THE LOS ANGELES COMPUTER SOCIETY NEWSLETTER

Volume 42 Issue 10
October 2024

User Friendly

LACS
A Computer and Technology User Group

IN THIS ISSUE

Watch your email for APCUG workshops and other upcoming events.

LACS IS A MEMBER OF APCUG

An International Association of Technology and Computer User Groups

www.apcug2.org
www.facebook.com/APCUG
www.X.com/apcug **(Twitter)**

TUESDAY, OCTOBER 8, 2024
GENERAL MEETING

Topic: Are you prepared for the Big One?
Speakers: Mark and Marsha Presky, LACS members. with Jose Morataya
Meeting Time: 7:00 to 9:00 PM — via Zoom
Socializing and Questions & Answers: 6:30

The Community Emergency Response Team (CERT) was developed by the Los Angeles Fire Department after examining the civilian responses to Japanese and Mexico City earthquake disasters in 1985. Over 100 untrained volunteers died due to the Mexico City earthquake. Neighborhood fire departments train volunteers for free. CERT training includes first aid, victim medical triage, search and rescue, cribbing, two-way radio training, terrorist response training, and setting up a command post, staging area or morgue. You could join the **Neighborhood Team Program (NTP)** which helps neighbors prepare for mass casualty disasters. We know that a major earthquake will hit Southern California. We just don't know when. How should you prepare? Mark, Marsha, and Jose will help you learn.

Meet Our Presenters

Jose Morataya is the Los Angeles City Battalion 4 CERT coordinator for Mar Vista, Westchester, Playa del Rey, Venice, and Playa Vista. He was the warehouse operations manager for Volkswagen. Mark, a LACS director, and Marsha, have taken CERT courses from the L.A. Fire Department. Mark graduated from UC–Davis and worked in pathology for the UCLA and Tarzana Medical Centers for many years.

LACS members on the PC groups.IO list will receive the Zoom link to this meeting before or on **October 6**. Just click on it to enter the meeting. Guests may ask for the link by emailing Leah Clark at leahjc@sbcglobal.net before or on **October 6.** See pages, 8, 9, 10, and 20 for help in using Zoom, or email Leah with questions. See more information about LACS at www.lacspc.org.

FROM YOUR PRESIDENT / EDITOR

NATIONAL CYBERSECURITY AWARENESS MONTH

The U.S. President and Congress have declared October as National Cybersecurity Awareness Month. This is an effort between government and industry to ensure every American has the resources they need to stay safer and more secure online.

This issue of User Friendly is dedicated to cybersecurity issues. LACS members, please keep safe out there.

LACS ELECTIONS

On pages 4 and 5 of this issue, see bios and pictures of the candidates willing to run for another term on the LACS board. Many thanks to them. Voting will take place at our November general meeting on November 12. Nominations will be taken from the floor on October 8.

We still have openings for a board secretary and two director positions. We especially need a secretary to stay in compliance with our 501(c)(3) non-profit status. We can't keep LACS a viable organization without volunteers.

A HINT

I was receiving much spam in my email spam folders. Then I tried clicking on "Block Sender" rather than just deleting the spam. The amount of spam I'm now getting is much less.

GROUPS.IO

Stephanie Nordlinger, our vice president and program chair had set up our Groups.io mailing list about five years ago and has been managing it ever since then. We cannot thank her enough for all her diligent work to keep our group's communications on track.

Larry McDavid, one of our newer members, has agreed to continue Stephanie's work. He was one of four founders of the North Orange County Computer Club and is active in numerous technical societies and local clubs. He owns and manages numerous Groups.io groups, including one with nearly 4,000 international members. Larry is active on the Groups.io Group Moderator's Forum and on the groups.io Beta test Group. We thank him for becoming our Groups.io manager and welcome him.

REQUESTS

1. We are now only using this address to communicate to our Groups.io mailing list: **pc@lacs.groups.io**. Use it send communications to all members of LACS.

Do **NOT** use the previous address of LACSList.groups.io. It is no longer active.

2. If you receive an email from the **Groups.io list** that appears to be Spam or is something you're not interested in, please **do not** mark it as spam. That will cause you to be deleted from the list. Just **delete** the message and **do not** mark it as spam. That will save us the bother of reinstating you. Thank you.

HALLOWEEN HISTORY

Halloween roots are in Celtic traditions. They celebrated their new year on November 1. On October 31, they celebrated Samhain, when they believed that the ghosts of the dead returned to earth. They would light bonfires and wear costumes to ward off these roaming spirits. This day marked the beginning of the cold, dark winter, associated with human death. In 835 A.D., the Christian Church set November 1 as *All Saints Day* to replace the Celtic holidays. The eve of All Saints Day became known as All-Hallows Eve and eventually, Halloween. It is still celebrated with bonfires, parades, and costumes.

GENERAL MEETING REPORT

September 11, 2024

By **Leah Clark,** LACS President/Editor

Internet Privacy
Mark Schulman

Mark spoke about browser privacy, VPNs, and email privacy.

Internet Browsing

What are the possibilities your personal data will leak out when browsing a website? When you use a router, you broadcast information over the airways. From there, it is sent to your Internet Service Provider (ISP), which then sends your request to the Internet. From there, it makes its way to the website server you are contacting.

People can rummage through your computer, see the websites you have been to, and dig a lot of information from your browser. People on your network can see where you are and where you're going. They can't see your data but can know who you are talking to. This enables "Bad Guys" to target you with phishing attacks.

ISPs can tell what websites you are going to and get information about you. As your information goes through the internet, it travels through many different servers where it can be snooped into. The websites you go to collect information.

Browser Privacy

If your computer is somewhere others can access it, they may snoop around. If you should use someone else's computer, you don't want to leave information in your browser. Mark explained that you should use your browser's **private or incognito mode**. It does not store information and cookies about where you have been. But, your ISP and the websites you visited will know where you have been.

Mark then demonstrated using a **portable browser** on a thumb drive. Install this software on a flash drive, then plug the flash drive into the computer you are using. All your information, cookies, etc., will be kept on the thumb drive. You must download the **portable version** of your browser to the flash drive. All of the history of where you have been is stored on the flash drive. No personal data is left behind on the computer you are using. It does not prevent the ISP from spying on your local network. You can get it from https://Portableapps.com. They have many other applications you can run from a flash drive.

Using a Secure Browser

The most popular browser is Chrome, but Mark doesn't always trust it. He likes five browsers: Vivaldi, Chromium, Firefox, Waterfox, and Brave. Mark has the links to these at the end of his presentation.

HTTPS Tip

When browsing, look for the little lock symbol; it is essential to protect your privacy. Be sure the address begins with HTTP**S**. This means all your information is encrypted between your browser and the server. A snooper can still see what websites you're going to. In most browsers today, you can force all your traffic to HTTPS.

Public Wi-Fi Tips

- Be sure HTTPS is turned on.
- Anyone using the same public Wi-Fi, including in hotels, can see the websites you are going to.
- Turn off your Wi-Fi when not in use when in public.

Search Engines

Mark said that DuckDuckGo and Startpage don't collect data like Google does.

VPNs

There are many VPN providers. The VPN service you are using puts them on the internet, so you are actually talking to them. Everything along the route is encrypted. Anyone snooping along the way cannot see what you are doing.

If you run https://whatsmyip.com , you can see your IP address, where you are, etc. If you run your VPM, you can tell it what country you want to be located in. It will look like you are in your chosen country and give you a different IP address. You may be able to watch TV from another country even if it's not available where you are by telling your VPN you are in that country.

Some VPNs may collect your data. Find a VPN company you can trust. Mark discussed some of the dark sides of VPNs and how to avoid a VPN company you can't trust. He recommended five VPN companies that have gone through and passed security checks.

VPNs don't protect you from malware and scams, make you anonymous if you log in, and have anything to do with email.

Email Privacy

The first thing to know about email privacy is that there isn't any. Email messages are not encrypted. Consider a secure email provider like Proton Mail, Startmail, Tutanota, or Zoho Mail to get around that. To be sure your email is secure, use an **encrypted attachment**. Put your information into a document, encrypt it, and attach it to your email. The receiver can decrypt it to see it. You and the recipient need a password to do this. Mark showed us how to do this.

A **Disposable Email Address** gives you an email address to use in place of your own for a short time. Mark likes 10minutemail.com and fakemail.net. It's handy when you submit your email address to get one thing you want without being bombarded with spam emails from the site. Mark demonstrated it.

Mark's last slide shows the links to sites discussed in this presentation.

Time was running out, so Mark can present Encryption at another time. LACS members and guests received the slides and the recording of this excellent presentation. See them for details not covered in this report. ❖

LACS BOARD NOMINEES FOR 2025

A board secretary is desperately needed.

We are grateful for the following officers and directors who have graciously agreed to serve for another term. We wholeheartedly thank them for their dedication.

LEAH CLARK, PRESIDENT, INCUMBENT

I joined LACS in 1998 after meeting a member at an RV park in Soledad Canyon, CA. That was soon after I retired from working as a Clinical Laboratory Scientist at UCLA for 43 years. My late husband, Joe, and I saw much of the USA in our motor home. LACS has kept me busy with volunteering and constantly learning new things. I have been welcome chair, director, secretary, and Genealogy SIG leader. I am now president and newsletter editor. This has enabled me to learn, make friends, and have fun.

STEPHANIE NORDLINGER, VICE PRESIDENT, INCUMBENT

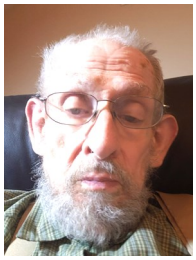
The Vice President invites general meeting speakers and may stand in for the president. My aim is to have varied and stimulating programs to interest and inform people. I welcome your input. I want to give this job to another member because organizations are better if they get new officers from time to time. LACS's wonderful members have taught me many better ways to use PCs and other technologies.

I joined the UCLA PC Users Group by 1985 and helped to incorporate LACS in 1991. I have been its President, VP, Editor, Counsel, Smartphone SIG Leader, author, product reviewer, and Groups.IO Coordinator. A nearly retired attorney, I would like more time for my other hobbies.

GAVIN FAUGHT, TREASURER, INCUMBENT

My name is Gavin Faught, and I'm looking forward to my fifth year as Treasurer of LACS. I do have other leadership experiences. At UC Davis, my alma mater, I was Vice President for the fraternity Phi Beta Lambda and at CSU Sacramento, I was Treasurer for the Accounting Society. Computer topics that interest me are information technology (IT), cybersecurity, and cloud computing. I have recently completed a UCLA Cybersecurity Boot Camp, and I have learned quite a lot from the experience.
My hobbies include playing and recording music and working out. I am looking forward to making LACS the best it can be.

IRV HERSHMAN, DIRECTOR, INCUMBENT



My journey to being a Director for LACS started as a boy; I got a crystal set and tuned in the AM stations that I could receive.
Next I became a Cub then a Boy Scout. I attended Scout Camp. When it ended the scouts used a phone patch at the radio shack to phone my parents to tell them when and where I would be arriving in Phoenix where my family lived. I became a radio amateur operator and obtained an FCC (Federal Communications Commission) Commercial First and Second Class Licenses. I look forward to continuing as a Director.

PAULA VAN BERKOM, DIRECTOR, INCUMBENT

I have a certificate of completion in Computer Science from WLA College. As a member of LACS, I have taken part in the Basics & Beyond and other SIGs. I have volunteered teaching computers to seniors at Emeritus Santa Monica College and at the computer Lab at Culver City Senior Center. I have learned much from LACS and have decided to share all this knowledge with the community by returning to the Board for another term as a director. As a member, I plan to reach out to our members and to other computer users to expand our scope of activities. I trust that you share my confidence in making LACS a premier computer user group.

LACS 2025 BOARD

LACS has an urgent need for a secretary, and there are two openings for directors. You are needed and wanted.

The LACS 2025 board members would greatly appreciate the support of our members in various ways, including suggestions for program presenters, contributions of articles for *User Friendly*, ideas for activities, or arranging special interest group meetings (SIGs). Any form of assistance would be highly valued. Let's work together to share the workload rather than burdening just a few individuals. With members' help, We are looking forward to a good year in 2025.

IS ONLINE BACKUP A GOOD IDEA?

It depends on what you're backing up. In general, it's unlikely to be enough.

By **Leo A. Notenboom**
The Best of Ask Leo, askleo.com

Backing up data using an online backup service can be an essential part of an overall strategy, but there are significant limits and considerations.

Online backup services can be a useful component of a broader backup strategy. There are several factors to consider, including security, completeness, speed, and cost, before deciding if online backup is right for you.

Online Backup

Online backups are convenient but not enough. They can be slow, incomplete, and vulnerable to security risks. Use them as part of a broader backup strategy, including local full-image backups, to ensure protection of your data. Of course, the best backup strategy is the one you'll consistently use.

The Cloud

"Moving to the cloud" is a popular buzz phrase, and online backup is one of the poster children of the concept. With ubiquitous connectivity, why not store essential data on servers on the internet—in the cloud?

By using third-party internet services and servers, you can keep all your mail on line. Your documents on line (Google Dos and Microsoft are two examples), and more. The advantage is that with a computer and a browser, you can access your documents from just about anywhere and be less concerned about system and software crashes on your machine.

So, if "the cloud" is such a good place for your data, is it also a good place for the backup of your data?

It's an option if used properly, but there are concerns to consider.

Online Backup Isn't Practical for Everything.

It's just not practical to back up everything thing on line. For example, uploading a complete imager backup of your machine would take days, if not weeks. This is because of your internet's limited upload speed.

Most online backup services ignore your system and back up only your data. Even then, you need to be careful to ensure they're backing up what you think they are. If you keep data outside of the default Documents folder, you may have to take extra steps to tell the service to back that as well.

The implication is simple: if you have a major system failure and lose everything, your online backup won't help restore your machine. It'll restore your data after you've rebuilt your machine and reinstalled the operating system and applications. It's a valid choice, but you need to be aware of it.

An Online Backup Requires Being Online

This might sound obvious, but many times, it's not: you must be online for an online backup to work.

If you add a lot of data — say a day's worth of active photography — that data will take time to upload and be backed up. If you turn your computer off at the end of the day and those photos have not yet been uploaded, they aren't backed up. They may automatically resume uploading when the machine is next turned on, but until then, if anything happens to that machine or hard disk, you risk losing them.

This is a common scenario when traveling with limited and slow connectivity. It's easy, particularly with photos, to accumulate data faster than you can back it up.

An Online Backup is...Online

Your backup is in the cloud. That's kinda the point, right? Accessible from anywhere? From any computer?

The risk is the same risk you run when using any online service: if someone steals your account information, they have access to whatever you've stored in the cloud. If you've been backing things up online and your backup account is compromised, the attacker could have access to everything.

The good news here is that this is something within your control; it goes back to Basics of Online Account Management and Safety at < https://askleo.com/12-steps-keep-getting-account-hacked/ >.

Use good, strong passwords; don't write them down; don't use the same password for multiple purposes; use a password vault; use two-factor authentication; don't share with people you don't absolutely trust; stay safe in open Wi-Fi hotspots; avoid malware, and so on.

The steps to keeping your online information safe are relatively easy, but the cost of failure can be fairly high.

An Online Backup Is on Someone Else's Computer

Many people complain about the security of their data apart from the security of their accounts. Those concerns typically fall into three categories:

- Your data will be exposed should the online backup service be hacked, as I mentioned above.
- Your data will be exposed should the online backup service receive a warrant or other demand from a law enforcement agency or other government entity.
- Your data will be exposed to the online service itself, who then might use it for purposes unknown.

Depending on where you live, where the online backup service is located, and the sensitivity of your data, these can be valid concerns.

As long as you stick with reputable online backup services, the technology typically encrypts your backups so that no one but you can see them. If you're still concerned, you can take the extra step of encrypting the data yourself.

Do This

So is an online backup a good idea? In my opinion, yes, **but only as part of a larger backup strategy**.

Start with a periodic full image backup of your computer. This way, you know everything is backed up. Should your hard drive ever die completely, you won't be faced with reinstalling the operating system and all your applications from scratch; you just restore the backup.

Then consider adding an online backup of your data. Depending on your approach, this could result in nearly real-time continuous backup of your data, or it could be an alternative to running your local backup program every day. When something goes wrong — from an accidentally deleted file to a destroyed computer (or even home) — you know that your *data*, at least, is safe.

I strongly recommend against using *only* an online backup service. And, to quote one of my earlier articles, "the best backup strategy is whatever you'll actually use" — so if online is the technique you'll actually use, use it.

Also, subscribe to Confident Computing at https://newsletter.askleo.com/ for less frustration and more confidence, solutions, answers, and tips in your inbox every week. ❖

LACS INFORMATION

HOW TO JOIN LACS'S MAIL LIST

LACS has an active general email list: PC@LACS.Groups.IO which goes to all members on the list. Members will receive meeting notices and Zoom links via this list. You can also ask questions, offer suggestions, and help others.

New LACS members should receive an invitation to join our list with two weeks to accept. Other LACS members who want to join the list should send an email to Larry McDavid, our Groups.IO Coordinator. (See your roster for contact info.)
He will send you an invitation to join. If you have any problems or questions about joining, please contact Larry.

USING PAYPAL OR ZELLE

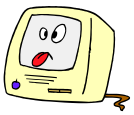
To pay LACS by PayPal, go to this link: www.paypal.com/paypalme/00001024 and then click on **Send**. Log in to your PayPal account or sign up for an account so that PayPal will know where to get the money to send. Follow the prompts. Enter the amount to pay, then click on **Add a note**. Say what the payment is for. If is for dues, add any updated information: physical and email addresses, phone number, and your dues type (regular, electronic , etc.) and if you don't want your contact information to be in our roster.

To pay LACS by Zelle, log into your bank with your username and password.

Select **Transfer Money > Send Money with Zelle.** Follow the instructions. The recipient is **Los Angeles Computer Society.** Select **Send by email**. The email address is: **lacomputersociety@gmail.com**. The wording may be a little different on your bank's site.

Email questions to Gavin Faught. See our roster for contact info.

FIX YOUR PC FOR FREE?



LACS member and presenter, **Jim McKnight**, has an open offer to LACS members to diagnose, repair, disinfect, or upgrade members' PC's for free. There are certain limitations to Jim's offer, so see the details by clicking the "Fix my PC for Free?" link at www.jimopi.net.

Non-members can wisely invest in a one-year **new regular** LACS membership ($40.00), and Jim will fix your PC problem, too. Contact Jim for specific considerations.

CHANGE CONTACT INFORMATION

Go to www.lacspc.org. Click on **Join LACS** in the bar under the picture. Under **Membership Update,** select **Click Here** to select either the DOC or PDF form. Fill it out; email it with your changes to Leah Clark. See the LACS roster or pages 9 or 10 of UF.
Or snail-mail it to
Los Angeles Computer Society
11664 National Blvd. #343
Los Angeles, CA 90064-3802.

ATTENDING A ZOOM MEETING

LACS members who are on our PC email list will receive a link, meeting ID, Passcode, and instructions to attend the LACS general meetings a few days before the meeting. **Please let Leah Clark know by the morning of the meeting if you don't have it or have a problem.**

You can put an icon to the link on your desktop so it's handy at meeting time.

1. Right-click a blank spot on your desktop.
2. Select **New** from the drop-down menu.
3. Select **Shortcut**.
4. Type or copy and paste the link in the box that says "Type the location of the item."
5. Click **Next**.
6. Type a name for the shortcut.
7. Click **Finish**.

LACS CALENDAR

LACS Board Meeting, Monday, October 7
Time: 7:00 P.M. (Open from 6:30 P.M.)
Place: Wherever you are via Zoom

LACS General Meeting: Tuesday, October 8
Time: 7:00 P.M. (Open from 6:30 P.M.)
Place: Wherever you are via Zoom

Please log in early so we can start on time. Allow time to be sure you have the link, to get or update your Zoom software if you have not used it before or recently, or to solve other issues before the meeting starts.

October 2: Rosh Hashana
October 11: Yom Kippur
October 14: Indigenous Peoples Day
October 31: Halloween

VISIT OTHER APCUG COMPUTER USER GROUPS AND SEE THEIR NEWSLETTERS

LACS heartily welcomes visitors from other user groups, and we are welcome to join other groups' meetings.

Go to www.APCUG2.org . Click on **Member Benefits**, then on **Groups Sharing Meetings** or on **Newsletters Online**.

UPCOMING MEETINGS/EVENTS

October 8: Are You Prepared for the Big One?, Mark and Marsha Presky with Jose Morataya

November 12: Encryption, Mark Schulman

December: Holiday Luncheon Party

Please watch your email and *User Friendly* for changes and updates.

ZOOM MEETINGS

Members on our PC email list will receive, via email, an invitation to join LACS Zoom general meetings. Click on the URL in the invitation before the meeting and follow the prompts.

If you have any questions or if you don't receive the link by the morning of the meeting day, contact Leah Clark at

leahjc@sbcglobal.net

ZOOM RECORDINGS

LACS members and meeting guests will receive links to the recordings of Zoom meetings via email.

HYPERLINKS

Underlined text (blue in the color edition) in User Friendly usually means it's a hyperlink to a website. Click on the link in the online version to see the referenced place. You can also copy and paste it into your browser's search or address bar.

USER FRIENDLY BACK ISSUES AND INDEXES

To see back issues of *User Friendly,* go to http://www.lacspc.org/category/user-friendly/.

For indexes to past issues, go to https://www.lacspc.org/category/uf-index/

To find a specific article or topic, use the search box on the top right.

MEMBERS HELPING MEMBERS

LACS members volunteer to help other members solve hardware and software problems by telephone or during the hours listed below. Select the topic from the list and then contact a person whose number is listed next to it.

Find a helper's email address and phone number on your roster. If you don't have your roster, call 424-261-6251. Only members in good standing may receive a roster. We hope you find this LACS free service useful.

If you are experienced using a particular program or hardware, please volunteer to be a consultant. You don't have to be an expert. To volunteer for this list or to make corrections, please email Leah Clark at leahjc@sbcglobal.net or call her at 424-261-6251.

Adobe Creative Suite: PDF, InDesign, Photoshop, etc. - 10
Android Smartphones - 8
Apple devices - 11
Anti Malware and Backup - 7, 8
Dragon Naturally Speaking - 3
Genealogy - 8
Groups.IO - 8
Hardware - 7
Lotus Word Pro, Approach - 7
Mozilla Firefox - 7
MS Excel - 8, 11, 12
MS Word - 1, 3, 8, 12
MS Outlook - 1, 8, 10
MS PowerPoint - 8, 11
MS Publisher - 2
PDF - 8
Photoshop - 10
Quicken - 8, 12
Thunderbird - 7
Utilities - 7, 8
Windows - 7, 8
WordPerfect - 8
Zoom - 2, 9

Preferred Time for Phone Calls			
Number	Name	From	To
1	Beckman, Loling	10:00 AM	6:00 PM
2	Clark, Leah	7:00 AM	5:00 PM
3	Hershman, Irv	11:00 AM	11:00 PM
7	McKnight, Jim	8:00 AM	7:00 PM
8	Nordlinger, Stephanie	9:00 AM	5:00 PM
9	Presky, Mark	Any	Any
10	Rozek, E. J.	Noon	8:00 PM
11	Van Berkom, Paula	9:00 AM	5:00 PM
12	Wilder, Joan	9:00 AM	9:00 PM

Note: Times are Pacific Times

OFFICERS, DIRECTORS AND LEADERS

TITLE	NAME	TERM
President	Leah Clark	2024
Vice President	Stephanie Nordlinger	2024
Secretary	**Open**	2024
Treasurer	Gavin Faught	2024
Director	Loling Beckman	2025
Director	Donna Benton	2025
Director	Mark Presky	2025
Director	Irv Hershman	2024
Director	**Open**	2024
Director	**Open**	2024
Director	Paula Van Berkom	2024
APCUG Representative	Leah Clark	
Corporate Counsel	Stephanie Nordlinger	
Database Manager	Loling Beckman	
Groups.IO Email Lists	Larry McDavid	
Newsletter Editor	Leah Clark	
Program Chair	Stephanie Nordlinger	
Publicity – Press	Mark Presky	
Publicity – Online Media	Open	
Quick Consultants	Leah Clark	
Webmaster	Paula Van Berkom	

Mailing Address: 11664 National Blvd., #343, Los Angeles, CA 90064-3802

Website: https://lacspc.org

Contact the President/Editor at 424-261-6251. Follow the prompts. This is a Google Voice number.

Please use your LACS roster for email addresses and phone numbers to contact any officer, board member or other member. If necessary, you may leave a message at the above number. **Only LACS members may receive a roster**.

Please note: The 2024 roster was in the middle pages of the May User Friendly. It was mailed to all LACS members, including those who usually receive only the electronic version. The roster will not be sent to anyone electronically. Be sure to keep it where you can find it when you need it.

HOW TO TELL IF YOUR COMPUTER HAS A VIRUS AND WHAT TO DO ABOUT IT

From the National Cybersecurity Alliance

Computer viruses make your devices sick, but you can usually help them heal if you act fast.

Since the first malicious, self-copying computer code, "Brain," was unleashed in 1986, viruses have caused headaches for many of us. Some viruses brick your devices and make them impossible to use, but more often viruses slow down your computer or steal your data. But you can take steps to boot a virus off your machine.

Since 2020, we have all likely become familiar with how real viruses and computer viruses mimic disease-causing viruses like influenza or COVID-19. They are highly contagious and can easily jump from a computer to other devices or networks. When battling a computer virus, your poor device feels run down and requires more rest than usual – it probably has difficulty performing even the simplest of daily tasks!

Like the real thing, computer viruses replicate themselves, spreading through your operating system and network. At the same time, the virus is wreaking havoc: it can damage programs, delete files, and make devastating changes to your hard drive, all of which can result in reduced performance. Some viruses will even crash your entire system. Viruses can also give their cybercriminal creators a backdoor to destroy or steal your sensitive data and documents.

The idea of having a virus on your computer is scary, but we're here to help! Here we've gathered tips on preventing, detecting, and defeating computer viruses.

How does a computer get a virus?

The most common reason your computer will get infected is because you downloaded or installed infected files. Pirated media and free games are common culprits, and so are phishing attacks where you click on a bad link, button, or email attachment. Once clicked, the virus or other malware installs itself. Similarly, viruses can infect your computer when you visit scam websites. Sometimes, you can unintentionally install a virus from an infected external drive, like a USB stick.

How do I tell if my computer has a virus?

If you notice any or all these symptoms, your computer might have a virus: you should act:

- Suddenly slow computer performance, meaning it takes a noticeably longer time to start up or open programs
- Problems unexpectedly shutting down or restarting
- Missing files
- Frequent system crashes
- Frequent error messages
- Unexpected pop-up windows
- New applications (like web browser toolbars) that appear without you downloading them
- Overworked hard drive, which you can detect if your device's internal fan seems to be whirring and working hard when you aren't doing much
- Emails that send automatically from your accounts without you sending them
- Lagging web browser, or your web browser constantly redirects
- Malfunctioning antivirus programs or firewalls

I think my computer has a virus! What do I do?

If you think your computer has a virus, you should act fast to try to irradicate the malicious code. Don't panic – we've broken down what you should do into a few easy-to-understand steps. If you can read this webpage from your device, you can probably save your computer and data.

1. Run a full system scan

If you suspect your computer has a virus, use antivirus software to run a full system scan of your device. It is best to set your antivirus program to do this automatically regularly so you can detect any issues before they become emergencies. Review the detected threats and take any action you can – many antivirus and antimalware programs guide you through this.

2. Restore to an earlier back-up

If you cannot delete the virus or infected files, try restoring your computer to an earlier backup before you began having problems. Then, scan your system again with antivirus software and see if the same issues exist.

3. Delete temporary files

Delete all the temporary files on your computer. How you delete these files is usually easy, but it depends on your operating system (like Windows or macOS). If you search for information for your specific system, you can find detailed information.

4. Go Safe Mode

If you are prevented from deleting files because your computer is malfunctioning, try booting up in "Safe Mode." Safe mode restricts certain programs so you can work to fix the issue without interruption.

5. Reinstall your operating system

As a final measure to get rid of a computer virus, you can reinstall your device's operating system (such as Windows or macOS). This can result in the loss of important files or other data. At this point, taking your device to a computer store and seeking professional help is a good idea. Many shops or experts will at least guide you through the process of reinstalling your operating system for free.

The only way to ensure that you eliminate a virus is to wipe your device and reinstall a new operating system on the machine.

- This is a good reason to practice good backup habits because the process (called "reimaging") eliminates everything on the hard drive (both the virus files and all of your files).
- Depending on the severity of the issue, you might be able to deal with malware or a virus without taking this step (by using a quality antivirus software or going into Safe Mode and removing bad files, for example). Still, reimaging is the most effective option to be close to 100% sure that the virus is removed.
- There have been rare instances where a computer virus survives reimaging. If youre considering this drastic step, you should consult a tech professional.

How To Prevent Computer Viruses

Just like with your immune system, an ounce of prevention is worth a pound of cure when it comes to computer viruses.

1. Use antivirus software

You should always have a trusted antivirus installed on your computer. It is best to boot up some antivirus software as soon as you start using a new device. You should be able to turn on regular

scans of your entire device so you know if there are any issues ASAP.

2. Follow the Core 4

By following four basic cybersecurity behaviors, you can forge good habits that make it tough for computer viruses to get through.

- Use complex passwords that are at least 12 characters long and are unique to each account; use a password manager to store all your passwords securely.
- Turn on multi-factor authentication (MFA, sometimes called 2-factor authentication) for any account that permits it.
- Turn on automatic updates for your hardware, software, and apps.
- Learn how to identify phishing – don't take the bait!

3. Be careful on public wi-fi

Public wi-fi in cafes, airports, and other businesses can be convenient, but these networks are often unsecured and leave your phone, tablet, or computer susceptible to viruses. A personal mobile hotspot or VPN (virtual private network) is a more secure way to connect when you are on the go.

4. Get your software fresh from the source

One of the oldest tricks in the cybercriminal's book is to sneak viruses and mal ware into software and files people want to ate. Always download software from verified sources and get all your apps from your de vice's official app store. You might think you're saving some money by pirating soft ware, movies, or other media, but you are al so putting your expensive device and net work at risk!

FOUR EASY WAYS TO STAY SAFE ONLINE

From the National Cybersecurity Alliance

Let's work together to build a safer digital world. We can increase our online safety through four simple actions, and whether at home, work, or school, these tips make us more secure when connected. Discuss them with family, friends, employees, and your community to become safer online!

Recognize & Report Phishing

Be cautious of unsolicited messages asking for personal information. Avoid sharing sensitive information or credentials with unknown sources. Report phishing attempts and delete the message.

Stay Safe with Three Simple Tips

1. Recognize

Look for these common signs:

- Urgent or emotionally appealing language, especially messages that claim dire consequences for not responding immediately
- Requests to send personal and financial information
- Untrusted shortened URLs
- Incorrect email addresses or links, like amazan.com

A common sign used to be poor grammar or misspellings, although in the era of artificial intelligence (AI), some emails now have perfect grammar and spelling, so look out for other signs.

2. Resist

If you suspect phishing, resist the temptation to click on links or attachments that seem too good to be true and may be trying to access your personal information. Instead, report the phish to protect yourself and others. Typically, you'll find options to report near the per-

son's email address or username. You can also report via the "report spam" button in the toolbar or settings.

3. Delete

Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. Just delete.

Use Strong Passwords

Simple passwords, such as 12345, or common identifying information, like birthdays and pet names, are unsafe to protect important accounts with personal information. Using an easy-to-guess password is like locking the door but leaving the key in the lock. Computer hackers can quickly break weak passwords. But it's impossible to remember a unique, strong password for every account!

The good news is that creating and storing strong passwords with the help of a **password manager** is one of the easiest ways to protect ourselves from someone logging into our accounts and stealing sensitive information, data, money, or even our identities.

Strengthen Your Passwords with Three Simple Tips. A strong password follows ALL THREE of these tips.

- **Make them long**—at least 16 characters—longer is stronger!
- **Make them random**—Use a random string of mixed-case letters, numbers, and symbols. For example:
  - cXmnZK65rf*&DaaD
  - Yuc8$RikA34%ZoPPao98t

Another option is to create a memorable phrase of 4–7 unrelated words. This is called a "passphrase." For example:

- Good: HorsePurpleHatRun
- Great: HorsePurpleHatRunBay
- Amazing: Horse Purple Hat Run Bay Lifting

Note: *You can use spaces before or between words if you prefer!*

- **Make them unique**

Use a different strong password for each account. For example:

- Bank: k8dfh8c@Pfv0gB2
- Email account: legal tiny facility free hand probable enamel
- Social media account: e246gs% mFs#3tv6

PRO TIP: USE A PASSWORD MANAGER

It's hard to remember all these strong passwords, and we don't want to save them in a file on a computer. Instead, use a password manager. See below!

Use a Password Manager

For most people, generating and remembering long, random, unique passwords for every account is impossible. Rather than write them down, use a password manager! A password manager is an easy-to-use program that generates, stores, and even fills in all your passwords. Password managers tell us when we have weak or re-used passwords and can generate strong passwords. They can automatically fill logins into sites and apps as we move from one to another.

When we use a password manager, we only need to remember one strong password—the one for the password manager itself.

Tip: *Create a memorable long "passphrase" as described above.*

There are many password managers to choose from. Some are free, like the built-in password managers in your web browser, and some cost money. Search a trusted source for "password managers," like Consumer Reports, which offers a selection of highly rated password managers. Read reviews to compare options and find a reputable program for you.

When we use a password manager, we are much more likely to use a long, random, and unique password on every site. And that makes it much harder for someone to steal our valuable information!

PRO TIP: Check whether your email accounts, banks, healthcare providers, and other important accounts enforce strong password requirements. If they let you use a short password or a dictionary word, ask them why. It's your information they're putting at risk!

Turn On MFA

Having more than a password to protect your online accounts would be best. Enabling multiple-factor authentication (MFA) makes you significantly less likely to get hacked. Enable MFA on all your online accounts that offer it, especially email, social media, and financial accounts.

Follow these Easy Steps to turn on MFA for each account or app!

1. Go to Settings. It may be called Account Settings, Settings & Privacy, or similar.
2. Look for and turn on MFA. It may be called two-factor authentication, two-step authentication, or similar.
3. Confirm.

Select which MFA method to use from the options provided by each account or app. Examples are:

- Receiving a numeric code by text or email
- Using an authenticator app: These phone apps generate a new code every 30 seconds. Use this code to complete logging in.
- Biometrics: This uses our facial recognition or fingerprints to confirm our identities.

Now that we've set up MFA when we log into our accounts, it may challenge us to complete the MFA step that proves our identities. It only takes a moment but makes us much safer from hackers!

Turn on MFA for every account or app that offers it. Enabling MFA will protect things like banking information, online purchases, social media, email, businesse, and your identity. PRO TIP: Check whether your email accounts, banks, healthcare providers, and other important accounts offer MFA and enable it by default. If they don't, ask them why not. It's your information they're putting at risk!

Update Software

Ensuring your software is up to date is the best way to ensure you have the latest security patches and updates on your devices. Regularly check for updates if automatic updates are not available.

Think Twice Before Putting Off Updates!

Many people might select "Remind me later" when they see an update alert. However, many software updates are created to fix security risks. Keeping software up to date is an easy way to stay safer online. To make updates even more convenient, turn on the automatic updates in the device's or application's security settings!

Be sure software is up to date with three simple Steps:

1. Watch for notifications

Our devices will usually notify us that we need to run updates. This includes our devices' operating systems, programs, and apps. Installing ALL updates is important, especially for our web browsers and antivirus software.

2. Install updates as soon as possible

When notified about software updates, especially critical ones, we should install them as soon as possible. Malicious online criminals won't wait, so we should not either!

3. Turn on automatic updates

With automatic updates, our devices will install updates without any input from us as soon as the update is available—Easy!

To turn on the automatic updates feature, look in the device's settings, possibly under Software or Security—search settings for "automatic updates" if needed. ❖

RESOURCES AVAILABLE TO YOU

From the National Cybersecurity Alliance

If you discover that you have become a victim of cybercrime, immediately notify authorities to file a complaint. Keep and record all evidence of the incident and its suspected source.

The list below outlines the government organizations you can file a complaint with if you are a victim of cybercrime.

- **FTC.gov:** The Federal Trade Commission is a free, one-stop resource, https://www.identitytheft.gov/ can help you report and recover from identity theft.
- **US-CERT.gov:** Report computer or network vulnerabilities to US-CERT (Computer Emergency Readiness Team) via the hotline: 1-888-282-0870 or www.us-cert.gov. Forward phishing emails or websites to US-CERT at phishing-report@us-cert.gov.
- **IC3.gov:** If you are a victim of online crime, file a complaint with the Internet Crime Complaint Center (IC3) at http://www.IC3.gov.
- **SSA.gov:** If you believe someone is using your SSN, contact the Social Security Administration's fraud hotline at 1-800-269-0271.

If you discover that you have become a victim of cybercrime, immediately notify authorities to file a complaint. Keep and record all evidence of the incident and its suspected source. ❖

HOW TO SURVIVE A DATA BREACH

From the National Cybersecurity Alliance

Nobody likes receiving a letter about their data being lost in a data breach. Sometimes, your sensitive information is exposed to the internet through no fault of your own. Because so much of our sensitive data is stored digitally, sometimes your information can be stolen even though you weren't personally targeted and you maintain good cybersecurity behaviors. Act fast when you find out your data might have been compromised in a breach.

- As soon as you find out your data might have been lost in a breach, keep informed about the matter. Monitor the breached organization's communications about the incident. Look up stories from high-repute news organizations and info from trusted cybersecurity outlets to help you understand the nature of the data breach and what you should do.
- Change your password for the affected account and make it unique, 16 characters long, and complex. Enable multi-factor authentication.
- Keep an eye on your financial accounts for any suspicious activity. If you notice anything unusual, contact the financial institution quickly and report the incident.
- Check your credit report for unauthorized activity. Obtain credit monitoring if offered by the breached organization. Report discrepancies to the credit bureaus.

Be aware cybercriminals exploit big data breach news by sending phishing messages designed to trick you into sharing sensitive information. Legitimate organizations never ask for sensitive information, like passwords or bank account numbers by email or text messages. ❖

FOR MANY HELPFUL TIPS AND TRICKS

Go to https://www.apcug2.org for all aspects of computing and operating systems.

SPECIAL OFFERS

Go to the APCUG website at https://apcug2.org/discounts-special-offers-for-user-groups/ for discounts and special offers for members of User Groups. Avast Anti-virus and Acronis True Image, and several book, media and training sites offer discounts including the two mentioned below.

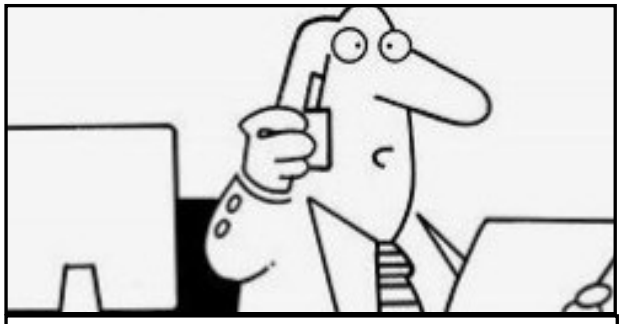
- Members can save at the **Pearson Technology** websites: InformIT, Cisco Press, Pearson IT Certification, Que Publishing, Adobe Press, and Peachpit Press. Informit.com/user_groups/index.aspx Code for print books: **ITCOMMUNITY.** Code for eBooks: **DIGITALCOMMUNITY**
- See books on digital imaging and photography, gaming, animation, film and video, post-production, audio, music technology, broadcast and theatre at Routledge | Focal Press today! They offer discounts to User Group members.

TECHBOOMERS.COM

For learning how to use internet-based websites and applications for free.

- https://TechBoomers.com
- https://www.youtube.com/watch?v=O2-bwYlYu1I

LAUGHING OUT LOUD



I sent my bank details and social security number in an email, but I put "PRIVATE FINANCIAL INFO" in the subject line, so it should be safe.

NOTICE

The columns, reviews and other expressions of opinion in *User Friendly* are the opinions of the writers and not necessarily those of the Los Angeles Computer Society. LACS became a California non-profit corporation on July 17, 1991. Its predecessor was the UCLA PC Users Group.

MEMBERSHIP INFORMATION and BENEFITS of MEMBERSHIP

Annual Membership Dues:

Regular New and Renewal,	
Printed Newsletter	$ 40
Electronic Newsletter	30
Family-Associate	12
Students	18
Contributor	50
Supporter	75
Benefactor	100
Gift Membership	20

A subscription to *User Friendly* is included with membership.

Associate members use the same mailing as a regular member; they do not receive their own subscriptions to *User Friendly*, but may read it on the LACS website. **Students** must prove full-time status. A member may give a 1-year, 1-time gift to a non-member.

Monthly general meetings are via Zoom. In-person or hybrid meetings may take place in the future.

Members also enjoy these special benefits:

— **Monthly Newsletter** *User Friendly*. We publish your article submissions or free classified ads to buy or sell your computer items.

— **Get FREE help** by phone or email (See your roster) from knowledgeable members who are Quick Consultants listed in *User Friendly.*

— **Get help by email** by using our group email list. Send your questions to PC@LACS.Groups.IO

— **Receive important news** and announcements via *User Friendly* and LACS's email list.

— **Free APCUG (**International Association of Technology and Computer User Groups) **Webinars, virtual conferences, programs, and technical information.** Check *User Friendly* and your email to see what's offered.

— Occasional **free software and computer books**, if you review them for *User Friendly*.

— **Annual Holiday Party**

— **Social Interacting** with others who have like interests in computers and technology.

— **Special Interest Groups** (SIGs) on various topics may be created by members.

All renewals are due in January. New members will pay the annual amount when they join.

Check # _____ **LACS New or Renewal Membership Application**

Date _____ **Dues may be paid by PayPal, Zelle, or check. If paying by check, make the check out to "Los Angeles Computer Society", and mail it with this form to:**

***Los Angeles Computer Society,* 11664 NATIONAL BLVD. #343, LOS ANGELES CA 90064-3802**

Please PRINT Clearly **[ ] New** **[ ] Renewal**

[ ] New / Renewal with printed newsletter - $40.00 [ ] Associate - $12.00 [ ] Student - $18.00

[ ] New / Renewal with electronic, no paper, newsletter - $30.00 [ ] Gift Membership - $20.00

[ ] Contributor - $50.00 [ ] Supporter- $75.00 [ ] Benefactor - $100.00 [ ] Other

Name: First Last

Name of Associate: First Last
(Same address as a primary member)

Address:

City, State, Zip + 4

E-mail Address: E-mail of Associate

Preferred Phone: Publish
Contact Info in Roster [ ] Yes [ ] No

Did a member of LACS invite you to join? If so, who? If not, how did you hear about LACS?

Revised Jan. 2024, ljc

First Class Mail

Editor…..……..... Leah Clark
Indexer …….....Leah Clark
Proofreaders ….....Irv Hershman,
Jim McKnight, Stephanie Nordlinger,
and Charlotte Semple

User Friendly is published by the Los Angeles Computer Society.
11664 NATIONAL BLVD, #343 LOS ANGELES CA 90064-3802
Voice-mail: 424-261-6251. Web site: https://www.lacspc.org

Los Angeles Computer Society

GENERAL MEETINGS ARE ON ZOOM.

Before each meeting, members and invited guests will receive an email with the URL link to the meeting. **Just click on the link**. If you haven't received it by the morning of the meeting, let Leah Clark know. When you click on the link, you will enter a waiting room. Then the host or a co-host will admit you to the meeting.

Please try to arrive at least a few minutes before the meeting start-time so you don't interrupt the meeting and any technical problems can be solved. If you need to take a break during a meeting, do not click on Leave or End. If you do, the meeting will be interrupted for someone to re-admit you from the waiting room. You may turn off your video when you are gone.