Member of apcug An International Association of Technology & Computer User Groups

The Rochester Computer Society, Inc.

a computer/tech club open to everyone

MONITOR

Vol. 42, No.1 web: www.rcsi.org Rochester, NY January 2023

January 10, 2023, 'Artificial Intelligence Trends in 2023', videos by Tony Dellelo

February 14, 2023, 'Best of CES' Consumer Electronics

In This Issue

Our Club

RCSI is a nonprofit 501(c)(3) group open for membership to anyone interested in computers and new technology. Established in 1981, our aim is to provide an exchange of information between users of digital devices. We are not in any way affiliated with any computer manufacturer or software company, and ***we do not sell your data or email address***.

Program Meetings

No admission fee for non-members. Everyone is welcome! Second Tuesday of every month, except July and August, from 6:30pm – 8:30pm.

Help's Half Hour (Q & A) 6:30pm – 7:00pm. *Members and Guests are welcome to attend and bring their computer related questions with them to get answered.*

7:00 – 7:15, Club Business

7:15 – 8:30+, Main Presentation

Come and join in the fun and enjoy a snack! **You are welcome to bring a guest**.

Become a Member

The club would like to have you as a member, and your subscription will help to keep us going. Go to our website, www.rcsi.org, and download a printed form for use by the Post Office mail, **or** enter your info online and pay with a credit card or PayPal, **or** attend a meeting.

QR Code Scams – Be Careful Where You Point That Smartphone

By Phil Sorrentino, Secretary and APCUG Rep
Sun City Center Computer Club

QR Codes seem to be everywhere today. You'll find them anywhere someone wants to give you more information than is possible by other means, like a sheet of paper or a machine-readable standard bar code. Initially, QR codes were created to track manufacturing processes where barcodes couldn't store enough information. However, a bar code has one dimension. A QR code is 2-dimensional and can store significantly more data than a bar code. Roughly speaking, a QR code may contain as many as 7,000 characters as opposed to a bar code that may contain up

"Your Computer User Group of the Air", Saturdays from 12:00 pm to 2:00 pm, with Nick Francesco, Dave Enright, and Steve Rae. Broadcasting on JAZZ 90.1 FM (WGMC) from Rochester, NY. Call 966-JAZZ (585-966-5299) or 800-790-0415, **www.jazz901.org**

Sound Bytes is the longest running computer call-in show in the known universe.

We have stopped printing the Monitor newsletter. Digital copies can be emailed or obtained from **www.rcsi.org** or my **Pcloud** storage at **https://tinyurl.com/tonydel-rcsi** (***this link works in PDF version only***). Also includes presentation slides, **past newsletters dating back to 1996** and articles too large for this newsletter.

Some Past Presentations:

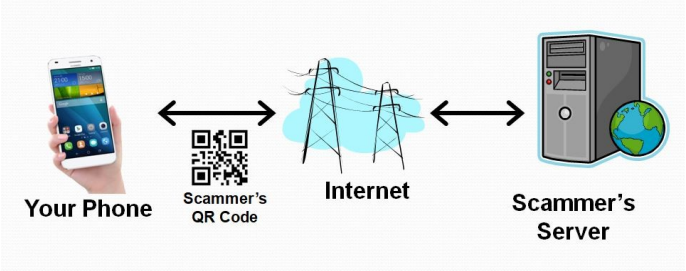
The New Space Race, 2021
Tech of South America
Autonomous Cars and Robots
Open Source and Free Software
Protecting Your Identity
Tablets, the Programs and Uses
Personal Finance Software
Amazing Browser Tips
Linux is Like Cars
Drones and Their Many Uses
Gifts and Gadgets for the Holidays
Cut the Cord, Streaming Services
3D Printing, ENABLE project
Internet Security and Privacy
Features, Mac OS X & Windows

to around 40 characters. That's over 170 times the amount of data. This increased amount of information makes the QR code so worthwhile.

QR codes were invented in Japan in the 1990s. They were first used by the automotive industry to manage production but have spread everywhere. There are even websites and apps that let you make your own. A QR code is a machine-readable, 2 dimension matrix of black and white squares. A QR code may represent many different data types, such as text, a hyperlink to a website, a telephone number, an email address, or a text or email message. QR codes, like billboards, clothing labels, walls, TVs, and even tattoos, can be placed on almost anything. QR stands for Quick Response. Quick Response comes from the manufacturing industry and deals with how fast a product can be replaced on the seller's shelves. Quick Response is "the rapid replenishment of a customer's stock by a supplier with direct access to data from the customer's point of sale." A QR code is merely a data storage representation of some information using the binary code. (For example, the letter A is represented by "01000001") The little squares and patterns of the QR code represent the binary information. The actual QR code is read-only, so it cannot record or steal any personal information on its own. Nowadays, the smartphone's camera app can scan the QR code when the camera is directed at it. (Most smartphones no longer have to download a separate app from the App store for reading QR codes.)

A QR code with an embedded hyperlink to a website can connect you to a specific website quickly and easily using your smartphone. There is very little one needs to know to take advantage of a QR code. But a lot of the latest technology is being used to accomplish the task. The three major technology components are your smartphone, the Internet, and a server (on the Internet, or "in the cloud"). This collection of technologies goes by the name "Client-Server Technology," and all three components have been developed to work together. For example, your smartphone has a camera App that connects the smartphone, as the client, to the server website whose URL was embedded in the QR code. (URL is the Universal Resource Locator, the term for a web address on the Internet.) This allows the provider of the QR code the ability to connect your phone with the QR code provider's server when you scan the QR code. Once connected to the server, the smartphone can access all the information that the server can provide.

QR codes take people from the physical world to the online (cyber) world. They let smartphones connect to an enormous world of information quickly and easily but, unfortunately they also allow smartphones to connect quickly and easily to a scammer's website. This is why scammers have started using QR codes in attempting to get in



APCUG, An International Association of Technology and Computer User Groups

https://apcug2.org/

Saturday Safaris

Exploring Technology in Depth

Saturdays:

12 pm – 2 pm EST

https://apcug2.org/saturday-safaris/

Tech for Seniors

https://www.techforsenior.com

hosted by Ron Brown and Hewie Poplock

Every Monday from 9-10 AM PT, (12-1 PM ET)

Broadcast with Zoom

The meeting ID is **526-610-331** (there is no password) and you'll be placed in a waiting room and then admitted.

# # #

APCUG Website Help

Windows & Android Tips:
https://apcug2.org/jerestips/

Apple Tech Tips:
https://apcug2.org/50-best-mac-tips-tricks-timesavers/

Penguin Platform (Linux):
https://apcug2.org/penguin-platform/

Chromebook Tips And Tricks:
https://apcug2.org/chromebook-tips-and-tricks/

touch with potential victims. It gets people online with the scammer's server. It is similar to "phishing" emails and telephone calls. QR codes are another way for scammers to get in touch with potential victims.

Many scammers (aka cybercriminals) have started to exploit the technology's convenience. Scammers create malicious QR codes to connect unwitting consumers to the scammer's server and dupe them into divulging their personal information. Anytime new technology comes out, cybercriminals attempt to find a way to exploit it. This is especially true with technology like QR codes. It seems like most people can figure out how to use them, but they probably don't really know how they work, and it's always easier to manipulate people when they don't understand their technology. Scanning the scammer's QR codes won't do anything malicious to your smartphone, such as installing malware. Still, it probably will take you to a website designed to try to get personal or financial information from you.

Like any other phishing scheme, it's impossible to know precisely how often QR codes are used for malicious purposes. Experts say they still represent a small percentage of overall phishing, but numerous QR code scams have been reported to the Better Business Bureau. As a result, many people know they need to be on the lookout for phishing links and questionable attachments in emails that purport to be from your bank. But thinking twice about scanning a QR code with your smartphone camera isn't second nature for most people yet.

Recently, a QR code scam was uncovered in a Texas city. Drivers were led to a scammer's website after scanning a QR code sticker on a parking meter. Eventually, around 30 such stickers were found. The QR code was supposed to help the motorist pay for online parking. However, instead of being taken to the city's authorized website, the motorist who scanned the fake stickers was led to a fake website that collected their credit card information. With a warning of the parking meter scam, officials in another city issued a warning to motorists after spotting similar stickers on parking meters.

Fake QR codes have even shown up in emails. Scammers may like using QR codes in phishing emails because they often aren't picked up by security software, giving them a better chance than attachments or bad links to reach their intended targets. It boils down to QR codes being just one more way for cybercriminals to get what they want and yet another threat for people to be on the lookout for.

So be careful when scanning QR codes. Here are some tips from security experts. Think before you scan. Be especially wary of codes posted in public places. Take a good look and determine if the sticker is part of the sign or display. If the code doesn't look like it fits in with the background, it may have been put there by a scammer. Be suspicious of any QR code that comes in an email. If you scan a QR code, look at the website it led you to and determine if it looks like what you expected. If it doesn't look appropriate, then leave the website. If it asks for personal information you don't think is appropriate, don't provide it. And, in the words of one of the Computer Club's past presidents, Matt Batt, "Be careful out there!"

From https://scccomputerclub.org/ , philsorr@yahoo.com.

RCSI Board Members

President:
Mark S. Lawson . . 544-5377
mslawson51@peoplepc.com

Treasurer:
Jerry Seward . . . . . .
jerry@jerryseward.com

Members-At-Large:
Bob Avery 385-4491
Webmaster
webmaster@rcsi.org, 9/23
Jan Rothfuss 347-6020
Membership & Help's Half Hour
jan_rothfuss@hotmail.com, 9/22
Tony Dellelo 734-6149
Programs & Monitor editor
tonydel@techie.com, 9/24

Planning Meeting

Held on 1st Tuesday of each month at 7 pm, * * ONLINE * *. We will be using Jitsi Meet. ANY CLUB MEMBER MAY ATTEND.

Got Questions?:

Windows: . . . . . Arpad Kovacs
podcomputer@gmail.com
Linux & some Mac: . . . . . .
Carl Schmidtmann
unixgeek@faultline.com

Monitor Newsletter

The Monitor is published monthly by members of RCSI. Articles by our members may be reprinted by other user groups or nonprofits, without special permission. A courtesy copy may be emailed to the author or Monitor editor. Limited copies (probably in black and white) will be printed and available at our meetings.

Club Mailing Address

Rochester Computer Society, Inc
PO Box 18516
Rochester, NY 14618

What Should I Assume About Workplace Technology Monitoring?

What to do when Big Brother happens to be your boss.

by Leo Notenboom, https://askleo.com/
Making Technology Work For Everyone

Many employers can and do monitor the technological activity of their employees. Here's what you need to consider doing.

What is a realistic perspective to take currently (in 2022) regarding information technology monitoring in the workplace? In other words, as an employee in an office I want to feel confident and not fearful regarding my efforts while working, not paranoid or distracted about it. Can you provide any helpful insight or redirect to someone who might be able to?

You won't like my insight.

I'm not saying you should be paranoid about your workplace… but I'm also not saying you shouldn't be.

Workplace technology monitoring

Employers' monitoring of digital activity in the workplace has only increased in recent years. Aside from asking your employer what they do and what their policies are and then trusting the answer you receive, there's really only one course of action: assume the worst.

Caveats

I'm not a lawyer, and none of this should be taken as legal advice. If you have a situation you think qualifies, contact appropriate legal counsel.

Speaking of the law: it varies depending on your location. As I understand it, workplace monitoring is generally completely legal. However, the devil is in the details, and the details differ depending on where you are.

The issue

Using technology at or owned by your workplace for anything other than work-related activity may be against your company's rules, whether those rules are explicitly stated or arbitrary.

You might think of this as only related to the obvious: running your side-hustle from the office, leaking sensitive data, wasting your time playing games, watching sports, or engaging in other online distractions.

Depending on those rules, though, it could be just about anything: checking personal email, messaging to friends and family, or even looking at your personal calendar could all qualify as being against policy.

It doesn't have to be restricted to using company equipment. For example, if your phone connects to company Wi-Fi while you're at work, that might also come under the corporate rules umbrella.

Tidbits of probably useless information

At 1,896 km, Guinness recognized **Yonge** St as the Longest Street in the World. Toronto, Ontario - Yonge St earned this distinction because north of Toronto, it morphed into Highway 11, continuing through towns, cottage country and wilderness for 1,896 kilometres (1,178 mi).

About 90% of the world's population kisses.

The Internet was originally called ARPANet (Advanced Research Projects Agency Network) designed by the US department of defense.

All insects have 6 legs. Spiders are arachnids and not insects.

Toilets use 35% of indoor water use.

The predecessor to what is now the international fast food restaurant chain Burger King was founded on July 23, 1953, in Jacksonville, Florida, as Instant Burger King.

In eastern Africa you can buy beer brewed from bananas. Banana beer is made from ripe (but not over-ripe) East African Highland bananas. To accelerate the ripening of bananas, a hole is dug in the ground, lined with dried banana leaves which are then set on fire. Fresh banana leaves are laid on top of them, and then the unripe bananas.

The name **New Holland** was first applied to the western and northern coast of Australia in 1644 by the Dutch seafarer Abel Tasman, best known for his discovery of Tasmania (called by him Van Diemen's Land).

It doesn't have to be restricted to being at the company workplace, either. If you take company equipment home, the rules could apply to whatever you do with that equipment there as well.

And, of course, the rules vary from company to company, and in the worst case (or company), from moment to moment.

The real issue at hand? Your company could be watching. They could see everything you're up to. And there's really no way to know if they are.

The safest bet

Knowing nothing else about your specific workplace or situation, there's really only one position you can take: assume your activity is being monitored. Period.

The implications are also pretty simple: never do anything using workplace resources that might go against company policies or guidelines. Never do anything unrelated to your work. Never do anything that might cause your activity to raise red flags or otherwise cause problems.

Yes, that's harsh.

But with no additional information, we must assume the worst in order to avoid breaking possible rules, or the possibility of having our non-work activity examined in detail.

How common is monitoring?

The Wall Street Journal reports that since the COVID-19 pandemic, upwards of 60% of employers with over 500 employees use some form of monitoring.

That's a lot.

Here's the thing, though: all that monitoring requires resources — people — to act on any results. If you are being monitored, does it really matter if no one looks at the results? How are the results used? Real-time monitoring? Twice-a-year performance reviews? Only for specifically prohibited activities? Something else? Perhaps just an empty threat?

There's no way to know.

Even if you work for a small company, the risk of being monitored remains.

What to do

If you can, ask.

Ask your boss. Ask your HR department. Ask your IT department. Ask someone who knows exactly what the rules are.

- Am I being monitored?
- What kinds of activities are being recorded?
- Why? What is done with this information?
- What are the "rules" I'm supposed to adhere to that the monitoring is supposed to keep track of?
- What happens when I do something "wrong"?

Windows & Android Tips

Judy Taylour

5 SIGNS YOU NEED A NEW LAPTOP – You might be shocked to learn that the most reliable Chromebooks have an honest-to-goodness expiration date. Once that date is reached, it's trash. The Chromebook will not get any more patches or updates. Take a look at the clear-cut signs buying a new laptop is in your immediate future.
5 signs you need a new laptop (komando.com)

HOW TO CREATE BOOTABLE WINDOWS 11 USB INSTALL MEDIA – Here's the process to create a bootable USB drive to perform a clean install of Windows 11.
How to create bootable Windows 11 USB install media – Pureinfotech

WHY DO SMARTPHONES NO LONGER COME WITH REMOVABLE BATTERIES? – There are several reasons, learn about them here.
Q&A: Why do smartphones no longer come with removable batteries? (ricksdailytips.com)

WHY YOU SHOULD DELETE YOUR YOUTUBE HISTORY OFTEN (AND HOW TO DO IT) – Good news: You can delete some or all of your YouTube watch history to better curate your recommended video feed. Here's more on why you should do it often—and how to do it in a few quick steps.
Why You Should Delete Your YouTube History Often (and How to Do It) (lifehacker.com)

Straight answers should set your mind at ease. At least your company is (hopefully) being open with you and you know the boundaries of allowed activities.

Then it's your responsibility to stay within those boundaries, and monitoring shouldn't be an issue.

But what if?
What if you can't trust your employer?

What if you can't trust their answers to whether you're being monitored or how that information might be used? What if there isn't anyone you feel comfortable asking?

You have two options.

1. Assume the worst. Assume anything you say or do with your company-provided technology can and will be used against you if needed. Toe the line.

or

2. Find other employment that you can trust.

I totally understand that option #2 is not an option for many people. That leaves you with only the first.

Do this
You are right to ask the question. It's important, I think, to understand what your employer may or may not be monitoring and how that information may be used. It's important to understand just how much leeway you have as you perform your job.

Hopefully, most employers are honest and understanding when it comes to your activity.

Hopefully, your activities respect the needs of your employer as well.

But as we all know, all employers are not most employers, and we've all encountered employees who push the limits of responsibility when it comes to their work.

END OF ARTICLE # #

* * * * * SOFTWARE and HARDWARE * * * * *

A Cautionary Tale of Cloud-Based Apps

By Joel Ewing, President
Bella Vista Computer Club

Insteon Home Automation

Around 2014 I started using Insteon home automation devices to control some plug-in electrical devices around my house. Insteon produced several different modules using a proprietary peer-to-peer communication protocol to communicate with an Insteon hub in your house, which used an Ethernet connection to your router and your home LAN to connect to Insteon-owned cloud servers on the Internet.

Scams

DID YOU GET AN EMAIL SAYING YOUR PERSONAL INFO IS FOR SALE ON THE DARK WEB? – Before you act, read this Consumer Alert from the FTC. Did you get an email saying your personal info is for sale on the dark web? | Consumer Advice (ftc.gov)

BRUSHING SCAMS: HERE'S WHY YOU'RE GETTING RANDOM PACKAGES – Across the United States and other countries, millions of people are surprised to receive packages they never ordered. In most cases, the source is a scam called "brushing." Here's why you're getting free loot. Brushing Scams: Here's Why You're Getting Random Packages (howtogeek.com)

HACKERS WANT GOOGLE ACCOUNTS. GIVE YOURS THIS SECURITY CHECK NOW! – Your Google account is one of the most important things on your devices, especially if you're a Gmail user. Here's a simple way to ensure yours doesn't end up in the wrong hands. Hackers want Google accounts. Give yours this security check now! (komando.com)

6 WAYS EVERYONE CAN STAY PROTECTED ONLINE IN 2022 – Despite knowing all the dangers of the internet, we often forget just how easy it is to fall into scams or not take our internet safety seriously enough when browsing. This is how thousands of people have their sensitive data and money stolen online every month. 6 Ways Everyone Can Stay Protected Online in 2022 (makeuseof.com)

The Insteon devices and hub use a unique combination of wireless RF (not Wi-Fi) and powerline signaling. Each device module acts as a repeater to ensure all modules can communicate with the hub. In addition, there was a smartphone/smartpad Insteon app that, in concert with the Insteon cloud service, allowed you to schedule state changes (turn-on, turn-off, dim) for the individual Insteon modules, manually change the module state remotely, or monitor the condition of modules in the case of sensor modules.

The smartphone Insteon app allowed you to monitor the state of the various modules while away from your house as long as you had Internet access on your smart device. Manual remote control of lights from outside the house was not that useful to me but could, I suppose, be used to add some randomness to simulate people in an empty house or turn off a light unintentionally left on. On the other hand, remotely controlling lights or other plug-in devices while in your house from the comfort of an easy chair or bed was very convenient, as was the scheduling of lights that should always go on and off at regular times.

The peer-to-peer communication between the modules and the hub made the system very reliable. Over the years, I've only had one module fail -- after one of our cats marked it as his territory in the usual cat fashion. Unfortunately, I've also had two hubs die on me in four years. After the 2nd one failed, I did some research and found that I shouldn't have plugged the hub into a UPS, as some of the high-frequency components of the AC output of a typical home UPS unit running on the battery tends to stress the hub power supply and cause early failure. Since then, I've plugged the hub into an outlet with only surge protection and have had no other hardware failures.

The modules I found most helpful were those that would plug into a regular outlet and provide a module-controlled outlet for the controlled light or other device. The most useful aspect of these modules was that they could be easily moved and redeployed for a different use. Over the years, we acquired three different varieties: an un-grounded dimmer (which could be used as a switch), an un-grounded switch, and a grounded switch rated for outdoor use. We also acquired a water-leak sensor, which was deployed in a storage area under the house near the water heater.

Over the years, we have made good use of the Insteon system. For example, we have used Insteon to control several table lamps in several rooms, indoor and outdoor Christmas lights, and heating devices in the cats' outdoor houses. Until April 13 of this year, we had never (outside of testing) gotten a warning from the water-leak sensor, but it proved its worth when torrential rain and a drainage problem outside resulted in water under the house. The leak sensor did its job and made it possible to resolve the issue before damage could be done.

The Demise of Insteon

After the water-leak detector saved the day (talk about fortunate timing), our Insteon automation stopped working. Trying to use the Insteon iPhone app to manually control the lights also failed with the app's inability to log on to Insteon. The Insteon hub's normal green LED was red. It was unclear whether there was some failure in our hub or what. After some research, some people had been concerned about the

Virtual Tours

Great Wall of China
Often cited as the only human-made structure that is visible from space. The Great Wall of China is probably the most well known Wonder of the World. It captures over 2,000 years of history and stretches more than 21,000 km across several provinces in China. That's as long as 5 times the length of Australia! This iconic landmark is usually teemed with tourists all year round. But you can visit it crowd-free on this Great Wall of China virtual tour.

Chichen Itza, Mexico
The ancient city of Chichen Itza is one of the most well restored Mayan sites in Mexico and also its biggest tourist attraction. El Castillo may be the most famous pyramid of Chichen Itza, but there are many other ancient ruins to explore. If you love astronomy, you'll love learning how each structure was intricately designed to align with specific planets and stars. Sounds fascinating? You can virtually tour Chichen Itza and explore some of its most popular sites and facts right from the comfort of your own home.

Travel back in time
Nearly 5,000 years ago, outside the ancient city of Memphis, Egyptians built pyramids as tombs for their kings. These monuments are still standing today in the city of Giza. Zoom in to explore them. With modern technology, you can even see the last standing wonder of the ancient world—The Pyramids of Giza.

long-term prospects of Insteon in 2021, that others were now reporting similar failures like ours, and that the Insteon forum for discussing device problems also seemed to be down. One of the possibilities for a red hub light was an inability to communicate on the Internet, but Internet access was otherwise working. Power cycling the hub produced no change. The conclusion at the time was there was some problem with the Insteon Internet service, but no indication the problem was permanent.

After being down for a day, speculation continued to increase, but no official word. By April 16, the consensus finally became that "Insteon is dead." The only semi-official notification received was an email finally sent to my Insteon account email on April 21 from SmartLabs Inc (the parent company of Insteon) revealing "Insteon Users: Important Notice to Creditors": a notice dated April 12, indicating that SmartLabs Inc had on March 22 assigned its assets for liquidation. A week after the initial April 14 failure, the insteon.com website now has a general notice that "the company was assigned to a financial services firm in March to optimize the assets of the company," which I guess is legalese for "expect an end of all service on some arbitrary date after March 22". It's beyond me why they couldn't just spend the same amount of effort and have the website clearly state that all Insteon cloud services for support of Insteon hubs have been discontinued as of April 14, 2022, so people wouldn't have to guess what's going on.

I was a little ticked off that Insteon gave no heads-up on what was about to happen. Even notification as they pulled the plug would have been an improvement to avoid wasting time diagnosing a problem that couldn't be fixed. But, unfortunately, in retrospect, Insteon's business model probably doomed them: they provided a free Internet service with an increasing number of users and very little long-term income from those like me once they had all the automation modules they had needed. Add to that the reduced sales from financial and supply chain disruption during the pandemic...
Perhaps the lesson to be learned here is that products that require a free cloud service to function should be regarded as having planned obsolescence -- you don't know what the plan is.

There are alternatives, but for most people that aren't technically savvy, or have access to someone that is, this means that their Insteon hub and device modules have become expensive doorstops.

Finding an Inexpensive Free Alternative

Having to replace all your Insteon modules and hub with a different system and hardware means throwing out hardware that may represent a sizable investment of hundreds of dollars. Unfortunately, there don't appear to be any suitable commercially available solutions that can utilize the Insteon hardware.

A cheaper Open Source alternative can restore the functionality of an Insteon hub and all the Insteon modules. Still, it requires some technical expertise to set up another machine on your home network with a specialized Operating System. That machine could be a Raspberry Pi with 2 GiB RAM, or an older (but not too old) retired machine. On the other hand, if you have a system that runs 24x7 that can support running a Virtual Machine with a UEFI boot and that can be network

Unusual Product

Kailo - Futuristic Patch That Uses Nanotech To Relieve Your Pain

Problem: Are you still in pain from an injury or fall several years back? Has this pain limited your ability to do certain physical activities and sometimes keeps you up at night?

Kailo is a non-invasive patch that is filled with billions of tiny nanocapacitors. Kailo works with the body's nervous system. Each Kailo contains nano capacitors that work as a bio antenna, which in turn assists the body in its reaction to pain.

When you are feeling pain, all you need to do is stick a Kailo patch to your body. Within moments, you will feel the pain go away. Kailo is reusable and lasts for several years. The only maintenance involves replacing the adhesive every now and then as needed.

Kailo helps a lot more than just back pain--in fact, it has been known to help relieve pain pretty much anywhere you place it. It has really helped so many people with migraines, menstrual cramps, knee pain, and other joint pains. Since this nanotechnology is so new, people are still finding new uses for it every day. Learn more about Kailo by clicking on the link below.

https://gokailo.io/offer-01/

"bridged" to appear on your local LAN subnet, then it is possible to use a Virtual machine with 1.5 GiB of RAM. on existing hardware.

The Open Source software that will do the job is Home Assistant. The Home Assistant server is available in image downloads of Home Assistant OS (HAOS) for installation on an x86-64bit or Raspberry Pi architecture. In addition, there are corresponding Home Assistant (HA) apps for smartphones that will allow you to configure and control the Home Assistant server, or it can be done using any browser and the exact LAN IP address and port for the HAOS server.

Conceivably you could run Home Assistant OS on an older retired computer, but it would have to be recent enough hardware to support 64-bit architecture and UEFI (non-secure) boot. If you use a virtual machine rather than actual hardware, it is required to set up bridged networking so the virtual machine gets its address on your LAN. In the case of my Linux system and KVM virtual machines, bridged networking was the most challenging part of the process. The Home Assistant OS must be on your primary home LAN subnet for the iPhone apps to find the Home Assistant server and for the Home Assistant server to detect your Insteon hub (and other IoT devices in your house that it can support). It would probably also be a good idea to configure your router to assign a fixed LAN IP address to the Home Assistant server machine.

When configuring Home Assistant for your Insteon hub, you will probably need to supply the login name and password on the base label on the hub. Once it connects with the hub, it should go through device discovery and gradually locate all the powered-up Insteon modules, except perhaps for sensor modules. I had to press the reset button on the module to get it to see my leak sensor module. The LED light on the hub will remain red -- apparently, that only turns green if the hub can talk to the Insteon cloud server and no longer exists.

The discovered Insteon modules will initially only be identified in Home Assistant by their Insteon hex ID value of the form hh.hh.hh and by the module type. If you haven't saved documentation that maps the module IDs to their location, you may have to power modules On/Off from Home Assistant one at a time so that you can associate meaningful names with the modules. Where I had only one module of that particular type, the module type was sufficient to know the related module location.

The Insteon scheduling was in the Insteon cloud, which is all lost and will have to be built again on Home Assistant. The approach is different, but I found it more convenient than what Insteon used. In Insteon, a schedule belonged to a device, or you had to define a "scene" of multiple devices if you wanted a schedule to affect multiple devices; you couldn't have more than one schedule set to trigger at the same minute. In-Home Assistant, you have Automation Entities, which include one or more triggers that initiate the automation and one or more actions that should be performed when the automation is triggered. The actions can change the state of one or more device modules within the same automation definition. If an automation action is triggered while a previous action is still in progress, you can specify if and how you want them to interact. To me, the Home Assistant approach is more natural and more flexible.

If smartphones are running the Home Assistant app, one of the possible automation actions is sending a message to the HA app on that smart device. The connection between the server and the smart device

* * Jokes Stolen from Everywhere * *

Parking
Norman and his blond wife live in Fargo, SD. One winter morning while listening to the radio, they hear the announcer say, "We are going to have 3 to 4 inches of snow today. You must park your car on the even numbered side of the street, so the snowplow can get through." Norman's wife goes out and moves her car. A week later while they are eating breakfast, the radio announcer says, "We are expecting 4 to 5 inches of snow today. You must park your car on the odd numbered side of the street, so the snowplow can get through." Norman's wife goes out and moves her car again. The next week they are having breakfast again, when the radio announcer says "We are expecting 10 to 12 inches of snow today. You must park.....", then the electricity goes out. Norman's wife says, "Honey, I don't know what to do." Norman says, "Why don't you just leave it in the garage this time?"

What did E.T.'s mother say to him when he got home? "Where on Earth have you been?!"

Doctor's office: All our records are electronic now, just fill out these 12 forms.

I would like to thank everybody, that stuck by my side, for those five long minutes my house didn't have Internet.

You're old enough to remember when emojis were called "hieroglyphics."

So apparently RSVP'ing back to a wedding invite 'maybe next time' isn't the correct response.

app is by LAN IP address, which can only work while your phone is on your home network. I don't know if a message to a phone not currently on the home LAN is queued to be sent when possible or what. If it is an alert that you need to receive promptly no matter where you are, there is probably some way to do that (email?), I haven't had the time to research that yet.

There are ways to make a Home Assistant server running HAOS at your home accessible from the Internet, but to do this securely on your own is a non-trivial exercise. The native communication for the HA server on HAOS uses an insecure http protocol on port 8123. You wouldn't want to open that port to the HAOS system on your router because your HA login credentials would be sent over the Internet in the clear, potentially exposing your home automation to attack. I don't know how to do it yet, but I know there are ways to create an https secure interface that could be used to either directly or indirectly access the HAOS system. That, in turn, requires that you own (at an annual charge) an Internet domain name that is defined to point to your external Internet IP for your home, and if you don't have a business IP account with a fixed Internet IP address, you also need some process to update the IP address of your domain name if your Internet provider changes your Internet IP address. I see this getting complicated in a hurry. Suppose you only want access to your HA server from the Internet to receive notification alerts from HA on your iPhone when you are away from home. In that case, I think it may be less work to find solutions that address the notification issue.

There is another secure and simple option if you must have access to all your Home Assistant automation away from your home over the Internet, but it is not free. You can subscribe to the Home Assistant Cloud service provided by Nabu Casa, Inc. at either $6.50 monthly or $65 annually. This service offers a secure Internet interface between your smart device and their service, which in turn uses a secure interface to the Home Assistant machine at your house. Since it is a charged subscription service, it is probably more likely to stay around than Insteon's free cloud service, but that does mean you can again become dependent on a third-party cloud application that is not under your control and become locked into one more continuing payment for the indefinite future.

It took almost a week to get all the bugs out, mostly trying different ways to get a virtual machine properly bridged to my home LAN. Still, I finally got everything I needed working: automation with HAOS running on its own [virtual] machine with remote control over my home Wi-Fi and LAN from the HA app on iPhones, all controlling the Insteon hub and Insteon modules. I have found the HA interfaces and flexibility more convenient than what was originally provided by the Insteon apps and Insteon cloud servers. The best part is that all the pieces required to keep it working within my home are now under my direct control with no added cost but time.

Reprinted from the Bella Vista Computer Club,
president@bvcomputerclub.org.

Odds and Ends

NORTONLIFELOCK MERGES WITH AVAST TO FORM NEW COMPANY CALLED 'GEN' – NortonLifeLock has settled on a new company name after merging with antivirus provider Avast two months ago: Gen. The full name is actually Gen Digital. But the company is already promoting itself as Gen through marketing materials and on its website. The term doesn't exactly connote cybersecurity or antivirus. However, the newly merged company selected the name to underscore its focus on protecting "digital life." "We're all a part of a new generation, regardless of age. It's not Gen X, Y or Z, it's Generation Digital," says CEO Vincent Pilette, who was previously the head of NortonLifeLock. But despite the new name, all the separate brands will continue to live on. "Yes, nothing will change on that front. The company name and logo change won't impact their consumer brands," a spokesperson for Gen told PCMag.
NortonLifeLock Merges With Avast to Form New Company Called 'Gen' | PCMag

SPEC SHOWDOWN: THE ORIGINAL IBM 5150 VS. TODAY'S PCS – Just for kicks, let's compare the specs of the 1981-vintage computer that inspired the birth of PC Magazine to some modern-day desktops.
Spec Showdown: The Original IBM 5150 vs. Today's PCs | PCMag

Data Privacy Week (January 22 - 28, 2023) spreads awareness about online privacy, helping individuals understand how to manage their data and showing organizations why it is important that they respect their users' data. https://staysafeonline.org/

* * * * * BITS and PIECES in the NEWS * * * * *

Editor's Note: To continue reading the following articles, you may copy the long URL at the end of the article and enter it into a web browser **or** click on the URL in the PDF or web versions of this newsletter.

Lightweight with maximum surface area

Metal foams are used in many applications, including cooling and filtration. Start-up Apheros' novel metal foams offer unprecedented properties.

By Karin Kelly

Dr. Julia Carpenter from the Complex Materials Group at ETH Zurich is the co-inventor and driving force behind the young company. Her metal foams have a unique microstructure. Compared to existing products, they impress with very low weight, an extremely large surface area and the ability to absorb liquids. These properties are achieved through a newly developed production method and enable the use of these metal foams in various applications.

Cooling of electronic devices

By 2030, electronic devices will consume 23% of global energy. Almost half of this, 10% of global energy, will be used for cooling. Currently, so-called "heat sinks" are used. They are usually supported by energy-intensive fans and air conditioners. High-end applications also use liquid cooling systems with heat exchangers. Metal foams enable efficient cooling without consuming energy. They are ideal passive heat exchangers and do not require fans or air conditioning.

Continue at
https://ethz.ch/en/industry/industry/news/data/2022/12/lightweight-with-maximum-surface-area.html

Say hello to the toughest material on Earth

A new study reveals the profound properties of a simple metal alloy

DOE/Lawrence Berkeley National Laboratory

Scientists have measured the highest toughness ever recorded, of any material, while investigating a metallic alloy made of chromium, cobalt, and nickel (CrCoNi). Not only is the metal extremely ductile – which, in materials science, means highly malleable – and impressively strong

(meaning it resists permanent deformation), its strength and ductility improve as it gets colder. This runs counter to most other materials in existence.

The team, led by researchers from Lawrence Berkeley National Laboratory (Berkeley Lab) and Oak Ridge National Laboratory, published a study describing their record-breaking findings in *Science* on Dec. 1, 2022. "When you design structural materials, you want them to be strong but also ductile and resistant to fracture," said project co-lead Easo George, the Governor's Chair for Advanced Alloy Theory and Development at ORNL and the University of Tennessee. "Typically, it's a compromise between these properties. But this material is both, and instead of becoming brittle at low temperatures, it gets tougher."

Finish this article at https://www.eurekalert.org/news-releases/973788.

* * * * * CLUB and REGIONAL NEWS * * * * *

APCUG

Wednesday Workshops, December 28, 12 pm ET**, *'Learning Linux'***
The Linux Team: Orv Beach, Cal Esneault, John Kennedy, and Dave Melton
Register for this workshop - https://forms.gle/812YiZZmBb9NEED36

Due to the holidays, we've moved the December Linux workshop to the 4th Wednesday. We hope you have a very Happy Holiday season. As we wrap things up, we want to hear from you at the end of '22. The team is sure there are some lingering questions you might want to ask or topics you might want to clarify. Is there something you would like to see again, or do you want to share some great news about Linux? We want to hear from anyone and everyone. Whether you are new to Linux, someone giving it a try from what you've learned in these workshops, or a more experienced user that wants to share information with the group or be there to help answer questions. We are also looking for suggestions for what the Learning Linux Workshops should be in '23. If you want to get your questions or things you'd like to see on the agenda (so you are guaranteed to get an answer), please email the "Host" at jkennedy@apcug.org so the team can prepare the response or demo. See everyone at the end of the month.

RCSI

We had our first 'Pot Luck' video night with submissions about future tech predictions for the year 2030, lab grown meat and another on milk production, smart home devices and how to install them, building a PC while you still can and GPT-3 is replacing programmers. All were very interesting and informative, thanks to everyone. For those of you who missed out, don't worry, we will do this again in the future.

Got Questions?:

Send an email to either person below and they will get back to you. The questions can be related to the OS (Operating System) or hardware related issues. Please give them time for a response, as they do this service on a volunteer basis. Thank you.

Windows OS: . . . . . Arpad Kovacs, podcomputer@gmail.com

Linux & some Mac: Carl Schmidtmann, unixgeek@faultline.com

New Meeting Place

Our Usual Meeting Place is being renovated.

St John's Meadows at Johnsarbor Drive, is on the left, past Clinton Avenue, when going West on Elmwood Avenue. The opening in the white fence is Johnsarbor Drive. At the 'T', turn right. The meeting is in the SECOND building on the left – **Chestnut Court**.

Our meeting place can change. Please check our website before each meeting. **www.rcsi.org**