calling, and how many other boards will that number spread to? If you call a number far, far away, and you plan on going through an extender or a re-seller, don't keep calling the same access number (I.E. As you would if you had a hacker running), this looks very suspicious and can make life miserable when the phone bill comes in the mail. Most cities have a variety of access numbers and services, so use as many as you can. Never trust a change in the system... The 414's, the assholes, were caught for this reason: when one of them connected to the system, there was nothing good there. The next time, there was a trek game stuck right in their way! They proceeded to play said game for two, say two and a half hours, while telenet was tracing them! Nice job, don't you think? If anything looks suspicious, drop the line immediately!! As in, yesterday!! The point we're trying to get across is: if you use a little common sense, you won't get busted. Let the little kids who aren't smart enough to recognize a trap get busted, it will take the heat off of the real hackers. Now, let's say you get on a computer

system... It looks great, checks out, everything seems fine. OK, now is when it gets more dangerous. You have to know the computer system to know what not to do. Basically, keep away from any command something, copy a new file into the account, or whatever! Always leave the account in the same status you logged in with. Change *nothing*... If it isn't an account with priv's, then don't try any commands that require them! All, yes all, systems are going to be keeping log files of what users are doing, and that will show up. It is just like dropping a trouble-card in an ESS system, after sending that nice operator a pretty tone. Spend no excessive amounts of time on the account in one stretch. Keep your calling to the very late night if possible, or during business hours (believe it or not!). It so happens that there are more users on during business hours, and it is very difficult to read a log file with 60 users doing many commands every minute. Try to avoid systems where everyone knows each other, don't try to bluff. And above all: never act like you own the system, or are the best there is. They always grab the people who's heads swell... There is some very interesting front end equipment around nowadays, but first let's define terms... By front end, we mean any device that you must pass through to get at the real computer. There are devices that are made to defeat hacker programs, and just plain old multiplexers. To defeat hacker programs, there are now devices that pick up the phone and just sit there... This means that your device gets no carrier, thus you think there isn't a computer on the other end. The only way around it is to detect when it was picked up. If it picks up after the same number ring, then you know it is a hacker-defeater. These devices take a multi-digit code to let you into the system. Some are, in fact, quite sophisticated to the point where it will also limit the user name's down, so only one name or set of names can be valid logins after they input the code... Other devices input a number code, and then they dial back a pre-programmed number for that code. These systems are best to leave alone, because they know someone is playing with their phone. You may think "but I'll just reprogram the dial-back." Think again, how stupid that is... Then they have your number, or a test loop if you were just a little smarter. If it's your number, they have your balls (if male...), if its a loop, then you are screwed again, since those loops

are *monitored*. As for multiplexers... What a plexer is supposed to do is this:

The system can accept multiple users. We have to time share, so we'll let the front-end processor do it... Well, this is what a multiplexer does. Usually they will ask for something like "enter class" or "line:". Usually it is programmed for a double digit number, or a four to five letter word. There are usually a few sets of numbers it accepts, but those numbers also set your 300/1200/2400 baud data type. These multiplexers are inconvenient at best, so not to worry. A little about the history of hacking: hacking, by my definition, means a great knowledge of some special area. Doctors and lawyers are hackers of a sort, by this definition. But most often, it is being used in the computer context, and thus we have a definition of "anyone who has a great amount of computer or telecommunications knowledge." You are not a hacker because you have a list of codes... Hacking, by my definition, has then been around only about 15 years. It started, where else but, MIT and colleges where they had computer science or electrical engineering departments. Hackers have created some of the best computer languages, the most awesome operating systems, and even gone on to make millions. Hacking used to have a good name, when we could honestly say "we know what we are doing". Now it means (in the public eye): the 414's, Ron Austin, the NASA hackers, the arpanet hackers... All the people who have been caught, have done damage, and are now going to have to face fines and sentences. Thus we come past the moralistic crap, and to our purpose: educate the hacker community, return to the days when people actually knew something...

63. Hacking DEC's   by The Jolly Roger

In this article you will learn how to log in to dec's, logging out, and all the fun stuff to do in-between. All of this information is based on a standard dec system. Since there are dec systems 10 and 20, and I favor, the dec 20, there will be more info on them in this article. It just so happens that the dec 20 is also the more common of the two, and is used by much more interesting people (if you know what I mean...) OK, the first thing you want to do when you are receiving carrier from a dec system is to find out the format of login names. You can do this by looking at who is on the system.

Dec=> ` (the 'exec' level prompt)