THE LOS ANGELES COMPUTER SOCIETY NEWSLETTER

User Friendly

Volume 38 Issue 10
October 2021

LACS
A Computer and Technology User Group

IN THIS ISSUE

APCUG EVENTS

Watch your email for APCUG workshops and other up-coming events.

LACS IS A MEMBER OF APCUG

www.apcug2.org
www.facebook.com/APCUG
www.twitter.com/apcug

apcug

An International Association of Technology and Computer User Groups

OCTOBER 12 GENERAL MEETING

Meeting Time: 7:00 – 9 PM – Via Zoom
6:30 to 7:00: Socializing and Questions & Answers
Topics: **New Security Issues & Solutions:**
Keyless Cars and Safe Power Sources

John Krout will cover several distinct but uncommon security topics in this order:

1. Theft of Keyless Entry Cars, including Q&A.
2. More Power To You in three parts, with Q&A after each part. The parts are:
   - **a.** Power Bank Batteries
   - **b.** Inverters
   - **c.** Small power strips and charger blocks for use at airports and on airplanes.

While observing Cybersecurity month, by popular demand we are not rehashing the old stuff. If you have other security questions or problems, you might read the articles on security in this issue of User Friendly and join the October 12 meeting between 6:30 and 6:50 to discuss them.

Meet Our Presenter

John Krout is a former Software Engineer with considerable experience in C and C++. He worked primarily on large computer systems development for federal government agencies in the Washington D.C. region. Now retired, he is free to speak and write about anything he wants. He lives in Arlington VA with his son, many computers and digital cameras, and too many cats.

Tuesday, October 12, 7:00 - 9:00 PM Via Zoom
6:30 - 7:00 Socializing and informal Q & A
LACS members on the PC groups.io list, will receive the Zoom link on or about October 10. Guests may apply for the link by emailing Leah Clark at leahjc@sbcglobal.net before October 10.
More information about LACS at https://www.lacspc.org

FROM YOUR PRESIDENT / EDITOR

October is Cybersecurity Awareness Month

Since 2004, Cybersecurity Awareness Month has been an effort between government and industry to ensure that everyone has the information they need to stay safe and secure online. It is co-led by the National Cyber Security Alliance (NCSA) and the Cybersecurity & Infrastructure Security Agency (CISA.) Over 3,000 companies, schools, governments, nonprofits and individuals from all 50 states and over 50 countries joined the campaign in 2020 by signing up as Champions.

LACS is a Champion!

This issue of *User Friendly* is focused on ways to keep safe online. I know most LACS members are savvy, know what they are supposed to do, and recognize something that just doesn't look right. But new threats keep coming up, and it is easy not to be vigilant all the time. So I hope every reader gets something that's helpful for them. Happy Reading!

Hybrid Meetings?

Some LACS members would like to see our general meetings be hybrid, i.e., meetings where some members can participate from home via Zoom, and others in-person, and those in both groups able to communicate with each other. To do this, we will need a few members to research how to accomplish this, what equipment will be needed, and to be willing to set it up before every meeting.

Please let me know if you are interested in helping with this.

The LACS 2022 Board

See page 4 of this issue to see the 2022 board members who were duly elected at the September general meeting. I thank them all and look forward to a good year for LACS. Please send me any suggestions or offers of help to keep LACS a helpful, productive organization. Every member counts, not just the board.

Holiday Party?

We would like to celebrate the upcoming holidays by getting together at a restaurant for a lunch or early dinner. It has been a long time since we have been able to get together in person. Remember our holiday dinners in the past when we invited our spouses and families and friends? After the last year and a half, we deserve to have some fun.

I think, if we can find a place with a separate room that's large enough for us to keep some distance, we can do this. Maybe we can require everyone attending to be vaccinated.

Please let me know if you can suggest a place, or have suggestions for how we can achieve this. Time is going fast, and restaurants will soon be booked for the holidays.

To LACS members and their families and friends

GENERAL MEETING REPORT

September 14, 2021

By **Leah Clark**, LACS President and Editor
Topic: **Music in Your Car**
Speaker: **Ray Baxter**
APCUG Speaker's Bureau
President and Treasurer, APCUG
Payson Computer Meet-Up Club, AZ
Join **Tech for Seniors**, Monday mornings at 9:00 AM at www.techforsenior.com

Zoom Meeting ID: 526-610-331

Technology has changed the way we listen to music in the car. We have come a long way from the AM radio to Bluetooth connectivity. Today the options are numerous and can be confusing. Auto manufacturers are now eliminating the expense of the CD player, so we must decide how to proceed.

Option 1: Convert (rip) the songs from your CD collection to mp3 files saved on your computer and copy them to devices to play music in your car.

Option 2: Choose a streaming service and play the music from your smartphone or an mp3 player via Bluetooth or a wired connection. Ray showed a video on using Amazon Prime streaming service in your car.

Option 3. Use both.

Ray discussed the pros, cons, and gave instructions for each of these options. He played videos demonstrating ripping a CD using Windows Media Player via your flash drive, aka thumb drive. He explained how to play ripped songs in cars equipped with USB connectors. Ray likes the ability to request songs or an artist verbally to allow hands-free usage. It's easier to carry one flash drive than several CDs and cases.

Then Ray showed us how to play song files from a smartphone by copying them to a micro SD card, getting the sound from your device to the car speakers. Bluetooth systems allow you to pair your smartphone or mp3 player with the car stereo head-unit to play music wirelessly. Ray played videos demonstrating this and options to connect your phone via a wire if your car doesn't have Bluetooth or if your vehicle is older.

Some other options to enable connecting your smartphone to your car are

- Android Auto
- Apple Car Play
- Amazon Echo Auto

Music formats will continue to change, and technology will continue to evolve. Either you grow with it or get left behind. This presentation was followed by Q & A with more tips and tricks.

Topic: **ElderKey**, the Elder Journey
Speaker: **Robert (Bob) Clymer**
rclymer@EverythingForMomAndDad.com

Bob and his colleagues are establishing a new company, **Everything for Mom & Dad,** to build software to aid caregivers and families with solutions that

- Focus on improving elder and family well-being.
- Manage everything together in one place by including medication lists, essential contact lists, important documents, and medical history, with access from anywhere to enable building a care plan and to-do lists for everyone.
- Guide everyone to get things right.
- Delivers peace of mind.

They are now in the software's developmental stage, with plans to have the first version by year-end.

Bob and his team are asking us to join one or more half-hour sessions in early October

- To access the "wireframes" or prototype screens to appraise what the screens look like.
- To use the screens to answer questions and fulfill requests, written or verbal.

Responses will be recorded and used in further designing the software

Participants will receive a **$25 Amazon Gift Card per session**.

Please contact Robert Clymer at rclymer@EverythingForMomAndDad.com or 818-929-8862
Bob hopes we will sign up, and he thanks us. He wants to come back in January to show the progress he has made.

We are happy that Bob has now joined LACS, and we welcome him.

See the Zoom recording of this meeting for all the information Bob gave.

LACS 2022 Board

The candidates for the LACS 2022 board were introduced, and a request was made for more nominations. Being that there were no more nominees and no position was contested, the nominations were closed, and Leah Clark called for the vote. The following slate was unanimously elected.

- President: **Leah Clark**
- Vice President: **Stephanie Nordlinger**
- Secretary: **Marcia Jacobs**
- Treasurer: **Gavin Faught**
- Director: **Paula Van Berkom**
- Director: **Irv Hershman**
- Director: **Annette Tossounian**
- Director: **Fred Kong**

Directors with terms running through 2022

- **Sylvia Davis**
- **Howard Krivoy**
- **Mark Presky**

We thank them all for their service and look forward to a productive LACS year.

See the September issue of *User Friendly, pages 4 and 5* and the next column of this issue for introductions to our 2022 board members.

Director, Annette Tossounian

I was born and raised in Culver City. In July 2018, I was appointed LACS secretary after the position had been vacant. I then agreed to be the welcome chair, starting in September 2018. I notice how computer technology is moving at an accelerating rate, and I find the best way to keep up is by being associated with LACS with the fine guest speakers, hands-on help with equipment, and being surrounded by similar minds with questions and answers. I enjoy retired life as a volunteer at food banks, and I donate blood monthly at the Red Cross. My hobbies are cooking, gardening, and stamp collecting.

Director, Fred Kong

Fred has agreed to run for this office because no one else has, and it has been vacant for too long. He has served as a director for two terms in the past. In addition, he has initiated, led, and served on innovative projects and functions during his many years of membership.

SEVEN WIFI SECURITY MISTAKES TO AVOID

By **Bob Rankin**
AskBobRankin.com

Wireless networking (WiFi) is convenient and essential if you have a smartphone, laptop, or tablet. But if you aren't careful, using WiFi to access the internet can leave you open to hackers and unauthorized moochers of your Internet service. Here are some of the biggest mistakes that people make with WiFi and how to avoid them.

Is Your WiFi Wide Open?

Several years ago, I got Verizon's FIOS high-speed Internet service at my home. And then something curious happened. Cars were stopping in front of my house and staying for 10 or 20 minutes. There was no reason for anyone to stop there, so my spider-sense began to tingle. After checking my wireless router, I found that Verizon had left it wide open. Without a WiFi password, anyone could connect! So I locked down the router's WiFi signal with a password, and my daily stream of visitors stopped.

MISTAKE #1: Failing to put a password (also called an encryption key) on your WiFi lets anyone within range of your wireless router join your network. If file and printer sharing are also enabled, random passers-by may be able to sift through files on every computer on your home or office network.

Unencrypted WiFi also allows eavesdropping on your Internet traffic, even if the snoop is not connected to your network. Data passing between a computer and a wireless router is broadcast in all directions as far as several hundred feet.

Moochers on unsecured WiFi networks may slow authorized users' traffic or even download illegally while leaving the network's owner with legal consequences. For these reasons,it's vital to set up your wireless network to use one of the encryption methods built into all wireless routers.

MISTAKE #2: While you're locking down your WiFi signal, don't make the mistake of choosing WEP encryption, the oldest and weakest encryption method. It can be cracked in about two minutes using software easily found online. WEP is often the first option on a router's list of available encryption methods, so don't be lazy and choose it for that reason. Instead, use the WPA2 method for the best protection.

(See my article Is Your Wireless Router REALLY Secure? to learn how a couple in Minnesota almost got framed for harassment, trafficking in child p**n, and threatening the Vice President because they used WEP encryption on their wireless router.)

MISTAKE #3: Weak encryption keys (WiFi passwords) are a related mistake. Strong encryption is of no use if a hacker can obtain your password by brute force attempts or by simply guessing it. Some wireless routers come with a default (factory set) password like "admin" or "password." And sometimes, internet service providers will set your WiFi password to your home phone number. Passwords like these are trivial for even the most clueless hackers to guess. It's also common for the router's login credentials and/or WiFi password to be listed on a sticker applied to your router.

Let me clear up a common point of confusion here. Your internet router has a username and password that you'll need to log in and change any settings. One of those settings is the WiFi password. So TWO passwords are being discussed here, and both are important. Your Internet Service Provider should have given you the router's username and password if they supplied the router. Otherwise, look for it in the materials that came with it.

Strong passwords should be at least 12 characters long and include a mixture of upper/ lower case letters, digits, and special characters. For example, the password "M@ry Had a L1ttl3 L4mb" is a much better choice than "123456" or "qwerty." You needn't worry about entering this password over and over. Typically, you'll only need the WiFi password when setting up a new device such as a laptop, tablet, smartphone, or wireless printer. (See Hey, Is This Your Password? to find out if your password is one of the 25 most common and easily guessed.)

I cannot provide detailed instructions for your specific router. But in most cases, you'll start by connecting to your router by entering this address: http://192.168.1.1 in your web browser. Then provide the admin username and password. If you need help logging into your router or changing the settings once logged in, contact your ISP or look for instructions online.

MISTAKE #4: Disabling the firewall built into most modern routers in the hope of getting faster internet is the fourth mistake. Firewalls keep unauthorized outsiders from getting into your network. They do not appreciably slow your Internet connection. So do not disable your router's firewall. (See Do I Really Need a Firewall? to learn more about firewalls.)

MISTAKE #5: Relying on stealth alone to escape hackers' attention is a mistake that some people make. Some people think they can get away without encryption or a password on their WiFi, just by hiding their WiFi router's SSID. Yes, most routers have a setting to disable the broadcasting of the router's SSID (name) so that other WiFi users within range won't "see" it on the list of available wireless connections. Disabling the SSID isn't a bad idea. It will make your WiFi signal invisible to most casual passers-by. But the SSID is included with many kinds of Internet traffic. A hacker with free "sniffer" software can intercept and discover your router's SSID.

MISTAKE #6: Similarly, **using MAC address filtering** to allow only specific devices to connect to your network isn't a reliable method either. MAC addresses are easily spoofed and, like SSIDs, are embedded in Internet traffic that can be intercepted. Another downside of using MAC address filtering is the inconvenience involved. You'll need to update your list of allowed MAC addresses whenever you want to connect a new device or allow a guest access to your WiFi. MAC address filtering is a good supplementary security precaution in some cases, but do not rely on it alone.

MISTAKE #7: Don't assume your Web browsing is private when out in public. If you're using WiFi to access the internet at a coffee shop or other public place, you should know that any unencrypted traffic flowing in or out of your phone or laptop is visible to nearby persons.

As long as you're accessing a web page with an address that begins with **https**, the data you send and receive is protected from sniffers and snoopers. That little "s" is your assurance that your connection is encrypted. ❖

VOW TO START USING A PASWORD MANAGER

By **Kurt Jefferson**, Editor
Central Kentucky Computer Society
CKCS Newsletter, January 2021
www.ckcs.org
lextown2 (at) gmail.com

I keep telling students in my CKCS classes that they need to start using a password manager. You should be using a password manager on your iPad, iPhone, Mac, Windows PC, and Linux PC. Seriously? Yes.

With a good password manager, you only need to remember one password. That's right. You don't need to remember the one you use when you buy from Amazon. And the password you use to pay your water bill. And the one you use to log into your bank account.

Password managers are apps that securely keep track of your passwords, allow you to create private notes, automatically log you into your password-protected websites, and more.

Some of the best include:

1Password
Dashlane
LastPass
Keeper
NordPass
RoboForm
Sticky Password
bitwarden
RememBer
Enpass

If you're reluctant to use a password manager, wired.com says you've got company. "Password managers are vegetables of the internet. We know they're good for us, but most of us are happier snacking on the password equivalent of junk food," writes *Wired* in an article headlined, "*The Best Password Managers to Secure Your Digital Life*."

As I read that, I said to myself, "Ain't that the truth." I know plenty of brilliant people who are committed to their habits, who are stubborn, and who cannot change. They don't use password managers. You probably know your web browser will save your passwords automatically for you. The website *Tech Republic* says this is a bad idea.

You should **never** allow your web browser to save your passwords because others can see them. The article describes step-by-step procedures that someone can use to view your saved passwords in Google Chrome, Firefox, and Safari browsers. The article concludes:

> Don't allow your browser to save your passwords. None of them. Not one. If you do, those passwords are vulnerable. All someone has to do is have access to your computer (remote or physical). Unless you use Safari or the Master Password feature in Fire-fox, those passwords are available for anyone to see. If you absolutely must have your browser store your passwords, and you're not using macOS, make sure to use Firefox and enable the Master Password feature. Use Chrome at the peril of your passwords. In place of having your web browser store your passwords, make use of a password manager.

If you use a Mac, you might avoid using Apple's built-in keychain system and opt instead for a password manager. Glenn Fleishman, who writes about security issues for Macworld, gets into the details and digs deeper into this if you're interested.

Tom's Guide spoke with several digital-security experts. While some are not fond of password managers, plenty of others use them, trust them, and rely on them.

Cybernews writes, "You really should use a password manager. Yes, they have their flaws and vulnerabilities. But it's still better than re-using the same weak passwords and writing them down as a note on your smartphone that becomes a playground for your kids after work." ❖

LACS NOTICES

WELCOME ALL

Gavin Faught, LACS Treasurer

New Members (1)

Robert Clymer

Renewals (3)

Shelby Croft

Heidi Feingersh

Roger Kohn, Supporter

HOW TO JOIN OUR MAIL LISTS

LACS members can join one, or both, of the lists shown by putting just their name in the message body of an e-mail to each of the lists they wish to join from the e-mail address they wish LACS to use. It's highly recommended to join both lists.

- **PC@LACS+subscribe (at) groups.io**
- **LACSLIST@LACS+subscribe (at) groups.io**

PC is for official LACS business only. **Lacslist** is for any other computer or technology – related messages and questions.

Email computer or technology-related questions or comments to all members on the LACSLIST to lacslist (at) lacs.groups.io.

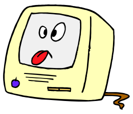
New members will receive one invitation to join each list; they must respond quickly or follow the above instructions.

If you have any problems or questions about joining the lists, please contact Stephanie Nordlinger: nordlacs(at)aol.com.

HYPERLINKS

Underlined text (blue in the colored editions) in User Friendly usually means it's a hyperlink to a website. Click on the link to see the reference.

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 jim@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.

HOW TO CHANGE YOUR CONTACT INFORMATION

Go to https://www.lacspc.org Click on **Member Forms** in the bar under the picture. Under **Membership Update,** select **Click Here** to select either the DOC or PDF form. Fill it out, and email it with your changes to membership@lacspc.org or mail it to

LACS, 11664 National Blvd. #343,
Los Angeles, CA 90064-3802.

ATTENDING A ZOOM MEETING

You should receive, via email, a link, Meeting ID, and Passcode to attend the LACS general meetings a couple of days before the meeting. **Please let Leah Clark know by the morning of the meeting if you don't have it.**

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.

LACS CALENDAR

LACS Board Meeting

Date: Monday, October 4, 2021 via Zoom
Time: 7:00 P.M. (Open from 6:30 P.M.)
Please arrive early so we can start on time.
Where: At your home or wherever you are

General Meeting

Date: Tuesday, October 12, 2021 via Zoom
Time: 7:00 P.M. (Open from 6:30 P.M.)
Where: At your home
Please arrive early so we can start on time.
Where: At your home or wherever you are

October: Cybersecurity Awareness Month

October 11: Indigenous Peoples' Day

VISIT OTHER COMPUTER USER GROUPS

Check out the URL below for information for visiting other user groups' Zoom meetings and for many more ideas for using Zoom and managing dealing with the stay-at-home restrictions.

https://apcug2.org/tech-things-to-learn-while-sheltering-in-place/

GENERAL MEETING PRESENTATIONS VIA ZOOM

October 12: New Security Issues and Solutions

This schedule is subject to Change. Check your email and *User Friendly* for updates.

ZOOM MEETINGS

To join a Zoom meeting, click on the URL on the invitation you will receive via email before the meeting and follow the prompts.

Contact Leah Clark at leahjc@sbcglobal.net if you have any questions or if you don't receive the link by the morning of the meeting day.

Please enter before our meeting starting time in case problems need to be solved and to ask questions. We want our meetings to start on time.

ZOOM RECORDINGS & PODCASTS

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

To listen to the podcasts of most of our past in-person general meetings, go to https://www.lacspc.org/category/audio-files/. Click on the session you want to hear.

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 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 that 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.

More Quick Consultants, and more categories are always needed. You may decline or postpone a call if it comes at an inconvenient time.

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 - 8, 1, 10
MS PowerPoint - 8, 11
MS Publisher - 2
Open Office - 6
Photoshop - 10
Quicken - 8, 12
Thunderbird - 7
Utilities - 7, 8
Visual Basic - 5
Websites - 5
Windows - 6, 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
5	Ialongo, Gilbert	9:00 AM	5:00 PM
6	Johnson, Carol	10:00 AM	9:00 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

OFFICERS, DIRECTORS AND LEADERS

Title	Name	Term
President	Leah Clark	2021
Past President	Stanley Johnson	2021
Vice President	Stephanie Nordlinger	2021
Secretary	Marcia Jacobs	2021
Treasurer	Gavin Faught	2021
Director	Newton Bernstein	2021
Director	Irv Hershman	2021
Director	Paula Van Berkom	2021
Director	Sylvia Davis	2022
Director	Fred Kong	2022
Director	Howard Krivoy	2022
Director	Mark Presky	2022
APCUG Rep.	Leah Clark	
Corporate Counsel	Stephanie Nordlinger	
CCSC Computer Lab	Loling Beckman	
Database Manager	Sylvia Davis	
Groups.IO Lists	Stephanie Nordlinger	
Hospitality Chair	Sylvia Davis	
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://www.lacspc.org

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

Please use your roster for email addresses and phone numbers to contact any officer, board member or other member, or you may leave a message at the above number. If you don't have your roster, please contact Leah Clark at leahjc@sbcglobal.net and she will email you a copy.

OCTOBER IS CYBERSECURITY AWARENESS MONTH

Do Your Part. #BeCyberSmart.

The theme for 2021 is **Do Your Part. #BeCyberSmart**, helping to empower individuals and organizations to own their role in protecting their part of cyberspace.

The Cybersecurity Awareness Month Champion program is a way to officially show your support and to receive valuable resources to promote Cybersecurity. Champions represent those dedicated to promoting a safer, more secure and more trusted internet. LACS is a Champion.

During October, the National Cyber Security Alliance will focus on a different area each week.

Week 1, October 4-8
Get Familiar with the Cyber Basics

At a time when we are more connected than ever, being “cyber smart” is of the utmost importance. This year has already seen more than a fair share of attacks and breaches. Cyberattacks are becoming more sophisticated, with more bad actors cropping up each day. Here are steps we can take daily to mitigate risks and stay ahead of malefactors.

Enable MFA

Multi-factor authentication (MFA) adds that necessary second check to verify your identity when logging in to one of your accounts. By requiring multiple authentication methods, your account is further protected from being compromised, even if a bad actor hijacks your password. In this way, MFAs make it more difficult for password cracking tools to enable attackers to break into accounts.

Use strong passphrases and a password manager

All too often, securing strong passphrases and password managers is overlooked. Using long, complex, and unique passwords is a good way to stop your account from being hacked, and an easy way of keeping track and remembering your passwords is by using a password manager.

Perform software updates

When a device prompts that it’s time to up date the software, it may be tempting to click postpone and ignore the message. However, having the latest security software, web browser, and operating system on devices is one of the best defenses against online threats. So, don’t wait - update.

Do your research

Common sense is a crucial part of maintaining good online hygiene. Do some research before downloading anything new to your device, such as apps. Make sure that it’s legitimate by checking who created the app, what the user reviews say, and if there are any articles published online about the app’s privacy and security features.

Check your settings

Double-check your privacy and security settings and know who can access your documents. This extends from Google docs to Zoom calls and beyond. For meetings on Zoom, for example, create passwords so only those invited to the session can attend, and restrict who can share their screen or files with the rest of the attendees.

Be cyber smart and maintain stellar online hygiene to protect yourself and others from cyber attacks. No single tip is foolproof but taken together, they can make a real difference in taking control of your online presence. Following these tips is also easy and free. Make a habit of practicing online safety to decrease your odds of being hacked. Prevent lost time, money, and annoyance.

Week 2, October 11-15
Fight the Phish

From ransomware to SolarWinds, the cybersecurity space has been as hectic as it has ever been over the last 12-24 months. However, for all of the emerging threats and news cropping up on the horizon, phishing -- one of the oldest pain points in cybersecurity -- continues to wreak havoc and is as big of a threat as ever.

Despite often being overlooked in terms of hype, phishing has been a mainstay in the cybersecurity threat landscape for decades. In fact, 43 percent of cyberattacks in 2020 featured phishing or pretexting, while 74 percent of U.S. organizations experienced a successful phishing attack last year alone. That means that phishing is one of the most dangerous "action varieties" to an organization's cybersecurity health. As a result, the need for proper anti-phishing hygiene and best practices is an absolute must.

Here are a few quick best practices and tips for dealing with phishing threats.

Know the Red Flags

Phishes are masters of making their content and interactions appealing. However, from content design to language, it can be difficult to discern whether content is genuine or a potential threat, which is why it is so important to know the red flags. Awkward and unusual formatting, overly explicit call-outs to click a hyperlink or open an attachment, and subject lines that create a sense of urgency are all hallmarks that the content you received could be potentially from phish. These indicate that it should be handled with caution.

Verify the Source

Phishing content comes in a variety of ways. However, many phishes will try to impersonate someone you may already know — such as a colleague, service provider, or friend — as a way to trick you into believing their malicious content is trustworthy. So don't fall for it. If you sense any red flags that something may be out of place or unusual, reach out directly to the individual to confirm whether the content is authentic and safe. If not, break off communication immediately and flag the incident through the proper channels.

Be Aware of Vishing and Other Phishing Offshoots

As more digital natives have come online and greater awareness has been spread about phishing, bad actors have begun to diversify their phishing efforts beyond traditional email. For example, voice phishing -- or vishing -- has become a primary alternative for bad actors looking to gain sensitive information from unsuspecting individuals. Like conventional phishing, vishing is typically executed by individuals posing as a legitimate organization — such as a healthcare provider or insurer — and asking for sensitive information. Simply put, individuals must be wary of any communication that asks for personal information, whether via email, phone, or chat, especially if the communication is unexpected. If anything seems suspicious, again, break off the interaction immediately and contact the company directly to confirm the integrity of the communications.

Phishing may be "one of the oldest tricks in the book," but it is still incredibly effective. And although it may be hard to spot when you may be in the midst of a phishing attempt, by exercising caution and deploying these few fundamentals, individuals and organizations more broadly can drastically mitigate the chances of falling victim to a phishing attack.

Week 3, October 18-22
Why You Should Consider a Cyber Career

Cybersecurity is one of the hottest sectors today, with new threats and challenges emerging each day. As a result, there is considerable push being undertaken by both business and education sectors to attract individuals toward a degree and career in cyber. So, are you interested in joining this exciting new workforce? Here are a few reasons why pursuing a degree and career in cyber might be right for you.

Hot Job Market

To say that the cybersecurity jobs market is hot would be a vast understatement. According to the U.S. Bureau of Labor Statistics, the job market for information security analysts will grow by 32 percent by 2028. It will be one of the fastest-growing job sectors in years to come. *Ventures* has found that there will be 3.5 million unfilled cybersecurity jobs in 2021. This means that cybersecurity professionals are among the most in-demand around the world and will be for some time.

Infinite Room for Personal and Professional Growth

Beyond just the ability to get a cybersecurity job, thanks to an ever-growing set of career tracks, cybersecurity offers various options for professionals to find a position that fits nicely with their own interests. Cybersecurity professionals work in everything from compliance to stress testing cyber defenses and software, so there are virtually limitless ways for professionals to apply their skills and look to grow them.

Investment in advanced cybersecurity pays for itself

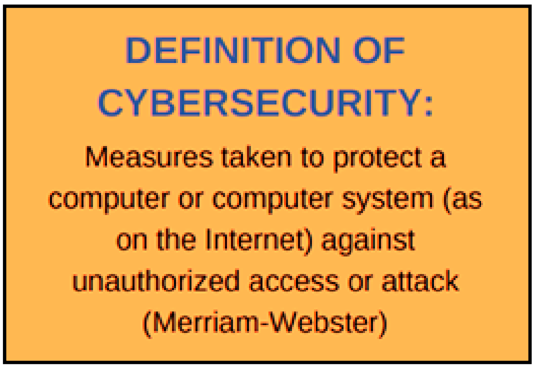
Due to the shortage of cybersecurity talent in the workforce, businesses and educational institutions are constantly rolling out new avenues to make cybersecurity careers more affordable. For example, new grants and scholarships are now becoming available each day for individuals interested in cybersecurity careers, while many businesses are beginning to offer tuition reimbursement or other financial perks. This means that a degree in cybersecurity may be much more affordable than you initially thought.

Graduate Growth

In addition to the interesting “on the ground work” that cybersecurity professionals get to take on every day, there is also a growing selection of highly tailored cybersecurity graduate programs that can further academic knowledge in cybersecurity as well. For example, graduate degrees ranging from Applied Cryptography to Network Vulnerability and Detection are now being offered nationwide by colleges and universities.

Additionally, as part of this deep-dive, cybersecurity professionals will also get the opportunity to network with other students from various backgrounds allowing them to open up further opportunities for future positions or businesses.

Editor's note: I realize not many LACS members are interested in a new career. But you may want to pass this information on to young people who are.



DEFINITION OF CYBERSECURITY:

Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack (Merriam-Webster)

Week 4 , October 25-29
Prioritizing Cybersecurity in a Hybrid Workplace

In this day and age, employees are more connected than ever. The hybrid workplace is here to stay, and for employees, this means relying on connected devices from their home office setups. According to recent data, smart home systems are set to rise to a market value of $157 billion by 2023, and the number of installed connected devices in the home is expected to increase by a staggering 70% by 2025. Here are some tips for securing those devices in this new normal where smart devices and online safety are a must.

Remember, smart devices need smart security

Make cybersecurity a priority when purchasing a connected device. When setting up a new device, be sure to set up the privacy and security settings on web services and devices, bearing in mind that you can limit who you are sharing information with. Once your device is set up, remember to keep tabs on how secure the data you store on it is, and actively manage location services to avoid unwittingly exposing your location.

Put cybersecurity first in your job

Make cybersecurity a priority when you are brought into a new role. Of course, good online hygiene should be part of any organization’s onboarding process, but if it is not, then take it upon yourself to exercise best practices to keep your company safe. Some precautions include performing regular software updates and enabling MFAs.

Make passwords and passphrases long and strong

Whether or not the website you are on requires it, be sure to combine capital and lowercase letters with numbers and symbols to create the most secure password. Generic passwords are easy to hack. If you need help remembering and storing your passwords, don’t hesitate to turn to a password manager for assistance.

Never use public computers to log in to any accounts

While working from home, you may be tempted to change scenery and work from a coffee shop or another type of public space. While this is a great way to keep the day from becoming monotonous, caution must be exercised to protect yourself and your company from harm’s way. Make sure that security is always top of mind, especially while working in a public setting, by keeping activities as generic and anonymous as possible.

Turn off WiFi and Bluetooth when idle

The uncomfortable truth is, when WiFi and Bluetooth are on, they can connect and track your whereabouts. So to stay as safe as possible, if you do not need them, switch them off. It’s a simple step that can help alleviate tracking concerns and incidents.

These are just a few simple steps towards achieving the best online safety possible. Staying safe online is an active process that requires constant overseeing at every stage - from purchasing and setting up a device to making sure that your day-to-day activities are not putting anyone at risk. By following these steps, you are doing your part to keep yourself and your company safe from malicious online activity. ❖

NATIONAL CYBERSECURITY ALLIANCE

Educating and empowering our global digital society.

USING ZOOM TO CREATE A PERSONAL VIDEO MESSAGE

From **Practicing Safe Computing**

By **Hal Bookbinder**

Originally published in the February 2021 issue of *Venturing into our Past,* Jewish Genealogical Society of the Conejo Valley and Ventura County **(JGSCV)**

Recently I was invited to create a short video tribute for a cousin who had passed away. The funeral home would be live-streaming the service. I used Zoom to create a 90-second tribute to be shared at the memorial service.

You have certainly seen the **Record** button on the bottom of the screen when in a Zoom session. If you clicked on it, you were likely informed that only the host can record. You can host your own one-person Zoom session to create a self-video.

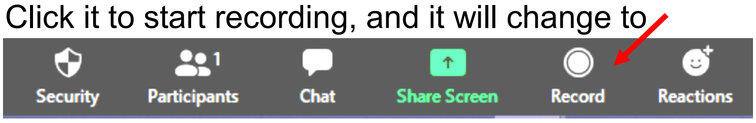
Sharing the video will generally require you to upload to the cloud, say to a Dropbox folder and provide a link to the person or persons with whom you would like to share. These video files are typically too large to email. For example, my 90-second video is 22 MB.

To get started, go to the https://Zoom.us website. If you do not have a Zoom account, you will need to create one. Click on **Sign Up**. IT'S FREE. If you have a Zoom account, log in. Now, hover over **Host a Meeting** in the upper right corner of the screen. Select **With Video On**. Click **Open Zoom Meetings** in the dialog box that will appear at the top center of the screen. If the dialog box fails to show, click **Launch Meeting** in the center of the screen.

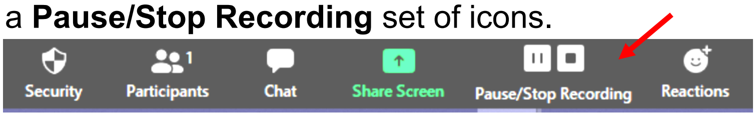
Select **Join with Computer Audio,** and you are in a Zoom session alone.

Bring your cursor to the bottom of the screen; a row of Zoom icons will appear, including **Record**.

Click it to start recording, and it will change to



a **Pause/Stop Recording** set of icons.



Proceed to record your video, selecting **Stop Recording** when done.

Once you click on **Stop Recording**, a message will be displayed in the upper-right corner of the screen, letting you know that an MP4 will be created "when the meeting ends." To record another video, select **Record** again. You can do this as many times as you like. So, if you are dissatisfied with a recording in progress, you can quickly terminate it and start over.

When you are finished, bring your cursor to the bottom of the screen to reveal the Zoom icons again. Click on the **End** button, and select **End meeting for all**. A pop-up will alert you that **Recording is in Progress**.

Zoom is now creating the MP4 video file(s). Once it completes, you will be given the option of selecting a folder for the video(s). If you just press the **Enter** key, it will default to the Documents folder, Zoom subfolder.

You will find two files in the destination folder for each time you started and stopped recording, an M4A audio file and an MP4 audio/video file.

A 90-second MP4 will take a couple of minutes for Zoom to build. A 45-minute video could take 30 minutes. Be patient. For more help, see https://support.zoom.us/hc/en-us/articles/201362473-Local-recording. ❖

Editor's note: I learned about this when I gave my DAR chapter's annual oral report to the state conference on Zoom in March. I had to do a lot of "retakes"! A link to a video could be sent as a greeting for any occasion, like a birthday.

REDUCING THE IMPACT OF DATA BREACHES

From **Practicing Safe Computing**
By **Hal Bookbinder**
Originally published in the January 2021 issue of *Venturing into our Past,* Jewish Genealogical Society of the Conejo Valley and Ventura County **(JGSCV)**

On Monday, November 30th, the “blackShadow” group revealed that it had hacked Shirbit, an Israeli insurance company. “blackShadow” tweeted photos of ID cards, driver’s licenses, and forms containing private information. The next day the Jerusalem Post quoted a leading hacking expert that “there have been multiple successful cyberattacks against Israeli infrastructure in the past year that have not been revealed to the public.”

“blackShadow” demanded payment of 50 bitcoin ($961,110), or it would continue to release hacked data. Each day, it posted significant amounts of data and doubled its price. Shirbit publicly refused to pay, and the Israeli government acknowledged it could not stop the release of data. It encouraged Israelis to obtain new ID cards and driver’s licenses. Then, on December 6th, the reporting abruptly stopped. So, one wonders what might have taken place behind the scenes.

U.S. laws require that organizations report data breaches to the impacted individuals and, in larger breaches, to the government. You can scan a list of 500 significant 2020 breaches of Personal Health Information (PHI) at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

How many organizations actually comply and how many quietly pay off the hackers is anybody’s guess. But be assured that eventually, your data will be exposed. Take these steps to lessen the impact of the inevitable breach.

1. Use different IDs and passwords for your accounts. Hackers know that many use the same IDs and passwords. So, when they discover this information at one site, they will try it on others.

2. Use dual authentication where offered and consider shifting from organizations that do not offer it. In dual authentication, a message is sent to your smartphone for your confirmation. So, a hacker would also need to have your device to be able to access your account.

3. Monitor your credit report and review your credit card, investment, and bank statements to ensure that no unauthorized transactions have occurred. Notice any missing credit card or utility bills.

4. If notified that your data was part of a breach, update your password and change it at any other site where you have used that password. Redouble your efforts to monitor your credit reports. Accept any offer by the organization to pay for credit or identity monitoring services.

5. Check https://haveibeenpwned.com to see if your email and password can be found for sale on the dark web. The results will be meaningful if you use strong passwords that others are not likely to have used as well. Change compromised passwords.

6. Consider placing a credit freeze with the three credit reporting agencies. This restricts access to your credit report, making it more difficult for identity thieves to open new accounts in your name.

7. Consider signing up for a credit or identity monitoring service that will alert you if your data has appeared on the dark web or someone has used your information to open a credit account.

For additional guidance, see GAO-19-230, DATA BREACHES: Range of Consumer Risks Highlights Limitations of Identity Theft Services ❖

JERE'S TECH TIPS

For many helpful tips and tricks for all aspects of computing, see *Jere's Tech Tips* at https://apcug2.org/jerestips/.

TECHBOOMERS.COM

teaches how to use various websites and internet-based applications.

- https://TechBoomers.com
- https://www.youtube.com/watch?v=O2-bwYIYu1I

SPECIAL OFFERS

Go to the APCUG website 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 the latest books on digital imaging and photography, gaming, animation, film and video, post-production, audio, music technology, broadcast and theatre from Routledge | Focal Press today! They offer discounts to User Group members. Focal Press Taylor & Francis Group

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.

LAUGHING OUT LOUD

Q. Why is a computer so smart?
A. Because it listens to its mother board.

Q. What do my dog and my cell phone have in common?
A. They both have collar ID.

Q. Why do spiders always know the answer to everything?
A. They are very good at finding things on the web.

This is your frustration computer. Whenever your actual computer makes you mad, take it out on this one. It's not real, and it's made of soft material.

From "How-To Geek

MEMBERSHIP INFORMATION

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 live in the same household or work at the same address 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 from knowledgeable members who are Quick Consultants listed in *User Friendly.*

— **Get help by email** by using our LACSLIST Group eMail List. Send your questions to lacslist (at) lacs.groups.io

— **Receive important news** and announcements via *User Friendly* and LACS's Group e-mail lists.

— **Free APCUG** (International Association of Technology and Computer User Groups) **Webinars.**

— **Free quarterly Virtual Technology Conference (VTCs)**

— **Information** on training and technical education.

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

— **Rewards** for recruiting; LACS will extend your membership for three months for each new regular member you recruit.

— **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.

Date: __________

Check # ________

LACS New or Renewal Membership Application

Please mail your dues and 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 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 Dec. 2020, ljc

First Class Mail

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

FREE!
Earn 3 months of free membership for every new regular member you bring in.

User Friendly is published by the Los Angeles Computer Society.
11664 NATIONAL BLVD, #343 LOS ANGELES CA 90064-3802
Voice-mail: 310-780-3302. Web site: http://www.lacspc.org

Los Angeles Computer Society

GENERAL MEETINGS WILL BE ON ZOOM UNTIL FURTHER NOTICE.

Before each meeting, members and invited guests will receive an email with the URL link to the meeting. 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 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.