

New Style

Inside

- Protecting from computer crackers
- The China Syndrome meets the internet
- Treasurer's report

Newsletter of the LaCrosse PC Users' Group

volume 21 number 9

September 2001

This month, Sept. 26, 7pm

Shane Lambert presents CD recorders and associated software. I recently wasted an entire day trying to create a CD to transfer files from the Aptiva, with its fouled up networking, to my other machines. I finally decided to stop trying to use a 700mb disk and used a 650mb, which worked. Perhaps my drive is too old to use the higher capacity disks. October's meeting is scheduled to be about upgrading your system.



Editorial

Don Atkinson

In case you're wondering, I selected the Uncle Sam rolling up his sleeves image some days before Oliphant's similar cartoon, printed in the Sept. 17 LaCrosse Tribune.

I've been torn between commenting on current events or not. I have done so on oc-

continues on page 5

Secretary's report

Carol M. Frank

August 29, 2001 meeting:

First of all, Jack Storlie announced that he has one hundred 100 meg Zip disks to give away. Call or e-mail Jack.

There was some talk about Windows XP. Shane said that it is impossible to go from Windows95 to WindowsXP directly. You must upgrade to Windows98 first. Core elements are replaced from Windows95 that make it incompatible with XP. XP is the most stable version of Windows so far.

There are several problems with Windows 2000, apparently it is vulnerable to the Code Red virus and installing it on a Compaq or an HP will void your warranty.

Dave Madsen has a message come up on his computer that says it can't identify the CD rom. Shane says that it can be several causes, like a loose connection, wrong driver, etc. The worst case is a dead drive, but with 50x CD drives going for \$29.95 it is easy just to replace it.

Shane has discovered Netscape 6 and highly recommend it. Its only drawback is that it looks just like AOL.

In the August newsletter Shane had requested members to download and install a

Jack asked why ZoneAlarm asks to access live updates to the Internet. Shane ex-

puter are trying to get updates. Jeff Butzler asked what it is OK to let out of a firewall.

you can let it out. The exception is MS Word and Excel. The ports these programs use are

Shane showing what an IP address looks like.



Visit our homepage at <http://www.lcpconline.com>

know what the program is, don't give it access. If it really needs to, it will ask again.

What are ports? There are 65,365 ports on every computer. They are outlets that different software can use to access the Internet. This saves time and avoids conflicts. Software is programmed to use a specific port.

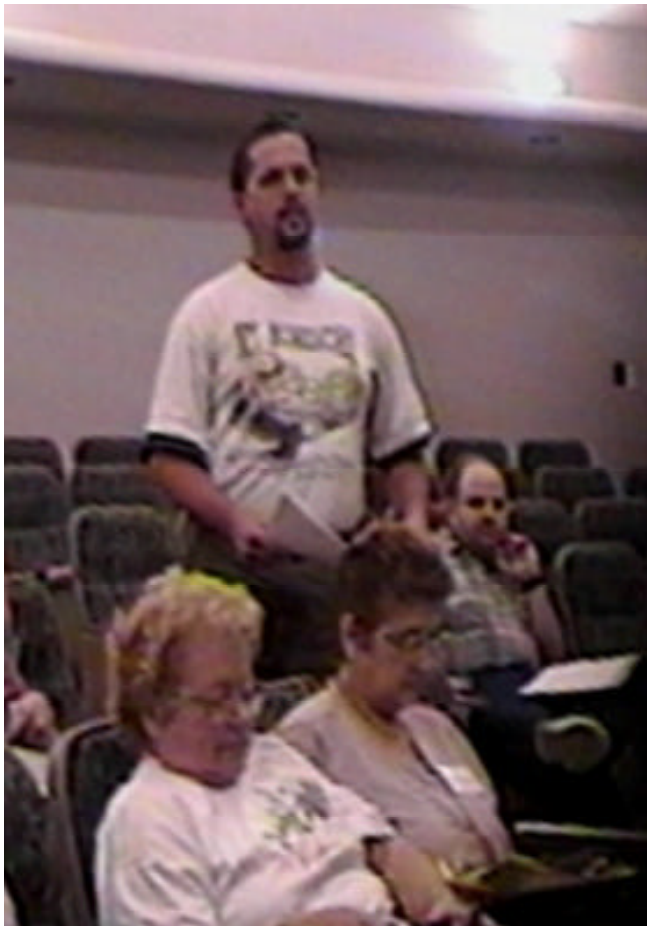
For example, browsers use port 80, FTP port 27, Telnet port 21.

If you are using two browsers at the same time, one will go to port 81. Port 1 is the port through which anything can be done to your computer. Usually this is the port used for Local Area Networking.

Some virus checkers and other programs come with a firewall. To find out what firewall you have, go to **DRC.com** and run their *SheildsUp* program for confirmation of which one you have. Some firewalls don't work together, like McAfee and Norton. ZoneAlarm will cooperate with other firewalls.

An important thing to remember is that the software doesn't automatically run. You must set it up and tell it to run.

Jeff Butzler, newcomer



What hackers use is an automatic port scanner. Port scanners generate random IP addresses and send out a ping (digital packet of information) to these addresses to see what response they get. If there is a response, (handshake) there is a port available in the computer at that IP address. Port scanners are illegal in the United States and if you see an offer to sell one, the seller is foreign. Shane himself has one legally to use to test firewalls as part of his business. He is restricted to using it one hour per week.

An Internet Protocol address is like a telephone number for your computer. It is not the same as an e-mail address or website. An IP address is an series of numbers and dots, like this: 225.28.488.2525. (*this isn't a real address*)

The would-be hacker, if determined, will keep pinging a certain IP address and will eventually determine what firewall is being used and figure out how to get in. Fifty pings per hour is a high rate and means someone is trying to get in. Immediately shut down your computer. Don't wait to shut down Windows, hit the power button. By the time Windows shuts down it can be too late. Of course

this presupposes that you have set up your firewall to alert you to this sort of activity.

Most good firewalls, like ZoneAlarm, can show the invading IP address. To do a reverse IP address lookup to find the domain name, go to **AMNESI.com**.

Would-be hackers beware! The FBI is very vigorous in tracking you down. If you ping a site they are monitoring, they will be at your door in fifteen minutes. They will ask questions after they take you and your equipment into custody.

Here are some commonsense security measures you can take.

Don't send personal information by e-mail. This is information like banking information, social security number and credit card numbers. No legiti-

Treasurer's report

Gary Stelzig

The club checking balance as of 9/12/2001 was \$837.94. We had income of \$100.00 from five renewals - Darrell Garner, Robert Guggenbuehl, Peter Schaettle, Leon Wolfe, and La Vonne Buchner - thank you. Expenses paid in August were \$13.60 for stamps, \$12.66 to photocopy the newsletter.

Renewals for September: John Benton, May Borgedahl, David Donskey, Betty Mullenbach, Arlene Wiese. Past Due: Ralph Dupae, Keith & Barb Barghahn, Richard & Shirley Dahlby, and Dennis Graves.

Our modest \$20 renewal fee for LCPC can be mailed to our lock box 2991 or to my address at 2032 South 30th LaCrosse, WI 54601 or bring to next meeting.

mate business will ask for this through e-mail, instead they would point you to their secure line at their website.

Make sure the site you are buying from has a secure line. Look for the secure symbol on the browser. Secure connection users need to be registered and installed on the vendor's server.

Don't have personal information on your laptop. Those can be stolen and passwords figured out.

Make your passwords difficult to figure out. A random collection of numbers and letters is best. (Close your eyes and hit the keyboard.)

Have fraud protection on your debit/credit cards.

And most of all don't worry too much about this, life is too short. Unless you live in the backwoods and pay cash for everything, there will always be a chance for theft and fraud. Just make it difficult enough for the average thief/hacker and they will move on to an easier target.

from *Hard-Copy, Journal of the Chicago Computer Society, July 2001*

Zen and the art of computer cracking

Jerry Maizell (jerry@maizell.com)

During the Meiji era in Japan (1868-1912), a university professor went to see Nan-in, a well-known Zen master. "What is Zen?" the professor asked.

Nan-in served tea, pouring the cup full, then overflowing, yet he kept pouring. The professor watched until he couldn't stand it. "It's overfull!" he cried. "No more will go in!"

"Like this cup," Nan-in replied, you are full of your own opinions and speculations. How can I show you Zen unless you first empty your cup?"

Everyone has opinions and speculations about computer technology. Much of both is absorbed from newspaper and TV reports and commentary, some of which is worthwhile, some of which only adds to the universe of confusion.

The difficulty is to separate the occasional stars in that universe from the mass of cosmic dust. It's easy to exaggerate the dangers of the Internet. It's also easy to underestimate them or to ignore them altogether.

But overarching all these is confusion about what those dangers are.

I get letters. Most are serious inquiries about or comments on useful subjects. Some reflect variants on common themes derived from contradictory pop culture sources.

One theme goes like this: "You write a great deal about Internet security and firewalls. But [a well-known syndicated newspaper computer columnist] says such fears are overblown, that all firewalls do is annoy users with false alerts. So why are you scaring people for nothing?"

Another takes an opposite tack: "There are so many TV news reports of stolen or hijacked credit card numbers, as well as other forms of Internet fraud, that I can't imagine why anyone is so foolish as to buy things online. Instead I use the dealer's 800 number."

The 1st reader relies on a computer version of Dr. Strangelove. He wants us to stop worrying and learn to love the cracker.

The other favors the expertise of actors with \$80 haircuts who read anything that's handed them by their producers, who can make a sensational story out of a PTA meet-

ing while warning you that the world will end soon, details to follow the next commercial.

The credit card myth

As it is the easiest of the two myths to dispel, let's take the 2d one 1st. And let me give that reader something new to worry about.

When you call that 800 number and place your order, to whom are you giving your cherished credit card number? At best it's a kid who would otherwise be working at McDonald's. What makes you think he can be trusted with your personal information?

At worst it may be a prison inmate doing contract work for the vendor as part of his rehabilitation from a life of theft, rape or murder.

Every day we hand our credit cards to strangers working as clerks and cashiers. Worse, we give them to restaurant waiters who disappear with them for 10 or 15 unsupervised minutes. They not only have your card number, but your signature.

While credit card fraud is a huge industry and a drain on the economy, our modern economy would stop altogether if everyone always had to pay in cash. Credit card companies therefore absorb the losses as a cost of doing business.

Most guarantee that cardholders will be responsible for no more than the 1st \$50 of fraudulent transactions. Naturally, some of that cost is passed on to us in the form of high interest rates on unpaid balances. But that cost is the same whether it's via your local gas station, Denny's, WalMart or Amazon.com.

Naturally, online as offline, one should deal with vendors one trusts.

The firewall myth

Just as it is true that most people you see on the street are not threats to your safety, it is true that most firewall alerts are not indicative of attacks on your system. Many merely reflect your browser's attempts to connect with websites or ads.

But there are bad guys on the street. So one learns to be generally aware of potential threats and take appropriate precautions according to the environment.

Growing up on Chicago's West Side, in Lawndale, in the days before air conditioning, we had no hesitation about sleeping in the park on hot July nights. Today, walking through some Chicago parks in broad daylight can be an adventure.

Had the Internet existed in my youth I don't know if it would have been as safe as Douglas Park was. I do know that the world is different today.

Let's take a tour of a few of the Internet's shadowy corners. It's safe, but keep your eyes peeled and don't get into any trouble.

Know your enemy

Some folks may wonder at my providing pointers to resources for doing bad things on the Internet. But the bad guys already know all this and much more. The only people who don't know are innocent

To effectively defend oneself against threats one should understand the nature of the threat. Ignorance is dangerous.

There was a time when cracking or intruding into computers was the sole preserve of a small group of sophisticated, if misguided, hackers. Many of them were also social rebels who had some sort of ethical discernment, distorted though it might have been.

Today any mischievous kid can just download some scripts and tools and spread misery. You should at least be familiar with what kinds of nasties that kid uses to turn your computer into a zombie that unwittingly becomes part of a distributed denial of service (DDOS) attack.

A good place to start is www.undergroundnews.com, whose slogan is "Dare to take the road to knowledge, power and information." Under "Resources" in the left column click Newbie, which takes you to a page headed "You too can learn the ways of the dark side."

This is a news site, presumably operated by "good guys." But you can get into some pretty deep waters if you want to. Take a look at their link to "Frequency," a zine that describes its content like this:

"What you will not find here is anarchy material, such as how to destroy a building or really screw up someone's life. We're more concerned with how things work, so for a simple example we will not publish how you can use a Trojan to destroy someone's computer. We may however, publish how exactly a Trojan does what it does. After that, we ask that you're smart enough to know right from wrong and do not attempt to use it for

ill purposes, as this is not the true hacker way.”

Now jump over to www.blackcode.com and explore the discussion forums, where you'll find questions and answers on cracking into other people's computers.

The motherlode of links to hacking, cracking and phreaking sites may well be 'www.startplaza.nu. Phreaking refers to cracking telephone and cellular services and equipment to get around the rules or obtain free or unauthorized access.

When I visited 'www.hack.co.za' it displayed the name of my computer, my IP address, ISP node and the names of three of the four browsers I have installed. An auspicious beginning.

Beyond the firewall

If you weren't convinced before, I trust that after perusing the above you will have installed a firewall, either one of the several commercial ones available or the excellent free-for-home-use ZoneAlarm (www.zonealarm.com) or the highly regarded (but I haven't tried it) Tiny Firewall (www.tinysoftware.com). I like ZoneAlarm because it is very easy to use.

There are several sites where you can test to see how open your system is to attacks. One of the more thorough is www.hackerwhacker.com, where you'll get one free system scan. They'll e-mail a password and link to you.

Here are the results I got from my HackerWhacker scan: "PROBLEM: This address (192.168.1.101) is a special address that only works on a Local Area Network. It doesn't work over the larger Internet. Try using another IP Address if you have one. This address is indicative that you are behind some kind of Internet protection (firewall) so much that even HACKER WHACKER cannot scan you. If you don't have another address, HACKER WHACKER cannot scan you. On a positive note, it also means in most cases you are virtually impervious to outside hackers."

My system is behind both a hardware firewall (a LinkSys Cable/DSL router) and ZoneAlarm. Either should be good enough on its own, but

I'm a belt and suspenders kind of guy when it comes to security,

Are you cracked?

Probably not. But it never hurts to check. Go to www.dshield.org, look below the map and click the "here" link in "Are you cracked? Click here to see."

DShield calls itself a distributed intrusion detection system, created by Johannes Ullrich in an attempt to solve the problem of too many firewall alerts by acting as a clearing house for firewall logs.

Users volunteer their firewall logs listing the addresses that have attempted to connect to their systems. Those connections may indicate that a hacker is probing a computer seeking vulnerabilities. Most are legitimate Internet traffic, such as a server checking if the computer is still online, a chat server sending a message or a legitimate company doing a connection survey.

But sometimes it may be an attacker scanning for a weak spot through which to enter, like a burglar knocking on apartment doors and rattling doorknobs to see if anyone's home.

DShield's idea is to compare many logs. Addresses that show up frequently may belong to potential intruders. Complaining to ISPs is often an exercise in frustration. DShield wants to expose the crackers. A known criminal is on his way to becoming an ineffective criminal, if not a punished one.

It's not a solution in itself, but a step in the right direction.

The site's Internet Primer offers a good introduction to the concepts involved, in plain English.

Now there's one more thing you should do: Turn off File and Printer Sharing, at least while you're on the Internet. If you're using a cable modem, leaving this setting on can result in your computer showing up when a neighbor opens his Network Neighborhood icon. He may not want to see what's on your computer, but why tempt him?

If you don't have a home network, open the Networks applet in Control Panel (or right-click Network Neighborhood and select Properties). Then select the File and Printer Sharing button and uncheck both boxes.

If you have a home network, select the TCP/IP element in the Networks applet, then Properties. (You may have two TCP/IP elements. Select the one for your network card, not the one for Dial-Up Adapter).

Select the Bindings tab, then uncheck File and Printer sharing. You can still share files

and printers via the NetBEUI protocol, even though it's turned off in TCP/IP. If you need help to do this e-mail me.

Citing Zen stories (koans), like the "Cup of Tea," is easy. Attaining Zen is difficult. Fortunately, attaining relatively secure computing, while not easy, is achievable with only a little effort.

To start, just empty your cup

The China syndrome meets the Internet and melts down

The nefarious propagandize the ignorant who pontificate to the gullible, who preach to the apathetic, who repeat anything to anybody because they don't really care whether or not it is true.

Thus are TV talking heads and anchormen born.

When I exposed the fallacy of "The Digital Divide" (Hard Copy, April, "Four candles, no ashes") I was under no illusion that this nonsense would really be dispelled by my little cry in the wilderness.

There are too many who stand to gain from that particularly big lie, ~ well as a great many well-meaning people who have been ensnared by its appeal to their commendable charitable instincts. Folks whose lives have been improved by computers and especially the Internet are easily fooled into thinking they will be working for a better world by spreading those blessings to the world's poor.

As my column explored in some detail, the world's poor have more serious problems than lack of a local ISP and the equipment to dial in. For one thing, most of them don't have a phone line within walking distance, not to mention a paved road.

Internet access? Many would be happy just to have access to a steady supply of potable water.

Another favored theme of pundits, politicians and poltroons is that the Internet will assure the downfall of all tyrannies, leading to a wonderful global community of peace and freedom for all.

"The Internet shall set ye free," they gush in a semi-religious frenzy.

Let's see if I can disentangle the information from the misinformation and disinformation of this beguiling fantasy.

WWI, the war that was supposed to make the world safe for democracy, actually made the world safe for WW2. WW2 freed Eu-

rope from Nazi tyranny, only to turn much of it over to Communist tyranny.

Now the wishful thinkers imagine that the brutal dictators of Iraq, Libya, Cuba, North Korea and especially China are going to be converted to "democracy" because they can't control a few propeller-heads, geeks and a handful of PCs?

China is the favored example. While only a tiny number of private citizens in China have Internet access (all of whose connections are monitored by the secret services), there are large numbers of Internet cafes in many cities. Thus, the story goes, users can e-mail anonymously with Hotmail, Yahoo or other webmail accounts. They can surf the Web unobserved, creating and accessing sites that tell the truth. Information is free and information is the one thing that tyrants can no longer control.

"The information genie is out of the bottle," we are told, "and the Chinese rulers can't stuff it back in."

That line of guff may satisfy those who are predisposed to believe that the Chinese leadership are just plain folks like us: The bad ol' days of the Tienanmen massacre are long gone. China wants and needs trade and trade requires communication and communication inevitably means freedom.

Editorial continues

casian in the past and, obviously, have decided to do so again.

There was horror of Sept. 11 and the euphoria following it. Perhaps euphoria is the wrong word, but there seems great joy and confidence that we will soon punish those responsible for the horrendous events of Black Tuesday and life will return to normal.

But there are many questions that need to be considered.

I hope what follows makes you uncomfortable, I especially hope it makes you think.

be careful what you wish for

First of all, I believe that if we markedly change the way we live our lives, they win. If we become paranoid, reject people because of their appearance, religion, or national origin, they win. This country has always been the beacon of liberty in the world. If our revolution had failed I doubt that the world would ever have heard of Simon Bolivar.

Let's not start down this road if we're not going to be willing to see it through.

The fact is that Internet cafes in China require a license. In order to get a license the cafe management must agree to maintain a register of users and a log of all Internet activity. The register and log must be regularly submitted to the police.

The websites of Chinese pro-democracy online publications have been wiped out by viruses and other attacks from China's police. Those who promote such sites are prosecuted for treasonous activities.

But the Communist Party of China is not satisfied with such low-tech solutions. They are planning for the future.

Not content merely to restrict Internet access, China is building a Great Wall in cyberspace. Rather than connecting to the Internet, those Chinese fortunate enough to have access will connect to a huge Intranet from which all uncensored news will be excluded.

"Millions of Chinese users will soon be logging onto this Intranet thinking that it will give them unrestricted access to information from around the world. They will actually be entering an antiseptic environment which has been carefully swept for all 'dangerous' content. A great deal of costly advanced technology will be required to set up a Chinese Intranet, but it is part of a grand strategy for

Make no mistake, I believe this war will last years and get very messy. There won't be two weeks of air strikes, narrated by Norman Schwartzkopf in a nightly briefing, and then a declaration of victory. It will be a test of national will to see it through, because we will not only kill the bad guys. We will also kill their families and innocent neighbors who don't support what they do, but are in no position to interfere. This is the nature of war.

Last week, a co-worker said to me "Why don't we just find this bin Laden guy and take him out?" First of all, we are not going to "take him out", or "terminate with extreme prejudice", or any other mealy mouthed euphemism, we are out to kill him, and his associates and followers.

Get your mind around this, we are going to be sending our relatives out to kill a bunch of people. They are not nice people, what they have done should condemn them to Hell and we are the ones who are going to send them on their way.

But along the way we will get our own hands dirty, we will deal with unsavory char-

controlling information that may even involve public security officials setting up a few subversive-looking sites as a way of entrapping unwary critics of the regime.

That quote is from Steven Mosher's book, "Hegemon: China's plan to dominate Asia and the world" (Encounter Books, www.encounterbooks.com; though if you want to buy it check the usual discount sites, like www.addall.com).

In 1979 Mosher became the first American social scientist invited to do research in China. He was also the first asked to leave because he declined to let his research be framed by the Party line.

Apparently because it was mentioned by one of the characters on the popular TV show, "The Sopranos," Sun Tzu's 2400-year old text "*The Art of War*" has become a best seller. Something similar happened a decade or so ago when the Michael Douglas character in the movie "Wall Street" also quoted the Chinese sage.

If pop culture succeeds in bringing ancient Chinese philosophy to a new audience no one will be more pleased than I. I remain somewhat skeptical, but hopeful, that readers will recognize the Chinese Internet syndrome in the light of Sun Tzu's classic pronouncement: "All strategy is based on deception."

acters, people that we would probably just as happily kill under other circumstances.

We've done it before. We saved the monstrous Communists from the monstrous Nazis and enabled them to enslave half of Europe and three quarters of Asia. But we believed at the time, and still do, that we chose the lesser of two horrible evils. We'll probably have to do it again in this war, be ready for it.

Along the way mistakes will be made. Targets are missed, some targets should never have been targeted at all. We'll see scenes of widows and orphans digging through the rubble that used to be their homes, however wretched. The media will show us their tears and wailing over their dead fathers, brothers, and sons, whether they were depraved terrorists or someone who was just in the wrong place when the bomb or shell dropped, or the troops moved in. Sorrow looks pretty much the same, regardless of who the deceased may be. Are you willing to accept this as the price of security and freedom, or will you call on the military to "be more careful from now on"? Are you willing to stand

continues on next page

aside and let the military do their jobs without interference or undue criticism?

There has been talk of declaring a war on terrorism, whatever its name, wherever it is incubated. It has been said "one man's terrorist is another man's freedom fighter". Are we just going to go after the Moslem terrorists? Just those between India and the Mediterranean, or the ones in the Philippines as well? Do we also plan to eliminate the Shining Path in Peru, or Yucatan separatists in Mexico? How about the IRA? The PLO has launched many attacks and killed hundreds in recent months. On Sept. 11 Arafat looked like a man who knew his life was hanging, not by a thread, but by a piece of spider's webbing. The Mujahadeen in Afghanistan were once our clients, it served our purposes for them to fight the Russians and they were glad for our money, arms and supplies.

If you're not willing to accept these messy facts the time to contact your legislator is now, before any blood is shed in your name. It may be possible to achieve our goals through diplomatic and economic pressure, without killing anyone directly.

the homefront

What about us, how will our lives change?

In the past, I have occasionally called your attention to efforts of the government to erode your rights, especially in the area of privacy. As Bette Davis said, "Fasten your seatbelts, it's going to be a bumpy night."

Decide right now if you're going to be willing to have your e-mail and phone calls monitored. If you want the government to have a "back door" into any security and encryption setup you install on your computer.

Decide if you'll accept having to show your identity documents whenever you enter a government building, concert, sporting event, airport, shopping mall, or if some law officer, or private security guard decides you need to be checked out.

"But Don," you say, "it won't get that bad. We've got our Constitutional rights." It can get that bad, it has in the past, in this country, and for some people it's that way right now.

Near the end of the Clinton administration a case came to light from Florida. Since 1997 three people have been held in "secure detention" (that's jail to you and me and them) on "unspecified charges". Not only

have these people not been convicted, or tried, their lawyers can't even find out what they're charged with. The government claims that to do so would endanger an ongoing investigation.

John Adams, champion of liberty and founding father, tried to prosecute for treason newspaper editors who were critical of his actions as president. Lincoln muzzled the press and suspended habeas corpus. This meant people could be arrested and held without charge or trial for as long as it pleased the government. It pleased the government to hold the Baltimore city council for the entire war. In 1942 tens of thousands of American citizens and resident aliens were compelled to leave their homes and reside in prison camps purely because of their national origin.

cowardly new world

When I was in high school I naively asked our parents and teachers "why didn't you do something to help the Jews before the war as they tried to flee Germany?" The normal reply was that they were unaware of what was going on. I believed such a thing could never happen again, I believed we were a better generation. I know better now. I saw this country, this people, stand by as an inept but ruthless leader tried to be a latter day Hitler in the fragments of what had been Yugoslavia. Maybe it was because the victims were Moslems, maybe because they were white, or maybe simply because I had misjudged my fellow citizens that we knew what was going on and did nothing. We cared more that black South Africans couldn't vote than we cared about the clumsy and slow genocide going on in Eastern Europe.

Remember the Clipper chip? In the mid nineties the government tried to compel manufacturers to include this chip into telephones and modems to allow wiretaps simply by sending a signal to the device. This week, the government is trying to expand the scope of wiretaps to "include any phone a terrorist may use". This effectively means every phone in the country.

Internet Service Providers have turned over to the government private records of the suspects, without benefit of court order. Investigators are reviewing months worth of e-mails, I wonder how much trouble I'd have getting copies of all my e-mails from AOL for the last six months. So much for guaran-

tees of confidentiality from private companies. Your records could fall under government scrutiny without your knowledge or the consultation of a judge.

In the name of public safety the government wants to increase monitoring in public places. Cameras with face recognition technology were used at this year's Super Bowl to try and identify wanted criminals. The manufacturer reports many inquiries in the last week. In New York and elsewhere, cars passing through toll booths are video taped. Some cities have cameras viewing and recording what happens on chosen streets. Are we willing to be under government surveillance whenever we leave our homes?

I've heard this ascribed to both Jefferson and Franklin, but I've never been motivated enough to find out who actually said it: "Those willing to give up a little bit of freedom for security will lose both and deserve neither." We must be careful that we do not change America so much in trying to protect it that ultimately destroy it.

Now is the time to decide what you're willing to accept, and share your views with your legislators. Bear in mind that we live in a republic, not a democracy. Our elected officials are expected to exercise their own best judgment, even if that contradicts expressed will of the people. If the vote is 250 million to 1, and the 1 belongs to the president, that is the vote that prevails.

You have the right to speak, do so if you wish, but no one has the obligation to listen.

where do I stand?

I've written this to try to help you clarify your own position and thinking, so you really shouldn't care what I think we should do. If you do care, read on. If not, thank you for your time and attention.

It was the late sixties and many of the multinational corporations were having executives kidnapped for ransom. A policy was announced by the head of corporate security for Coca-Cola in South America. He told them "If you kidnap any of our people, go ahead and kill them. We will not pay a penny of ransom. We will spend whatever is necessary to find out who you are. When we do, we will kill you, your wife, your children, parents, brothers, sisters, cousins, your dogs, pigs and chickens." There were no cases of Coca-Cola executives being kidnapped.



I want us to make such an example of these terrorists that no one will ever again consider targeting civilians going about their business in peacetime.

We should destroy their bases and kill or capture every person found in these camps. These cowards claim that they are willing to die for their cause. Are they also so anxious to see their wives and children die for it? We should not target refugees or non combatants, but we should not cancel operations because they are in the target area.

This is certainly unfair, but if they are killed they can complain to God, they just get in line behind the thousands murdered by their relatives.

They started it, they set the ground rules, we need the courage to finish it.

If we obtain their records, we track down anyone who has ever sent them money or other goods. These people forfeit all their money, businesses and property.

If a government is supporting terrorists, the head of state and appropriate ministers are arrested and tried. If they want to resist we destroy the country's infrastructure, not just the military. Every power plant, refinery, bridge, tunnel, dam, water distribution network is targeted.

In the mid eighties the Army ran a commercial featuring a song that said, in part:

I'm out here in the darkness and the rain is pouring down.

Never was like this in my home town.

It's not like this in my home town, but that's all right by me.

You see, I'm out here for my home town, cause freedom isn't free.

No, freedom isn't free, the life we have lived was paid for with the blood and lives of those who have gone before us.

We are now faced with the horrible truth that to protect ourselves from those that hate us we have to be willing to fight.

We have to be willing to die.

And we have to be willing to kill.

God have mercy on us all.

if you made it through all that, you need a break

Computer Terminology Explained

from rec.humor

Printed in the October 1997 issue of the I/O Port Newsletter

Don Singleton, TCS email don@apcug.org

Alpha -- Software undergoes alpha testing as a first step in getting user feedback. Alpha is Latin for "doesn't work."

Beta -- Software undergoes beta testing shortly before it's released. Beta is Latin for "still doesn't work."

Computer -- Instrument of torture. The first computer was invented by Roger "Duffy" Billingsly, a British scientist. In a plot to verthrow Adolf Hitler, Duffy disguised himself as a German ally and offered his invention as a gift to the surly dictator. The plot worked. On April 8, 1945, Adolf became so enraged at the "Incompatible File Format" error message that he shot himself. The war ended soon after Hitler's death, and Duffy began working for IBM.

CPU -- Central propulsion unit. The CPU is the computer's engine. It consists of a hard drive, an interface card and a tiny spinning wheel that's powered by a running rodent - a gerbil if the machine is a 286, a ferret if it's a 386 and a ferret on speed if it's a 486.

Default Directory -- Black hole. Default directory is where all files that you need disappear to.

Error message -- Terse, baffling remark used by programmers to place blame on users for the program's shortcomings.

File -- A document that has been saved with an unidentifiable name. It helps to think of a file as something stored in a file cabinet - except when you try to remove the file, the cabinet gives you an electric shock and tells you the file format is unknown.

Hardware -- Collective term for any computer-related object that can be kicked or battered.

Help -- The feature that assists in generating more questions. When the help feature is used correctly, users are able to navigate through a series of Help screens and end up where they started from without learning anything.

Input/Output -- Information is input from the keyboard as intelligible data and output to the printer as unrecognizable junk.

Interim Release -- A programmer's feeble attempt at repentance.

Memory -- Of computer components, the most generous in terms of variety, and the skimpiest in terms of quantity.

Printer -- A joke in poor taste. A printer consists of three main parts: the case, the jammed paper tray and the blinking red light.

Programmers -- Computer avengers. Once members of that group of high school nerds who wore tape on their glasses, played Dungeons and Dragons, and memorized Star Trek episodes; now millionaires who create "user-friendly" software to get revenge on whoever gave them noogies.

Reference Manual -- Object that raises the monitor to eye level. Also used to compensate for that short table leg.

Scheduled Release Date -- A carefully calculated date determined by estimating the actual shipping date and subtracting six months from it.

User-Friendly -- Of or pertaining to any feature, device or concept that makes perfect sense to a programmer.

Users -- Collective term for those who stare vacantly at a monitor. Users are divided into three types: novice, intermediate and expert.

Novice Users -- People who are afraid that simply pressing a key might break their computer.

Intermediate Users -- People who don't know how to fix their computer after they've just pressed a key that broke it.

Expert Users -- People who break other people's computers.

This article is brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an International organization to which this user group belongs.

LCPC Board

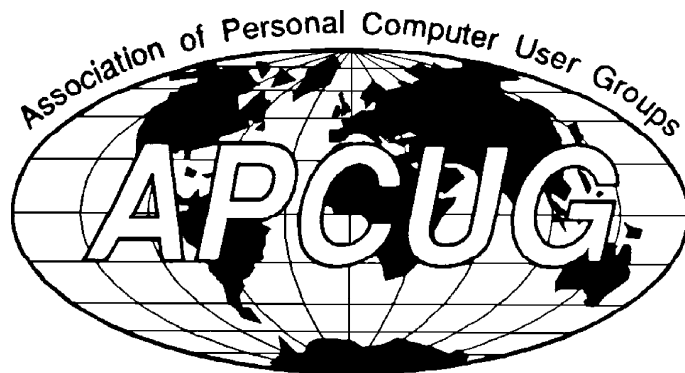
Shane Lambert—President, Board 784-5445
shane@couleeweb.net

Marian Havlik—Vice-president, Board ... 782-7958
havlikme@aol.com

Gary Stelzig—Treasurer, Board 788-7075
gstelzig0@aol.com

Don Atkinson 784-0150
Newsletter editor and publisher donaldeatkinson@aol.com

Carol Frank 784-0150
Secretary, Board, newsletter, programs
carolmfrank@aol.com



WWW.APCUG.ORG

LCPC is a member of APCUG

New Style is published eleven times a year, monthly Jan-Oct and a combined Nov-Dec issue

General meetings are held the last Wednesday of Jan-Oct in the Overholt Auditorium at the Lutheran Hospital. The combined November-December meeting is held the second Wednesday in December.

Thank you, Gundersen-Lutheran, for making this wonderful facility available.

Meetings begin around 7:00 PM. Everyone is welcome, attend a meeting or two with no obligation to join.

Dues are \$20 for one year following payment. Membership entitles you to attend meetings, tap into the corporate wisdom, receive special user group discounts from publishers and others, receive (and contribute to) this newsletter. You may also obtain software provided by publishers for review of the product. Unsigned articles are by the editor.

Other user groups are welcome to reprint with proper credit.

The newsletter is printed the Wednesday before the meeting, please submit articles by the 13th of the month. Upload to:

lacrossepcug@aol.com

Commercial advertising rates available upon request. Member's personal ads are free.

LCPC

P.O. Box 2991

LaCrosse, WI 54602-2991