E · U · A

Volume One, Issue 2 **June 26th, 1998**

The BBS'ers guide to the arts of Hacking, Phreaking, Cypherpunks, Net-surfing, bad-assed type of mag that give people the "inside information." Are you interested? Do you want to know more? The Electronic Underground Affiliations sole purpose is to provide current information about network security, Internet news, information about the local scene and how you fit into it all.

"The reason 'hackers' seek out new knowledge is not for personal profit, but for general knowledge."

Inside this Edition...

There's a storm brewing on the Internet are you ready for it?

"*Aut Hack Vincere Aut Mori*"

Who Is Kevin Mitnick? Keving Mitnick was arrested on computer hacking charges in February 1995. Still awaiting trial, he has been imprisoned for over three years since his arrest, has been denied bail, and repeatedly denied the right to have his defense analyze the evidence the government holds against him. Despite the lack of any allegations of physical harm or profit motives by Mitnick, he has not been granted bail. Individuals accused of crimes as serious as murder, rape, and drug trafficking are often granted bail, allowing them to remain free from incarceration prior to trial if they can provide reasonable assurance that they will appear for the trial. Despite the concept of "innocent-until-proven-guilty," his status in "pre-trial detention" forbids him access to privileges accorded to other inmates. He is forbidden visitors other than attorneys and blood-relatives.

E.U.A. Submissions

e-mail: archive_@hotmail.com

Subject: article

Format: plain ascii text/PGP-encrypted

Articles, letters, submissions must be submitted prior to the 15th of each month

ELECTRONIC UNDERGROUND AFFILIATION

Recent Rulings on Mitnick's Case:

The Ninth Circuit Court turned down Kevin's request for bail. They said he was a "flight risk". Just where do they think he would go? What happened to our open-minded fair Ninth Circuit? I have never been one to be paranoid about conspiracies, but something is very wrong with this picture. Please write to your congressmen. Write to reporters. Some of you have asked where Kevin is. Metropolitan Detention Center is in a highrise building in downtown Los Angeles. This is a location where prisoners are supposed to be "detained" for a short time while they await sentencing or trials. The Bureau of Prisons states that prisoners are to be incarcerated at MDC for no longer than one year. Kevin has been there for three years, three months. By the time they go to trial, Kevin will have been in this "hole" for more than four years. Those government gestapo forces are inflicting cruel and unusual punishment on Kevin. If there is any truth behind, "what goes around, comes around" .....our government will pay a very high price for what they have done. And it couldn't happen to a more deserving bunch.

FREE KEVIN MITNICK !

Looking for *new* hardware?
Have equipment that you would *trade*?

Looking for a "*hard to get*" piece of gear
Check out the Hardware Exchange
available on the Information Attic

"*You'd be suprised as to what we can get.*"

Kevin Mitnick page 1Despite his need to prepare for his trial, his access to the law library is limited to five and one-half hours per week. This is absurd considering the estimated 200 million pages of documentation that must be examined prior to trial. Mitnick's case should be of concern to not only computer users, but to everyone. If the prosecution succeeds in their efforts, the Mitnick case could be used as a precedent to stifle the rights of other accused hackers. Is this what future holds for those accused of computer crime? Perhaps. The area of -computer law and computer crime is still in its infancy. The line between permissible and illegal computer usage is often unclear and blurred at best. Current wire-fraud and mail-fraud statutes encompass wide areas of common behavior. Similarly, computer crime statues are broadly worded and criminalize behavior that many individuals may commit without ever realizing such actions are illegal. It is then within the discretion of the federal prosecutors as to whether to seek an indictment and arrest. When the limits of permissible activity are so unclear, does it make sense to hold individuals who have merely been accused of such behavior *WITHOUT BAIL FOR YEARS* before trial? The federal government is apparently using the Mitnick case to instill fear in the minds of computer users and to discourage activities they consider to be "hacking." The government apparently wishes to encourage individuals who have merely been accused of hacking-related offenses to plead guilty, rather than face lengthy pre-trial detention without benefit of bail. Kevin Mitnick's case will be ground breaking. It will set the precedent and tone of future government behavior in all new areas of law. When proscribed behaviors are unclear should the government draft broad prohibitions, investigate, arrest, indict, hold without bail, and then clarify standards of behavior years later at the trial? *Article submitted by*

Archive_@hotmail.com

ELECTRONIC UNDERGROUND AFFILIATION

The Ethics of Hacking written by Dissident

I went up to a college this summer to look around, see if it was where I wanted to go and what-not. The guide asked me about my interests, and when I said computers, he started asking me about what systems I had, etc. And when all that was done, the first thing he asked me was "Are you a hacker?"

Well, that question has been bugging me ever since. Just what exactly is a hacker? A REAL hacker?

For those who don't know better, the news media (and even comic strips) have blown it way out of proportion... A hacker, by wrong-definition, can be anything from a computer-user to someone who destroys everything they can get their evil terminals into. And the idiotic schmucks of the world who get a Commodore Vic-20 and a 300 baud modem (heh, and a tape drive!) for Christmas haven't helped hackers' reputations a damn bit. They somehow get access to a really cool system and find some files on hacking... Or maybe a friendly but not-too-cautious
hacker helps the loser out, gives him a few numbers, etc. The schmuck gets onto a system somewhere, lucks up and gets in to some really cool information
or programs, and deletes them. Or some of the more greedy ones capture it, delete it, and try to sell it to Libya or something. Who gets the blame?

The true hackers...that's who. So what is a true hacker? Firstly, some people may not think I am entirely qualified to say, mainly because I don't consider myself a hacker yet. I'm still learning the ropes about it, but I think I have a pretty damn good idea of what a true hacker is. If I'm wrong, let one correct me...

True hackers are intelligent, they have to be. Either they do really great in school because they have nothing better to do, or they don't do so good because school is terribly boring. And the ones who are bored aren't that way because they don't give a shit about learning anything. A true hacker wants to know everything. They're bored because schools teach the same dull things over and over and over, nothing new, nothing challenging.

True hackers are curious and patient. If you aren't, how can you work so very hard hacking away at a single system for even one small PEEK at what
may be on it? A true hacker DOESN'T get into the system to kill everything or to sell what he gets to someone else. True hackers want to learn, or want to satisfy their curiosity, that's why they get into the system. To search around inside of a place they've never been, to explore all the little nooks and crannies of a world so unlike the boring cess-pool we live in. Why destroy something and take away the pleasure you had from someone else? Why bring down the whole world on the few true hackers who aren't cruising the phone lines with malicious intent?

True hackers are disgusted at the way things are in this world. All the wonderful technology of the world costs three arms and four legs to get these days. It costs a fortune to call up a board in an adjoining state! So why pay for it? To borrow something from a file I will name later, why pay for what could be "dirt cheap if it wasn't run by profiteering gluttons"? Why be forced, due to lack of the hellacious cash flow it would require to call all the great places, to stay around a bunch of schmuck losers in your home town? Calling out and entering a system you've never seen before are two of the most exhilarating experiences known to man, but it is a pleasure that could not be enjoyed were it not for the ability to phreak...

ELECTRONIC UNDERGROUND AFFILIATION

The Ethics of Hacking True hackers are quiet. I don't mean they talk at about .5 dB, I mean they keep their mouths shut and don't brag. The number one killer of those the media would have us call hackers is bragging. You tell a friend,"or you run your mouth on a board, and sooner or later people in power will find out what you did, who you are, and you're gone...

I honestly don't know what purpose this file will serve, maybe someone somewhere will read it, and know the truth about hackers. Not the lies that the ignorant spread. To the true hackers out there, I hope I am portraying what you are in this file... If I am not, then I at least am saying what I think a true hacker should be. And to those wanna-be's out there who like the label of "HACKER" being tacked onto them, grow up, would ya?

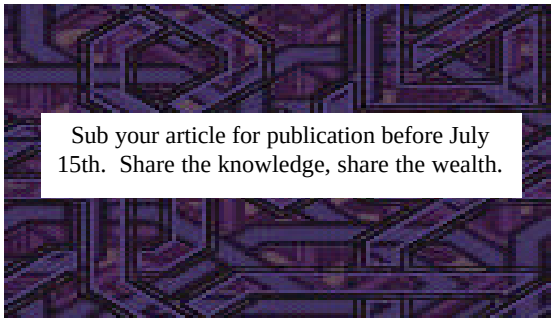
Oh yeah, the file I quoted from... It has been done (at least) two times. "The Hacker's Manifesto" or "Conscience of a Hacker" are the two names I've seen it given. (A file by itself, and part of an issue of Phrack) Either way, it was written by The Mentor, and it is absolutely the best thing ever written on the subject of hackers. Read it, it could change your life.
Spread it around, but don't change anything please. . .

H/P/A/V/Ix Oriented BBS Listing

Apoc2k	847 831 0484
Moo'n'Oink	847 256 5928
Information Attic	910 347 2582
The Centre	207 490 2158
Taipan Enigma's &TOSE	510 935 5845

Do you know of a BBS that you want to add into the next issue?

E-mail me and let me know! ! !



Some Social Engineering Tips

Be professional: You don't want someone to not buy what you're doing. You're trying to create an illusion. You're trying to be believable. Be calm: look like you belong there.

Know your mark: Know your enemy. Know exactly how they will react before they do. Do not fool a superior scammer: Trying to outscam an observant or smarter person will end in disaster.

Plan your escape from your scam: Lets say someone is suspicious. Don't burn your bridges and walk away. Save the source.

Try to be a woman: It's proven that women are more trusted over the phone. Use that to an advantage. Get a woman's help if needed. It's even better if you're actually a woman (a rarity in our biz).

Watermarks: Learn to make 'em. They are invaluable for a mail scam.

Business cards and fake names: Use them for professional things. Manipulate the less fortunate and the stupid

Use a team if you have to: Don't be arrogant and overly proud. If you need help, get it

ELECTRONIC UNDERGROUND AFFILIATION

The Illinois Computer Crime Prevention law, adopted in 1981, and amended in 1987.

This is article 16D of the "Criminal Code of 1961."

16D-1. SHORT TITLE

Section 16D-1. Short title. This Article shall be known and may be cited as the "Computer Crime Prevention Law."

16D-2. DEFINITIONS

Section 16D-2. Definitions. As used in this Article, unless the context otherwise indicates:

(a) "*Computer*" means a device that accepts, processes, stores, retrieves or outputs data, and includes but is not limited to auxiliary storage and telecommunications devices connected to computers.
(b) "*Computer program*" or "*program*" means a series of coded instructions or statements in a form acceptable to a computer which causes the computer to process data and supply the results of the data processing.

(c) "*Data*" means a representation of information, knowledge, facts, concepts or instructions, including program documentation, which is prepared in a formalized manner and is stored or processed in or transmitted by a computer. Data shall be considered property and may be in any form including but not limited to printouts, magnetic or optical storage media, punch
cards or data stored internally in the memory of the computer.

(d) In addition to its meaning as defined in Section 15-1 of this Code, "*property*" means: (1) electronic impulses; (2) electronically produced data; (3) confidential, copyrighted or proprietary information; (4) private identification codes or numbers which permit access to a computer by authorized computer users or generate billings to consumers for purchase of goods and services, including but not limited to credit card transaction and telecommunications services or permit electronic fund transactions; (5) software or program in either machine or human readable form; or (6) any other tangible or intangible item relating to a computer or any part thereof.

(e) "*Access*" means to use, instruct, communicate with, store data in, retrieve o intercept data from, or otherwise utilize any services of a computer.

(f) "*Services*" includes but is not limited to computer time, data manipulation or storage functions.

(g) "*Vital services or operations*" means those services or operation required to provide, operate, maintain, and repair network cabling, transmission, distribution, or computer facilities necessary to ensure or protect the public health, safety, or welfare. Public health, safety, or welfare include, but are not limited to, services provided by medical personnel or institutions, fire departments, emergency services agencies, national defense contractors, armed forces or militia personnel,
private and public utility companies or law enforcement agencies.

16D-3. COMPUTER TAMPERING

Section 16D-3. Computer Tampering. (a) A person commits the offense of computer tampering when he knowingly and without the authorization of a computer's owner, as defined in Section 15-2 of this Code, or in excess of the authority granted to him:

(1) Access or cause to be accessed a computer or any part thereof, or a program or data;

(2) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and obtains data or services;

(3) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and damages or destroys the

computer or alters, deletes or removes a computer program or data;

(4) Inserts or attempt to insert a "program" into a computer or computer program knowing or having reason to believe that such "program" contains information or commands that will or may damage or destroy that computer, or any other computer subsequently accessing or being accessed by that computer, or that will or may alter, delete or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer, or that will or may cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such "program."

(b) Sentence.

(1) A person who commits the offense of computer tampering as set forth in subsection (a)(1) of this Section shall be guilty of a Class B misdemeanor.

(2) A person who commits the offense of computer tampering as set forth in subsection (a)(2) of this Section shall be guilty of a Class A misdemeanor and a Class 4 felony for the second or subsequent offense.

(3) A person who commits the offense of computer tampering as set forth in subsection (a)(3) or subsection (a)(4) of this Section shall be guilty of a Class 4 felony and a Class 3 felony for the second or subsequent offense.

(c) Whoever suffers loss by reason of a violation of subsection (a)(4) of this Section may, in a civil action against the violator, obtain appropriate relief. In a civil action under this Section, the Court ma award to the prevailing party reasonable attorney's fees and other litigation expenses.

16D-4. AGGRAVATE COMPUTER TAMPERING

Section 16 D-4. Aggravated Computer Tampering. (A) A person commits aggravated computer tampering when he commits the offense of computer tampering as set forth in subsection (a)(3) of Section 16D-3 and he knowingly:

(1) causes disruption of or interference with vital services or operations of State or local government or a public utility; or

(2) creates a strong probability of death or great bodily harm to one or more individuals.

(b) Sentence. (1) A person who commits the offense of aggravated computer tampering as set forth in subsection (a)(1) of this Section shall be guilty of a Class 3 felony.

(2) A person who commits the offense of aggravated computer tampering as set forth in subsection(a)(2) of this Section shall be guilty of Class 2 felony.

16D-5. COMPUTER FRAUD

Section 16D-5. Computer Fraud. (a) A person commits the offense of computer fraud when he knowingly:

(1) Accesses or causes to be accessed a computer or any part thereof, or alters, deletes, or removes any program or data contained therein, in connection with any scheme , artifice to
defraud, or as part of a deception;

(2) Obtains use of, damages, or destroys a computer or any part thereof, or alters, deletes, or removes any program or data contained therein, in connection with any scheme, artifice to
defraud, or as part of a deception; or

(3) Accesses or caused to be accessed a computer or any part thereof, or a program or data, and obtains money or control over any such money, property, or services of another in connection
with any scheme, artifice to defraud, or as part of a deception.

(b) Sentence. (1) A person who commits the offense of computer fraud as set forth in subsection (a)(1) of this Section shall be guilty of a Class 4 felony.

(2) A person who commits the offenses of computer fraud as set forth in subsection (a)(2) of this Section shall be guilty of a Class 3 felony.

(3) A person who commits the offenses of computer fraud as set forth in subsection (a)(3) of this Section shall:

(i) be guilty of a Class 4 felony if the value of the money, property or services is $ 1,000 or less; or

(ii) be guilty of a Class 3 felony if the value of the money, property or services is more than $1,000 but less than $ 50,000; or

(iii) be guilty of a Class 2 felony if the value of the money, property or services is $ 50,000 or more.

16D-6. FORFEITURE

Section 16D-6. Forfeiture. 1. Any person who commits the offense of computer fraud as set forth in Section 16D-5 shall forfeit, according to the provisions of this Section, any monies, profits or proceeds, and any interest or property which the sentencing court determines he has acquired or maintained, directly or indirectly, in whole or in part, as a result of such offense. Such
person shall also forfeit any interest in, security, claim against, or contractual right of any kind which affords him a source of influence over any enterprise which he has established, operated, controlled, conducted or participated in conducting, where his relationship to or connection with any such thing or activity directly or indirectly, in whole or in part, is traceable to any item or benefit which he has obtained or acquire through computer fraud.

Proceedings instituted pursuant to this Section shall be subject to and conducted in accordance with the following procedures:

(a) The sentencing court shall, upon petition by the prosecuting agency, whether it is the Attorney General or a State's Attorney, at any time following sentencing, conduct a hearing to determine whether any property or property interest is subject to forfeiture under this Section. At the forfeiture hearing the People of the State of Illinois shall heave the burden establishing, by a
preponderance of the evidence, that the property or property interests are subject to such forfeiture.

(b) In any action brought by the People of the State of Illinois under this Section, the circuit courts of Illinois shall jurisdiction to enter such restraining orders, injunctions or prohibitions, or take such other action in connection with real, personal, or mixed property or other interest subject to forfeiture, as they shall consider proper.

(c) In any action brought by the People of the State of Illinois under this Section, wherein any restraining order, injunction or prohibition or any other action in connection with any property or interest subject to forfeiture under this Section is sought, the circuit court presiding over there trial of the person or persons charge with computer fraud shall first determine whether there is probable cause to believe that the person or persons so charged have committed the offense of computer fraud and whether the property or interest is subject to forfeiture pursuant to this Section. In order to make this determination, prior to entering any such order, the court shall conduct a hearing without a jury, where the People shall establish: (1) probable cause that the person or person so charged have committed the offense of computer fraud, and (2) probable cause that nay property or interest may be subject to forfeiture pursuant to this Section.

Remember privacy is a right! Don't allow your privacy to be taken, make it a part of your everyday life. E.U.A. staff endorses the use of PGP.

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP for Personal Privacy 5.0

mQCNAzREUqUAAAEEAKJFFJOXdfzrNKLFWqazNGab7BDorQy9nEXgr+1cJc2BveGO
VvjOWbVcrbzg29RrDPVuYWjzVM/ZOkUdHanRhz7F6XVRCT0HuVa0legiondwOlCf
MUwmEUKjjGMu34tc7gPS7B+S0rLuElsFFSqTXoQHEpuipZ+QXAPEUJI/rUJVAAUR
tCVhcmNoaXZlIDxhcmNoaXZlLmluZm8uYXR0aWNAanVuby5jb20+iQCVAwUQNERT
awPEUJI/rUJVAQG5OQP7BdLdrZty2hwa3Mo9ZqMMwYXpv7/zChxl4dV17IinmjXv
0Nr51YGPl3VKwywuMgC4PqJR/4001lY4taDnM1YNb2kqq4OgEFuwTEbgpV/MBAsm
7g8z61QiU96WmVOdA+WuFEKO0g69Yak+Jlstn7ErbNbWj3JQ8G/9fnIefUKci9SJ
AD8DBRA0gMFiDdWMgJZc8rERAr0rAKCFpTrS3BC5nB9X91RTpM7ndBBaZQCg4j6m
kLesV7HOjClExHbRqArT+88=
=9ebu
-----END PGP PUBLIC KEY BLOCK-----

E.U.A.
Electronic Underground Affiliation

For more information about the E.U.A., dial 847.578.5437, the Information Attic is aimed at setting a new standard in the Free Exchange of information and ideas.

Electronic Underground Affiliation

Idea:	The Free Exchange of Information and Knowledge.
Purpose:	To Ensure that Information and Knowledge are available to anyone seeking.
Goal:	To enlist the assistance, wisdom, knowledge and information of as many users as possible.
Ethic:	Unlike society, the EUA, will not be hindered by the social stigmas of our day. We will not discriminate others on the basis of: 1) Sex, 2) Race, 3) Religious Beliefs, 4) Affiliation, 5) Physical Impairments

How to Join: Forward the following to archive_@hotmail.com

Handle:	E-mail address (SysOp's Use Only):	Do you run a BBS [Y,N]:
If Yes, #:	What BBS(s) do you Frequent (at least two):	City:
State:	What is your profession?	What is your computer specialty?

Why should you be allowed access to the Information Attic/EUA?
What special skills, information or knowledge do you feel you could offer the other users on the Information Attic/EAU?

EUA Staff and Assistants

Beta Publisher & Editor	Archive
Midwestern Digital Distribution	Highlander
Pacific Northwester Digital Distribution	PhrackWolf
Canadian Digital Distribution	Zarkov
Australian Digital Distribution	Fs0
Web & HTML Publishing	Aurellia
	Belladonna

Article Submissions and Assistant

Who is Kevin Mitnick
Jump0 out of Northern NC
Recent Rulings
2600 WebPublications
The Ethics of Hacking
by Dissident
The Illinois Computer Crime Bill
acquired by Archive