"Members Helping Members"

Nominations For The April Elections Commence This Month

INSIDE THIS ISSUE:

T i p s & T r i c k s

Submitted by: Jim Rutledge

Best Keyboard Shortcuts to Save You Time
Getting used to using your keyboard exclusively
and leaving your mouse behind will make you
much more efficient at performing any task on
any Windows system. I use the following key-
board shortcuts every day:

Windows key + R = Run menu

This is usually followed by:
cmd = Command Prompt
iexplore + "web address" = Internet Explorer
compmgmt.msc = Computer Management
dhcpmgmt.msc = DHCP Management
dnsmgmt.msc = DNS Management
services.msc = Services
eventvwr = Event Viewer
dsa.msc = Active Directory Users and Com-
puters
dssite.msc = Active Directory Sites and Services
Windows key + E = Explorer

ALT + Tab = Switch between windows
ALT, Space, X = Maximize window
CTRL + Shift + Esc = Task Manager
Windows key + Break = System properties
Windows key + F = Search
Windows key + D = Hide/Display all windows
CTRL + C = copy
CTRL + X = cut
CTRL + V = paste
Also don't forget about the "Right-click" key
next to the right Windows key on your key-
board. Using the arrows and that key can get just
about anything done once you've opened up any
program.

L C A C E Q u i z o f t h e M o n t h
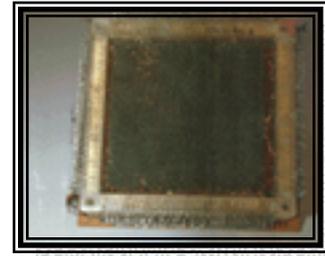
What Is It?
This form of computer memory was widely used
through the late 1950's to the early 1970's. This
memory block can store up to 32 bits, or four
characters. The "On" or "Off" switches are cre-
ated by having an iron magnet in the shape of a
donut intersected by horizontal and vertical wires.
The "1" and "0" switch setting was created by al-
ternating the direction of the positive and negative
currents.

Be **THE FIRST** club member to submit the cor-
rect answer to **J.J.** what the following item is
and you will be awarded 2-Free movie tickets.
The first to submit their answer at the February
meeting will win.   **L.C.A.C.E. officers are not
eligible**
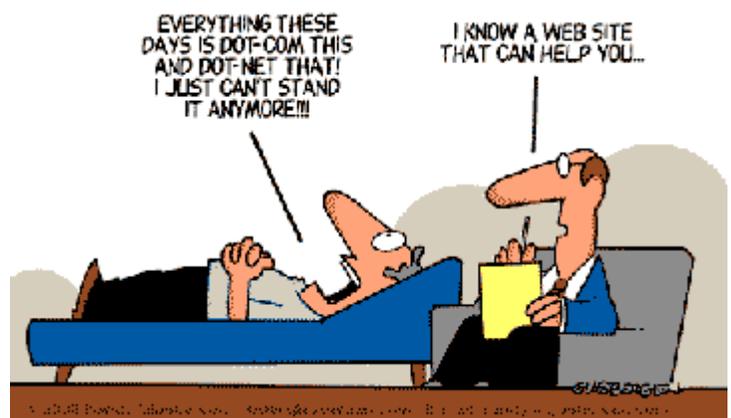
Why do I get SO MUCH spam?

Submitted by: J.J

The answer to that question is simple. First, sending spam email is cheap! A spammer can send out a direct marketing email to hundreds even thousands of recipients for under one cent. **Second, believe it or not people buy things and reply to junk email.** NEVER EVER BUY ANY GOODS OR SERVICES ADVERTISED BY SPAM! It just encourages more spam, If there is something advertised by spam you are actually interested, find it somewhere else online, it is time users Banned Spam. So when you put the two reasons together you get the simple and basic answer that spamming is profitable. People are making a lot of money by swamping your inbox with all kinds of junk, scams, and offensive material.

So the real question is **How Do Spammers Get My Email Address?**

The question we hear more than any other is: How did my email address become public knowledge? The companies and persons responsible for flooding your inbox with junk email, advertisements, and offensive adult content, are very smart and determined technically savvy internet users.

This document is meant to not only inform you on why the problem is so pervasive, and why without some defense it will only get worse. And second, to dispel a few myths about spam and how not to get spammed.

MYTHS:

1. **If I don't give out my email address, spammers won't get it.** This is the I use my hotmail address for signing up for websites, and I only give out my real address to people I know. This is a fairly effective strategy, and in the short term it may actually work for you, however within a matter of time you address will be located, exploited, and shared.

Signing up for adult sites is why you get "those kind of emails sent to you". The annoying question – "What kind of websites do you visit?" Contrary to un-informed belief, you do not have to visit or sign up for adult sites to get pounded with junk email advertising "XXX HOT fill in the blank".

2. **I complain to the spammers ISP, that way their account is deactivated.** People have been complaining to ISPs since spam started, and spam has not slowed down. Email headers are forged, or originate from thousands of different servers, sometimes switching servers multiple times for the same message batch.

REALITY:

You may be aware of one or more of the following "tactics" of getting your email address and abusing that information to bombard you with trash. Below is a list of the more popular methods of getting your address:

1. **They buy your name from a list:** These junk mail & targeted email lists have been around almost as long as the internet itself. For as cheap as $100.00 anyone can buy a list of over 11 million addresses. These lists we're created by numerous unscrupulous website owners, and online stores that would "share" their customer's information for some money. As you can imagine it is impossible for spammers to identify your likes, or interests, when sending mails to such a large group. So a "shotgun" mailing is sent out, product offers, get rich quick schemes, adult porn sites, Korean & Chinese ??? mailings, are all sent out to all 11 million names.

2. **Opt-in Lists:** These two little words (or one hyphenated one however you look at it) are quickly becoming infuriating. These lists are developed by partnering with legitimate websites which make you check "Don't send me offers", well sooner or later you'll forget to check one of the boxes, and you're added to an opt-in list. Although many opt-in lists are legitimate and will honor your removal requests, for every one there are three that are not truly "opt-in" lists. You ask to be removed from an email from "MarkertingPartners Ltd", and tomorrow you get two messages saying you opted-in at one of the partner sites of "SuperOptIn Ltd".

3. **Email Extractors:** These software tools are very skilled at scouring the internet for email addresses. Websites, Forums, Alumni sites, news posts, etc. These robots can locate thousands of email addresses an hour. And spam-

mers run them day and night.

4. **MX Server Extractors:** These programs exploit internet mail server protocols. When an email is sent to you it is handed over to your Mail Provider's server, which starts "communication" with the sender. The sender's server asks to deliver a message to a user on your server, but before the message is actually accepted by your server it wants to know who it the mail is addressed to. So your address is sent over, and your server replies whether the name is OK, or the address does not exist on the server (what happens when a message is "bounced" back to you). Basically the MX server extractors mimic the communication without actually trying to send the message. Think of it as someone ringing your doorbell and asking if "Joe" is home, no one named Joe may live at your house, however if the person at your door tries enough names sooner or later the may stumble upon yours, and you will say "Yes". (You are smart enough to stop answering after the first or second name guess however most email servers are not). Programs exist that can mine over 5000 email addresses per minute, and believe it or not they sell for less than $100.00

5. **Viruses, Spyware, and Mailicous Code:** Not to long ago viruses & spyware started to appear that transparently load themselves or are sent via email to your mail client. As soon as you open books, contact lists, and distribution lists, and "report" their findings back them, the read you address to home base.

So when someone claims they don't get any spam at all, either they have not had their email address very long, or more likely there ISP does a pretty good job filtering spam at the server level before it gets to them, which probably means legitimate mail is also being deleted before it gets to them as well. So if you are like the rest of us, you have to fight back yourself or just quit using email.

Have you invited any of your friends to this months club meeting?

Jim Rutledge (above) and Les Larkin (below) doing there backup presentation at the January meeting.

Good Job Guys

Browsing Safety: Help Protect Your Personal Information Online

October 21, 2002
http://www.microsoft.com/security/articles/
saferbrowsing_personalinfo.asp

Most of us don't even pause before filling out a contest entry form at the hardware store and leaving personally identifiable information in a jar on the counter. We feel more wary in the online world, but you can take steps to help control of personal information.

As a rule of thumb, you should provide personal information only to Web sites that you consider to be reputable and to have a valid reason for asking for the information. If you're buying online from a trusted Web site, for instance, the site probably has a good reason to ask for your address and credit card information.

Consider Combinations of Information

Even if a single piece of information—such as your mother's maiden name—seems fairly innocuous, consider how it might be used if combined with other information about you that's available online. For example, a birth date and postal code alone might be enough to identify a person who lives in a rural area.

When you are choosing a user ID and password, many Web sites will offer you a choice of "secret" questions that you can answer to confirm your identity should you forget your password. Avoid questions that could reveal personally identifiable information, such as your mother's maiden name. By knowing that single piece of information, an unauthorized user may be able to access sensitive information you have stored on that site, such as your credit card number or your health history.

What Could Your Browser Tell?

Think carefully about what personal profile information you configure into your Web browser. For example, some Web browsers let you create a personal profile that includes not only your business addresses and phone number, but your age, gender, children's names, group memberships, home address, and home tele-

phone number.

In order to deliver customized content based, for example, on your gender or hobbies, a Web site may tap into your profile. So before you fill in any of the blanks in a profile, ask yourself whether you want a Web site to know that information.

Be Careful What You Share

If you use a computer in a public space, such as a library or Internet café, always sign out of any account you have accessed and close the browser before you walk away. If you don't, the next person who uses the computer might be able to access the information you entered.
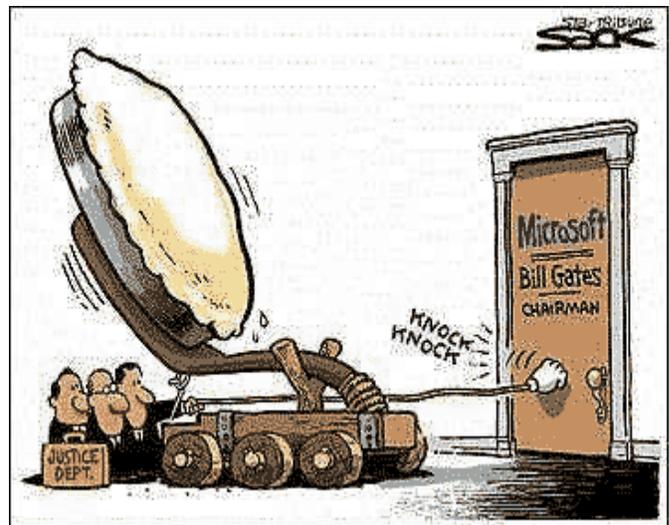
Remedies for Virus Relief

June 14, 2002

When you hear about a computer virus going around, it's time to make doubly sure that your computer is not vulnerable to catch—or pass along—the infection. Besides the preventative actions you can take, there are things you need to do if you think you have a virus to get your computer back to health.

7

How Do I Know If a Virus Alert is Genuine?

Is it real or is it a hoax? If you've seen or read about a new virus via a reputable news source or publication, it is probably not a hoax. However, if you receive an e-mail, even from someone you know, regarding a new virus alert that asks you to pass it along, stop! This is a common trick used by virus creators to spread the infection.

Instead of forwarding a virus alert e-mail to your address list, confirm whether or not the virus alert is real by contacting either your antivirus vendor or Microsoft® Product Support Services.

Once you've confirmed that the virus threat is real, the next course of action is to fix it.

How Do I Know If I Have It?

Unless you have antivirus software installed on your computer, you simply won't be able to know if it has been infected. In many cases, a virus can slow your computer's processor or trigger other unusual behavior; however, these symptoms can also be caused by a number of unrelated reasons.

Keep up-to-date with the latest virus definitions by regularly visiting your antivirus software vendor's Web site to download them, or by running scheduled updates to your antivirus software. Only then will your software be able to recognize the latest identified threats.

How Do I Get Rid of It?

Once you have identified that you have a virus, follow the directions on your antivirus software vendor's Web site to download the latest definitions or updates that will fix or remove the virus. In some cases, you may also need to follow the steps provided to manually remove viral code within your system.

If you need further assistance, you can contact your antivirus software vendor or Microsoft Product Support Services for support in removing the virus. (To obtain virus removal support from Microsoft Product Support Services, you will need current antivirus software installed on your computer.)

How Do I Know It's Gone?

In most cases, if you download the latest virus definitions from your antivirus software vendor, this will take care of the virus. However, you still need to be alert, because many times a Trojan horse is spread like a virus or could be spread with a virus, but may not show symptoms for quite a while, if ever. If you notice your computer or Internet connection running without

should go to your antivirus software vendor's Web site to install the latest definitions or scan your machine to detect the presence of any Trojan horses.

How Do I Help Protect My Computer from Viruses?

There is no magic bullet that will protect your computer or files from infection. One of the best strategies against any security breach is a well-informed and proactive defense.

The most important actions you can take are:

- Install antivirus software and keep it current, ideally updating it weekly. This is your first and best defense. See "Checklist: Use Antivirus Software".

- Use Windows Update to scan and update your Windows operating system with the latest free software patches, including those for Microsoft Internet Explorer and Microsoft Outlook Express. See "Checklist: Keep Software Up-to-Date".

- Use Office Products Update to keep Microsoft Outlook® and other Microsoft Office programs up-to-date to help guard against virus intrusions.

- Learn how to set security features. See "Checklist: Check Your Settings".

- Install a firewall, especially if you use a high-speed Internet connection. See "Checklist: Install a Firewall".

Other good practices to follow:

- Be cautious about visiting unknown or untrusted Web sites. Untrusted or disreputable Web sites can transmit a virus directly into your computer. Staying on the main routes of the information highway will help protect your safety.

- Don't open e-mail attachments from anyone you don't know—and be wary of those from people you do. Some viruses spread by mailing themselves to contacts in an infected computer's address book. If you have any doubts about the safety of an attachment, check with the source before opening it.

By using discretion, keeping your antivirus software up-to-date, and erring on the side of caution, you can help correct and protect the health of your computer system. Prevention is often the best medicine.

Members Email Addresses

Ruth Donahue-Allisonr	allison98@juno.com
Jim Ashworth	Blue_unicorn@netzero.com
William & Diane Brumbachb	brumbach@cs.com
Linda Busch	lindashrub@juno.com
Bob Carpenter	cubs14@ripon.alumlink.com
Tom Fitzsimmons	tomfitzsimmons@juno.com
Jack Frost	jfrost@megsinet.net
Richard Graling	mtndew@mc.net
Mr. G	mrG3165@aol.com
Phil Grimm	pgrimm4@attbi.com
Arnie Gudyka	arngood1@juno.com
Terri Hanlon	Terhanlon@aol.com
Henry Henriksen	bruisarandziggy@aol.com
Marshia Hobson	marsgraphics@netscape.net
Dwight (J.J.) Johnson	jj1450xl@ix.netcom.com
Donna Kalinoski	donnaleek@juno.com
Steve Kostelnik	steve_kostelnik@usa.net
Lester Larkin	LesLarkin@NetZero.net
John Lawless	jay@iwc.net
Mark McDonald	markym36@aol.com
Mike McEnery	mmcenery@core.com
John Nabors	jog@nomad.net
Lee Nordstrom	LeeNord@mw.sisna.com
Marcia Rose	Mrose74801@aol.com
James Rutledge	jrutnet1@home.com
Leslie Salsburg	leslie164@juno.com
Paul Schintgen	paulj@theramp.net
Walter Sheets	eddoc85@netzero.net
Gerald Straw	ilotgks@concentric.net
Grace Vogt	gracemvogt@msn.com
Steve Yeaton	hiflyer9@bigfoot.com

As much as we try, we do make errors. Please advise us if there is a mistake in your E-Mail address or if it is not included in this listing. Send E-Mail to editor@lcace.org with the additions and/or corrections. Thank you. This listing last updated – April 1, 2002

L.C.A.C.E. HOTLINE
**Call: 847-623-3815
or
fax: 877-349-4080**

Http://www.lcace.org

Member's Web Sites

TIME TO RENEW

If it is time for you to renew your membership, please fill out a new Application and a Member's Profile Sheet. These forms can be obtained at the meetings or downloaded from our WEB site.

Your Advertisement Should have been placed here.

L.C.A.C.E.
c/o Group Ambassador
409 S. Elmwood Ave.
Waukegan, Illinois 60085-5219

See the **CLUB PICURES** at:

Take a good look, you just might see yourself.

http://lcace.org/photoAlbums.htm

L.C.A.C.E Online
View our Site
http://www.lcace.org
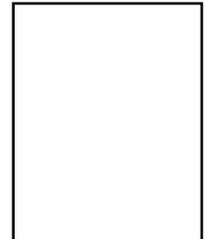
E-Mail Us At:
Web-master

webmaster@lcace.org

Sign the Guest Book and tell us what you think
- LCACE E-mail addresses
- LCACE information
- LCACE history and pictures
- LCACE meeting, location and map
- LCACE members e-mail addresses
- LCACE online membership application

NEXT MEETING
February 8, 2003
Grayslake Public Library
12:00pm—3:00pm
Meeting Room Opens 1200
This month:
MP3 Player + USB Flash Drive
Presented by
PINGTEC

**Reminder The March is
March 1, 2003**
(rescheduled meeting date)

L.C.A.C.E
Lake County Area Compuer Enthusiasts
409 Elmwood S. Ave.
Waukegan, IL 60085-5219

ADDRESS CORRECTION REQUESTED