THE GUIDE

To (mostly) HARMLESS

HACKING

#Contents of Volume 4:

Guide to (mostly) Harmless Hacking
Vol. 4: Information Warfare Series
No. 1: Hacker Wars: Fighting the Cybernazis

There is a war underway in cyberspace. It is a war between the forces of repression and those of us who treasure freedom. On the side of repression are governments who fear the untrammeled freedom of speech that is today's Internet -- and several bands of computer criminals who have the nerve to call themselves hackers.

I prefer to call them cybernazis. They are the spiritual descendants of the Nazis of the Germany of the 1930s, who burned books in their campaign to keep the German people ignorant.

The tactics of today's cybernazis are to shut down people's email accounts, deface Web pages, and to use terror tactics to get people kicked of their Internet service providers. In some cases cybernazis also target their victims with massive credit card fraud, death threats, and worse.

So far, the cybernazis have been far more successful than governments in shutting down Web sites with which they disagree, blocking email, and getting people whose ideas they dislike kicked off Internet service providers.

It's a war that has targeted this Happy Hacker email list ever since we started it in August 1996. The cybernazis have felt we merit a wide range of attacks, not only digital but including blackmail and threats against those who have been courageous enough to be part of Happy Hacker.

The most serious battle in these wars took place Oct. 4-21, 1997. It targeted Bronc Buster. During the course of this battle, jericho and Modify sent me many email messages that made it clear that Bronc was being hit because of his high quality Web site (hope you can find it still up at http://showdown.org) and his association with Happy Hacker.

This war escalated beyond an initial spate of forgeries beginning Oct. 4, 1997 that attempted to make it look like Bronc was a self-confessed pedophile, into scorched-core warfare that shut down the

Succeed.net ISP repeatedly. They attacked Succeed.net because it was providing Bronc with a shell account.

I helped muster both the FBI and volunteer technical help from an Internet backbone provider to aid Succeed.net in its struggle against these vindictive computer criminals. If you, too, get hit by the cybernazis, too, tell me about it. I will be delighted to help you fight them.

****

I don't want to get sued disclaimer: Just because jericho and Modify acted as spokesmen for the attackers, and in the case of jericho claimed considerable knowledge of technical details of the attacks, does not mean they are guilty of anything. Nosirree. I am not saying they did it.

****

So, do you want to join us in our battle against those cybernazis, against those who are trying to wipe out freedom on the Internet? Want to enlist in the good guy side of information warfare? One way is to learn and practice defensive skills against hacker war criminals.

In this GTMHH No.1 of the Information Warfare Volume we will cover hacker war only. But an understanding of hacker war will prepare you for No. 2, which will help you protect yourself from far broader attacks which can even lead to your 'digital death," and No. 3, which will lay the foundation for becoming an international information warfare fighter.

What Exactly Are Hacker Wars?

Hacker wars are attempts to damage people or organizations using cyberspace. There are several types of hacker war tactics. In this Guide we will discuss some of the more common attacks.

Web Page Hacking

Lots of people ask me, "How do I hack a Web page?" Alas, gentle reader, the first step in this process ought to be physiologically impossible and unsuitable for description in a family publication.

The typical Web page hack begins with getting write permission to the hypertext files on the Web server that has been targeted. Amazingly, some Web sites accidentally offer write permission to anyone (world writable)! If so, all the hacker warrior need do is create a bogus Web page, give it the same name as the desired page on the Web site to be hit, and then transfer it via ftp.

Otherwise it is usually necessary to first break into the Web server computer and gain root or administrative control.

Hacked web pages usually consist of dirty pictures and bad language. I have hunted down many hacked Web sites. Wise political analysis, witty repartee and trenchant satire have been absent from every one I have ever seen -- with the single exception of one hack in Indonesia by the East Timor freedom fighter group. Perhaps because they risked their lives to have their say, they made their hack count.

But maybe my standards are too high. Judge for yourself. Parental discretion and antinausea medicine advised. Collections of hacked Web pages may be found at

http://www.skeeve.net/
http://www.2600.com/hacked_pages

However, even if someone's cause is good and their commentary trenchant, messing up Web sites is a pitiful way to get across a message. They are quickly fixed. One has to hack a really famous Web site to make it into an archive.

If you believe in freedom enough to respect the integrity of other people's Web sites, and are serious about making a political statement on the Web, the legal and effective way is to get a domain name that is so similar to the site you oppose that lots of people will go there by accident. For example, http://clinton96.org was hilarious, clean, effective, and legal. http://dole96.org was also taken by parody makers. They are both down now. But they were widely reported. Many political sites linked to them!

To get your web spoof domain name, go to http://internic.net. You will save a lot of money by purchasing it directly from them instead of through an intermediary. In fact, all you need to do is promise to buy a domain name. If you get tired of your parody Web site before you pay for it, people have told me they have just given the name back to Internic and no one demanded payment.

****

You can get punched in the nose by a giant corporation warning: If you get a parody domain name so you can put up a Web site that makes fun of a big corporation, even though you are not breaking the law, you may get sued. Even if you win the lawsuit, you could spend a lot of money in self defense. But you may be able to get lots of good publicity by alerting reporters to your plight before taking down your Web site. So in the end, especially if you get sued, you may make your views known to even more people than if you had hacked their Web site.

****

If you want to keep your Web site from being attacked, I recommend using a company that does nothing but host Web pages. This makes it easier to avoid being hacked. This is because the more services an Internet

service provider offers, the more vulnerabilities it exposes. For example, my http://techbroker.com is hosted by a Silicon Graphics box that does nothing but run a Web server. My @techbroker.com email, by contrast, is hosted on a machine that does nothing but host a POP (post office protocol) server. For sending out email, I use yet another computer.

DOS Attacks

A second type of hacker war is denial of service (DOS)attacks. Because they harm many people other than the direct targets, DOS may well be the most serious type of hacker war.

Spammers are a favorite target of DOS warriors. Spammers also, if my sources are telling the truth, fight back. The weapon of choice on both sides is the mail bomb.

Recently (June-Oct. 1997), hackers fought a massive war against spammer kingdom Cyber Promotions, Inc. with the AGIS Internet backbone provider caught in the middle. Cyberpromo went to court to force AGIS to give it Internet access (AGIS eventually won and kicked off Cyberpromo). But in the meantime it was seriously hurt by a barrage of computer vandalism.

While the vandals who attacked AGIS probably think they have a good cause, they have been doing more damage than any hacker war in history, and harming a lot of innocent people and companies in the process.

According one source on the AGIS attacks, "The person who really did it 'owned' all of their machines, their routers, and everything else inbetween (sic)." So, although the attacks on AGIS apparently consisted of computer break-ins, the use of the break-ins was to deny service to users of AGIS.

****

Newbie note: An Internet backbone is a super high capacity communications network. It may include fiber optics and satellites and new protocols such as Asynchronous Transfer Mode. An outage in a backbone provider may affect millions of Internet users.
****

****
You can go to jail warning: Attacking an Internet backbone provider is an especially easy way to get a long, long stay in prison.
****

Other DOS attacks include the ICMP (Internet Control Message Protocol) attacks so familiar to IRC warriors; and an amazing range of attacks on Windows NT systems. http://www.dhp.com/~fyodor/ has a good list of these NT DOS vulnerabilities, while Bronc Buster's http://showdown.org is great for Unix DOS attacks. Please note: we are pointing these out so you can study them or test your own computer or computers that you have permission to test.
While Windows NT is in general harder for criminals to break into, it is generally much easier to carry out DOS attacks against them.

****
You can go to jail, get fired and/or get punched in the nose warning: DOS attacks in general are pathetically easy to launch but in some cases hard to defend against. So not only can one get into all sorts of trouble for DOS attacks -- people will also laugh at those who get caught at it. "Code kiddie! Lamer!"
****

Sniffing

Sniffing is observing the activity of one's victim on a network (usually the Internet). This can include grabbing passwords, reading email, and observing telnet sessions.

Sniffer programs can only be installed if one is root on that computer. But it isn't enough to make sure that your Internet host computers are free of sniffers. Your email, telnet, ftp, Web surfing -- and any passwords you may use -- may go through 20 or more computers on their way to a final destination. That's a lot of places where a sniffer might be installed. If you really, seriously don't want some cybernazi watching everything you do online, there are several solutions.

The Eudora Pro program will allow you to use the APOP protocol to protect your password when you download email. However, this will not protect the email itself from snoopers.

If you have a shell account, Secure Shell (ssh) from Datafellows will encrypt everything that passes between your home and shell account computers. You can also set up an encrypted tunnel from one computer on which you have a shell account to a second shell account on another computer -- if both are running Secure Shell.

You may download a free ssh server program for Unix at ftp://sunsite.unc.edu/pub/packages/security/ssh/ssh-1.2.20.tar.gz, or check out http://www.cs.hut.fi/ssh/#ftp-sites.

If you are a sysadmin or owner of an ISP, get ssh now! Within a few years, all ISPs that have a clue will require ssh logins to shell accounts.

For a client version that will run on your Windows, Mac or any version of Unix computer, see the DataFellows site at http://www.datafellows.com/. But remember, your shell account must be running the ssh server program in order for your Windows ssh client to work.

To get on the ssh discussion list, email majordomo@clinet.fi

with message
"subscribe ssh."
     But ssh, like APOP will not protect your email. The solution? Encryption.
PGP is popular and can be purchased at http://pgp.com. I recommend using the
RSA option. It is a stronger algorithm than the default Diffie-Hellman
offered by PGP.

****
Newbie note: Encryption is scrambling up a message so that it is very hard
for anyone to unscramble it unless they have the right key, in which case it
becomes easy to unscramble.
****

****
Evil genius tip: While the RSA algorithm is the best one known, an
encryption program may implement it in an insecure manner. Worst of all, RSA
depends upon the unprovable mathematical hypothesis that there is no
polynomial time bounded algorithm for factoring numbers. That's a good
reason to keep up on math news!
     The key plot element of the movie "Sneakers" was a fictional discovery of a fast algorithm to factor numbers. Way to go, Sneakers writer/producer Larry
Lasker!
****

****
You can go to jail warning: In many countries there are legal restrictions
on encryption. In the US, the International Traffic in Arms Regulations
forbids export of any encryption software good enough to be worth using. If
we are serious about freedom of speech, we must find ways to keep our
communications private. So fighting controls on encryption is a key part of
winning the battle against repression on the Internet.
****

Social Engineering

As we saw in the GTMHH on how to break into computers, social engineering usually consists of telling lies that are poorly thought through. But a skilled social engineer can convince you that he or she is doing you a big favor while getting you to give away the store. A really skilled social engineer can get almost any information out of you without even telling a lie.

For example, one hacker posted his home phone number on the bulletin board of a large company, telling the employees to call him for technical support. He provided great tech support. In exchange, he got lots of passwords. If he had been smart, he would have gotten a real tech support job, but then I can never figure out some of these haxor types.

ISP Hostage Taking

A favorite ploy of the aggressor in a hacker war is to attack the victim's Internet account. Then they trumpet around about how this proves the victim is a lamer.

But none of us is responsible for managing the security at the ISPs we use. Of course, you may get a domain name, set up a computer with lots of security and hook it directly to an Internet backbone provider with a 24 hr phone connection. Then, checking account depleted, you could take responsibility for your own Internet host. But as we learned from the AGIS attacks, even Internet backbones can get taken down.

If you point this out, that you are not the guy running security on the ISP you use, bad guy hackers will insult you by claiming that if you really knew something, you would get a "secure" ISP. Yeah, right. Here's why it is always easy to break into your account on an ISP, and almost impossible for your ISP to keep hackers out.

While it is hard to break into almost any computer system from the outside, there are vastly more exploits that will get you superuser (root) control from inside a shell account. So all

your attacker needs to do is buy an account, or even use the limited time trial account many ISPs offer, and the bad guy is ready to run rampant.

You can increase your security by using an ISP that only offers PPP (point to point) accounts. This is one reason that it is getting difficult to get a shell account. Thanks, cybernazis, for ruining the Internet for the rest of us.

But even an ISP that just offers PPP accounts is more vulnerable than the typical computer system you will find in a large corporation, for the simple reason that your ISP needs to make it easy to use.

****

Newbie note: A shell account lets you give Unix commands to the computer you are on. A PPP account is used to see pretty pictures while you surf the Web but in itself will not let you give Unix commands to the computer you are logged into.

****

Because it is easy to break into almost any ISP, haxor d00d cybernazis think it is kewl to take an ISP hostage by repeatedly breaking in and vandalizing it until the owner surrenders by kicking the victim of the attacks off. This was the objective in the assaults on Succeed.net in Oct. 1997.

****

You can go to jail warning: I usually fubar the names of ISPs in these guides because so many haxor types attack any computer system I write about. Succeed.net is a real name. If you want to attack it, fine. Just remember that we have boobytrapped the heck out of it. So if you attack, men in suits bearing Miranda cards will pay you a visit.

****

Why Should I Give a Darn? -- Ways Bystanders Get Hurt

To most people, hacker wars are Legion of Doom vs. Masters of Deception stuff. Interesting, but like reading science fiction. But what does it have to do with your life? You may figure that if you never do anything that gets some computer dweeb who thinks he's a haxor mad, you won't have a problem.

Yet chances are that you may already have been brushed by hacker war. Have you ever tried to login to your online provider and couldn't make a connection? Did you call tech support and they told you they were "down for maintenance"? Tried to send email and gotten a message "cannot send mail now. Please try again later"? Sent email that disappeared into cyberspace without a trace? Gotten email back with a "User unknown" or worse yet, "host unknown" message? Been unable to surf to your favorite Web site?

It could have been technical error (cough, cough). But it may have been more. A cardinal rule of online services is to never, ever admit in public to being hacked. Only if a reporter "outs" them first will they reluctantly admit to the attack. This is because there are cybernazi gangs that, when they hear of an online service under attack, join in the attack.

Why cybernazis do this is not clear. However, what they accomplish is to make it hard for small companies to compete with giants such as America Online. The giant online services can afford a large staff of computer security experts. So with the cybernazis rampaging against the little Internet service providers, it is not surprising that so many of them are selling out to the giants.

I don't have any evidence that the cybernazis are in the pay

of giants such as AOL. In fact, I suspect cybernazis are trying to drive the small competitors out of business solely on the general principle that they hate freedom of anything.

It is common for hacker wars that start as a private disagreement to spill over and affect thousands or even millions of bystanders.

For example, in Sept. 1996, syn flood attackers shut down the Panix ISP for several days. In Oct. 1997 the ISP Succeed.net was shut down by a team of hackers that deleted not just Bronc's but also over 800 user accounts. Many other ISPs have suffered shutdowns from hacker wars, often because the attackers object to political views expressed on their Web pages.

On June 4, 1997, hacker wars made yet another quantum leap, shutting down the Internet backbone service provider AGIS in retaliation for it allowing Cyberpromo and several other spam empires to be customers.

Tomorrow these skirmishes could pit nation against nation: power grids that serve hundreds of millions failing in the dead of winter; air traffic control systems going awry with planes crashing; hundreds of billions, trillions of dollars in banking systems disappearing without a trace. Pearl Harbor. Digital Pearl Harbor. Famine. Years before we could climb out of an economic collapse as bad as the Great Depression.

You think this is a ridiculous exaggeration? Those of use who have been in the bullseye of the cybernazis find this future easy to believe.

Winn Schwartau has been warning the world of this coming disaster since June of 1991. Someone must be listening, because in September 1997 an industry group, formed in the wake of hearings by the US Senate's Permanent Subcommittee on Investigations, appointed Schwartau team leader, Manhattan Cyber Project Information Warfare/Electronic Civil Defense (see http://www.warroomresearch.com/mcp/ and http://www.infowar.com).

Schwartau, in his book Information Warfare, tells us about some of the

attacks the cybernazis have made on his family. These attacks have included massive credit card fraud, tampering with his credit rating, turning off his home power and phone, and even tampering with the local emergency services dispatch system so that all ambulance, fire and police calls were directed to his home instead of to those who called 911 for emergency help.

Those of us on the front lines of cyberwar have seen these attacks first hand. The cybernazis, as Schwartau discovered, were willing to even risk the lives of people who had nothing to do with him.

Yes, we know hacker wars do to us, and we know what it does to you bystanders.

Why You May Get Hit

Hacker war happens to other people, right? Spammers get hacked. Hacker gangs pick fights with each other. But if you behave politely around computer criminals, you are safe, right? OK, as long as you don't live in the neighborhood of one of us Internet freedom fighters like Schwartau or me you are safe.

Wrong. Dead wrong.

Let's look at an example of a hacker war, one that doesn't seem to have any motivation at all. We're talking the Internet Chess Club. Not exactly controversial. In mid Sept. 1996 it was shut down by a syn flood attack in the aftermath of daemon9 publishing a program to implement the attack in the ezine Phrack.

There have been many bystanders hit with the wars against this Happy Hacker list. It all started with cybernazis who wanted stop you from getting email from me. For example, on Dec. 6, 1996, someone had written to the dc-stuff hackers email list (subscribe by emailing majordomo@dis.org with message "subscribe dc-stuff) saying "I think they (or maybe 'we') will survive, Carolyn's book." Rogue Agent replied:

I'm just doing my part to make sure that it doesn't happen. Ask not what the network can do for you, ask what you can do for the network.
We shall fight them in the routers, we shall fight them in the fiber, we shall fight them in the vaxen... I'm an activist, and I won't stop my activism just because I know others will take it too far.

On Dec 20 Rogue Agent wrote to me:

Ask Netta Gilboa; her magazine's in shambles and her boyfriend's in prison, while she lives in fear. Ask Josh Quittner (author of Masters of Deception); for a while there, he had to change his (unlisted) phone number literally every two weeks because of the nightly anonymous calls he was getting. Somehow they always got the new number. Ask John Markoff (coauthor of the hacker best-seller Takedown); he can't even let people know what his email account is or he gets spammed the next day.
This is not a threat... All I'm doing is telling you what's coming...
you're playing with fire. There is a darker element in my culture, and you're going to meet it if you keep going.

"This is not a threat." Yeah, right. That's what most of the guys who threaten us say.

Five days later, while it was still dark on Christmas morning, the owner of the Southwest Cyberport ISP where I had an account was woken by an alarm.
His mail server was down. No one using that ISP could get email any more.
They had been hit by a massive mailbombing by someone styling himself johnny xchaotic. jericho surfaced as the public spokesman for the attacker, claiming intimate knowledge of his techniques and motivations.

The evening of Dec. 28, someone cracked the dedicated box that Cibola Communications had been providing us at no cost to run the Happy Hacker majordomo. The intruder erased the system files and sent email to the owners

threatening worse mayhem if they didn't cave in and boot us off. The attackers also wiped the system files from a computer at the University of Texas at El Paso that I was using for research, and sent threats to all email addresses on that box. The attacker called himself GALF. It was not the first or last time that GALF has struck Happy Hacker.

Damaged computers, threats, extortion, blackmail. That's life around here. After awhile it gets kinda boring, yawn -- just kidding.

****

Newbie note: In case you are wondering whether you can get killed in one of these battles, I have found no reports, not even rumors, of any hacker war murders. These guys only kill people by accident as a side effect of their digital mayhem. Like sending an ambulance that could save a dying child to the home of an Internet freedom fighter instead. However, if someone should threaten to kill you, you should report it and any associated computer attacks. Despite what you may hear, those of us hackers who are not computer criminals cooperate enthusiastically with law enforcement.

****

How to Get into a Hacker War

"I want to fight in a hacker war. How do I get in?"

I get email like this all the time. Many newbie hackers long for my frequent experiences of being attacked by a talented gang of computer criminals. The excitement! The opportunity to go mano a mano with bad dudes and prove you are better than them!

There is some truth to this view. To be honest, I get a thrill fighting those criminals -- using legal tactics, of course. Believe me, if we catch the Succeed.net attackers, you will hear about it. But before you

make the
decision to join us freedom fighters, count up the cost. It isn't always
fun.

But I've stood up to them. And, shoot, I'm just an old lady. So if you want to attract a hacker war, and believe you are as tough or tougher than me, be my guest. But before you start provoking attacks, please wait for me to get
out the next two parts of this Information Warfare series, so you can learn
how to repair your credit rating and recover from other digital disasters.
You'll find plenty of things in the next Guides in this series that will
help you survive even the most determined hacker war. Even the kind of war
that attempts to steal all you own, wipe out your identity, and threaten the
lives of your family.

So just how do you get into a hacker war? The easiest way is to attend a
hacker convention. There are all sorts of twisted people at these things,
kind of like the bar scene in Star Wars. "He said, he doesn't like the way
you look." If you fail to grovel and suck up to those d00dz, or, worse yet,
tell them firmly that you favor freedom of speech, or even worse yet, make
fun of them for being cybernazis, you can be in for lots of excitement.

How to Keep from Getting Caught -- NOT!

So you want to be the attacker in a hacker war? So you think you can keep
from getting caught? According to jericho, writing in his "F***ed Up College
Kids" ezine, "You have media whores like Carolyn Meinel trying to teach
people to hack, writing guides to hacking full of f***ups. Telling these
people what to do, but not giving them enough information to adequately
protect themselves."

I agree with jericho, if you decide to become a computer

criminal in a
hacker war, I'm not talented enough to teach you how to keep from getting
caught.

In fact, no one can teach you how to keep from getting caught. I'll tell
you exactly why, too.

At a Def Con V panel I hosted (Las Vegas, July 1997), jericho boasted "When I break in, I close the doors behind me." He makes a big deal about how
hackers can keep from getting busted by deleting or modifying log files.
Yeah. Right. Not!

Let me tell you the REAL story about what happens when hackers think they
are covering their tracks. Sure, an ordinary sysadmin can't restore a
deleted file on a Unix system. But there are people out there with the
technology to restore deleted files -- even files that have been overwritten
hundred of times. They can restore them regardless of operating system.
There are people out there who can extract everything that has been on a
hard disk for the last several months -- or years. I know those people. I
arrange for them to read those hard disks. Guess who's toast:):):)

Then there is surveillance. Some 31337 haxor is sitting at his box raising
hell and "closing doors after him." What he doesn't know is that thanks to a
court order inspired by his boasts, someone is sitting in a van a hundred
yards away -- picking up every keystroke. Van Eck radiation, luser. Or
picking up the signals that run down the power cord of your computer. Ever
heard of Tempest?

Even if the cybercrime detective doesn't have all this high-tech hardware
on hand, the history of hacker crime shows that criminals will talk in
exchange for lenient sentencing. Commit one easy-to-prove federal felony,
let's say posting someone's stolen email on one's public ftp

server (who do
we know who has done this?), and the Feds have lots of bargaining power
against him.

So even if I wanted to help people become ubercriminals, I can't. Not
because I don't know how. Because there is no way. The 31337 d00dz who tell
you otherwise are seriously ignorant.

I predict the Succeed.net attackers are will wind up in jail. Soon. Perhaps not for that crime. But their days of freedom are numbered. It is only a
matter of picking which of their many crimes will hold up best in court, and
who will give evidence against whom. Time to study game theory -- can you
say "prisoners' dilemma," wannabe ubercriminals? Who's the narc?

"But, but," I can hear the Super Duper computer criminals sputtering. "My
buddies and I break the law all the time and we've never been busted. OK,
OK, my other buddy got busted, but he was lame."

It's just a matter of time. They need to go straight before their number is up. Or make the decision to obtain their "get out of jail free" cards by
informing on their gang before their day of doom comes up. They have much
better bargaining power if they make a deal before arrest.

****

If you happen to be a cybernazi who is having second thoughts, and would
like help making a deal with the authorities, please contact me anonymously
using my pgp key:

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

mQENAzRWYacAAAEIALYjWhzd8qO/MteFrb2p9SsY5GHdFAxT7R1M4X/jt5Nd/VKR
qCJoS4F/kQ6NwsM/mopjd4yVunxvs4QUK7eZ5A2rZuEps4EadXwwBPI63RfHci5o
BiXs9fGYtpTx7bv9dJE/Z9tved8s24asib06vLDqzyCFDXrRoYLO8PwEmifwWVWW
OL+5Th45m6cirXuwi1Idjy66AZwt8ARFnns5FA5OCb82NW54RsFKbKR2u2wUfT72
rRJg0ICt/WtZdr2dBccXEgp1232s5rgwiRvqmGjMOruUDfU2nNHH3pOk8JrefIXl
dwV0yjErb7wcecCFIrHfQKcxVoNXHlgJ6afePjcABRG0J0Nhcm9seW4gTWVpbmVs
IDxjbWVpbmVsQHRlY2hicm9rZXIuY29tPokBFQMFEDRWYaceWAnpp94+NwEB9bsH
/ilWgT2ix3B79UFfrjSE9EYCjKh1CWiIGMohdjjmV8Q3lSJIoikPtUZNak4lBTh/
wuD5ea0DZuoDe6i4EagBmRgTCvATXQqD74XtNSZSPhIQMOytJUJLlmuAnDEm96XS
30xguSFrXNjHYS19prE1yi2vQe/PJ7/K1QQwy725hjI5fnq4TnldxloaESNvurKh
Mc3GwQWF1JmpaFup3+hrEwUxcQ2PJn3xkgcjKkj1x7emDIGLCgF1RIJDLM63Q5Ju

```
bCqodumjX0pe8kHL3tRaDux+eAZ4ZD73HvF4lYi7QLKGDwX1Vv9fmbJH4tCqo3pq
RBhG32XmkTuDe0EExdSET+w=
=09hD
-----END PGP PUBLIC KEY BLOCK-----
************************************************************
```

How to Protect yourself in a Hacker War

What, you don't find getting caught up in a hacker war immensely entertaining? You don't want to be the innocent bystander caught in the crossfire of an rm command? Here are a few rules that can help you. But remember, these are only the most basic of protections. We'll cover the industrial-strength techniques in later Guides in this series, as well as how to catch the culprits.

Top Ten Beginner Defenses in Hacker Wars

10) Backup, backup, backup.
9) Assume anything is being sniffed, unless protected by strong encryption.
8) Assume your phone is tapped.
7) Never, never, ever telnet into your shell account. Use Secure Shell instead.
6) Pick a good password. It should be long, not a name or a word from a dictionary, and should include numbers and/or characters such as !@#$%^&*.
If you use a computer where others have physical access to it, don't write your password on anything.
5) This applies to shell accounts: assume your attacker will get root control anyhow, so your password won't do you any good. That means you should encrypt any files you don't want to have passed around, and send your shell history files to /dev/null each time you log out.
4) Do you use the Pine or Elm email programs? Don't keep email addresses in

your shell account. Your saved mail files are a good place for cybernazis to find email addresses and send out threatening and obscene messages to them.
GALF specializes in this tactic.
3) Regularly patrol your Web site. You never know when it may sprout rude body parts or naughty words. Preferably use a Web server hosted on a computer system dedicated to nothing but Web sites. Best of all, use a MacOS web server.
2)Disable Java on your Web browser. Don't even *think* of using ActiveX or Internet Explorer.
And, the number one defense:
1) Join us Internet freedom fighters. It will take many of us to win the battle against those who want to pick and choose whose voices will be heard on the Internet.