The Rochester Computer Society, Inc.

a computer/tech club open to everyone

M⬚NIT⬚R

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.* **Yes, you may bring the problem computer with you.**

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.

Feb 13, 'Best of CES 2024',

'Thunderbird Email Client', 'Calendar Apps'

Mar 12, TBD

In This Issue

President's Corner

Wyzedom - The Wisdom of Battery-Powered Products

Greg Skalka, President
Under the Computer Hood User Group

Batteries are the new normal. Throughout history, humans have found different ways to power their devices. Humans initially provided the power but soon enlisted animals to plow, power mills, and pull wagons. The industrial age was powered by burning fuels like coal and oil, which brought significant progress but released a lot of carbon dioxide into the Earth's atmosphere. We must transition to low- or carbon-free energy to reduce climate change. Electricity is the best medium to distribute that energy, and batteries are the primary way to store it. As we move into an all-electric world, we will need

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:
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
Features, Mac OS X & Windows
The New Space Race, 2021
Tech of South America
Internet Security and Privacy
AI and Digital Assistants
Emerging Technologies
My Favorite Android Apps

more electricity, batteries, and some good strategies for charging and disposing of those batteries.

When I look around my house, I see many things that are now powered, or now powered by electricity, but were not when originally invented. Toothbrushes, razors, can openers, corkscrews, safes, clocks, clothes washers – all these things were originally human or mechanically powered but now have electrically-powered versions.

Stoves cooked by chemical processes (burning fuel) and clothes were dried by natural processes (outdoor air on a clothesline). Still, these tasks are predominantly accomplished by using electricity (or soon will be, with the eventual elimination of residential natural gas). Automobiles, trucks, trains, and planes were all powered by burning fuels but are now on the path to eventual electrification. Many of these things are mobile, or at least would be hindered in use by being tethered by a cord, and so will need batteries to operate.

My house now has several electric items it didn't have before. My wife has bought some electric soap dispensers for the kitchen and bathroom. Instead of pressing down on the top of the bottle to dispense some liquid hand soap, you put your hand under the nozzle, and a sensor detects it and squirts some in your hand. It is more hygienic, but it has batteries that require replacement or recharging periodically, and it is just another device that can break. Do we really need it?

How many battery-powered devices do you think you have in your home? Ten? Twenty? Fifty? One hundred or more? I don't know how many I have, but it could well be that last guess. I pondered this question recently as I sat on the only seat in our master bathroom. From that vantage point, I could see nine devices that contained a battery, with another two that I knew were nearby in cabinets. Multiply 11 by the number of "rooms" in our house, and we would have over one hundred batteries to deal with.

These bathroom devices I found are probably a fairly representative sample of the types of battery-powered devices we own and fall into two classes, depending on if the batteries can be removed. Six of them (two electric toothbrushes, a shaver, a Bluetooth speaker, a face scrubber, and one hair trimmer) have rechargeable batteries that can't be removed. The other five (wall clock, clock/thermometer, flashlight, another hair trimmer, and a bathroom scale) have replaceable batteries. These five typically use disposable single-use batteries, though all but the wall clock (which is powered by a coin cell battery) use AA or AAA batteries, which would allow the use of rechargeables.

Being powered by batteries does not limit the usefulness of any of these bathroom devices. The toothbrushes are charged inductively through their holders and can stay charged constantly; their charging

is transparent to the user. The other four devices that don't have removable batteries must be plugged into a wall outlet to recharge, but since a full charge typically provides many uses, we are seldom caught with a dead battery. My shaver, for example, can go for well over a week of normal use on one charge, so I typically plug it in to charge after I have used it on Sunday mornings. It charges fully in an hour or so before I need it again. Like the hair trimmer and face scrubber, it also can be used in a pinch while charging; having a cord does not significantly degrade its usability. The remaining devices with removable batteries either have a long battery life (typically years for the clocks and scale) or rely on a quick battery change to keep going.

Moving from the bathroom into the bedroom, I find only slightly fewer battery-powered devices. There are remote controls for the TV, cable box, DVD player, ceiling fan, and window air conditioning unit. A couple of flashlights, a clock, and a cordless phone are in its charging base. These fall into the same two battery categories and present no particular problems to the user by being powered by batteries (other than having some replacement batteries on hand when needed).

Moving from the bedroom to the hall, I see one of my favorite battery-powered devices, the Wyze night light. These small stick-on lights can be used to illuminate your path at night. They detect your motion and turn on, and can be linked to turning on a series of them when triggered. I have a set of three on my stairs (top, middle, and bottom) to keep me from falling and breaking my neck in the morning when it is dark, and I don't want to wake my wife by turning on the ceiling light fixtures.

I love my Wyze lights, but keeping them charged can be problematic. In normal use in my stairs location, they run for about three weeks on a charge. I have come to rely on them to light my way, and so I do not want to wait until they are discharged. I initially tried charging them on a two-week schedule, taking them down (they are magnetically attached and easily removed) every other Sunday. They must be charged during the day when not needed and take about 2 hours to charge fully from a USB charging source. The Wyze lights have a USB-C connector, and to protect that connector, I use USB magnetic charging cables and adapters.

The problem in charging the Wyze lights came from having to charge each one separately. I initially used one USB AC charger and cable and had to charge the three lights sequentially. This took at least six hours, and I had to be around most of the day on Sunday to swap them on the charger. Occasionally I was not, so I sometimes had problems getting all three lights charged before dark.

I celebrated with the First Lady most of the day on Mother's Day and did not get my Wyze lights charged before dark. I decided to find a better way to charge these lights. Possible solutions to my problem included:

1. Faster charging – The process would not take all day if each light could charge faster. This would require some investigation to determine if this would be possible.
2. Parallel charging – If I could charge all three lights simultaneously, it would take 1/3 of the time, and I would not have to hang around to swap lights on the one charging station. It would require buying a three-output USB charging station and two more USB charging cables.
3. Have an alternate set of lights – If I bought a second set of Wyze lights, I could charge the alternate set over the two weeks and then swap them all out at once. This would be the fastest and most versatile but requires buying another set of lights.

I first investigated if faster charging was possible. I bought a MakerHawk USB 3.0 Tester from Amazon a while ago; it can be used

to test USB-powered devices and USB cables and to monitor USB charging. Connected between a USB charging source and a device to be charged, it can display the voltage, current, power, charging mode, and other things.

I used the USB 3.0 tester while trying to charge a Wyze light with several different power sources (USB AC charging cubes and USB power source batteries) and several other USB cables. No matter what combination of source and cable I used, the power into the Wyze light remained between 0.951 W and 0.976 W. A higher power into the light would be needed to charge faster, so it appears speeding up charging is not possible.

I found another dual-output USB charging block and a couple more cables in my household stock and set them up in the spare bathroom I use for charging. This method worked well, and I could set them up and walk away, knowing they would all be charged when I remembered and returned.

Using another set of Wyze lights as a charging spare might be slightly easier, as I could charge them sequentially at my leisure over the two-week operating period. It would, however, require buying another $26 set of lights, and I'd still have to keep track of which lights are charged and which are not.

Ultimately, I've found the parallel charging method works the best for me. It gets the lights all charged at once and has the benefit of

Bats have one way valves in their arteries which prevent blood from flowing backwards. This is why they are able to hang upside down, without the blood rushing to their heads.

American alligators are cold-blooded reptiles and can grow from 6 to 11 feet long and inhabit wetland areas. American alligators thrive in bayous, lakes, and some golf courses and are found in Louisiana and Florida.

Horses' eyes are located on the sides of their heads, so they have a wide field of vision. They can see nearly 360 degrees and have blind spots only immediately in front and behind their bodies.

Toads are actually just a type of frog. Often, toads have a drier, bumpier (warty) skin and prefer drier habitats. They usually have shorter hind legs and rounder stouter bodies than most typical frogs.

Just like your bones, a turtle's shell is actually part of its skeleton. It's made up of over 50 bones which include the turtle's rib cage and spine. A turtle cannot come out of its shell.

With over 20,000 species of bees in the world, most are not honey bees. They are only a small part of the many types of bees found worldwide. Honey bees are the only insects that produce quantities of food for human consumption.

having the "charging station" set out for less time, which makes my wife happier. I've now adopted this charging method for my bike lights and switched to charging my front and rear rechargeable safety lights simultaneously rather than sequentially.

Reprinted from www.uchug.org, president@uchug.org.

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

Do You Know the Preferred Tool of Online Criminals?

By Bob Rankin
a Translator for the Technology Impaired
offering Free Tech Support

It's been 45 years since the first spam email was sent, and it's still the favorite tool of crooks and criminals online. A report from security group F-Secure says that spam is the most common method used to distribute malware, phishing attacks, malicious URLs, and scams. Read on to learn the tell-tale indicators of malicious emails, and the true origin of spam...

Spam: Still Number One With Crooks

You've got software to protect your computer from viruses, spyware, ransomware, and rogue websites. You're careful to keep all your software up to date. Your identity theft spider sense tingles with every suspicious phone call. But then that innocent-looking email pops into your inbox. It appears to be from your friend, your bank, or your favorite online store.

I got one recently that said "A user has just logged into your Facebook account from a Samsung S10 device. We are sending you this email to verify that it is you. Thank you, Facebook Team." It looks very much like the actual account warnings that Facebook does send out. The subject line says "Please respond immediately."

So you click, and you've been had. Because of the sense of urgency created by this message, one might ignore the fact that it was sent from "ebxjwwptsoqwvbbqjivcqpoduuxdur.com.au" (clearly not Facebook HQ) and that there were 50-odd sketchy addresses in the Reply-to header.

Spam is still the most effective attack vector for hackers and online criminals, according to research from F-Secure. They reported that phishing, spam, and other email threats were the source of 51% of all attempted malware infections. Hopefully you were not in the 51% Club.

Cybercriminals capitalized on fear and confusion during the Covid-19 pandemic, and continue to use malicious email attachments containing infostealers – malware that steals passwords and other sensitive information. Facebook, Chase Bank, Microsoft, PayPal, and Bank of America were the most frequently spoofed brands. As usual, cybercriminals are taking their cue from water -- by traveling along the path of least resistance.

Here are some of my tips for staying safe from phishing attacks. First, see my article How Hackable is Your Password? to learn how to **maintain strong, unique passwords** for all accounts and change

HANDS ON WITH MICROSOFT COPILOT IN WINDOWS 11, YOUR LATEST AI ASSISTANT – The first generative AI built into an operating system is here. We take Microsoft Copilot out for a spin. **Hands On With Microsoft Copilot in Windows 11, Your Latest AI Assistant | PCMag**

MICROSOFT OFFICIALLY INTRODUCES COPILOT FOR WINDOWS 11 – Microsoft said that its new AI companion will be available starting on September 26, 2023, as part of the new Windows 23H2 (2023 Update) features. The chatbot is also expected to be available on Microsoft 365 apps and services, Outlook, and Microsoft Edge (formerly Bing Chat on the browser). Microsoft officially introduces Copilot for Windows 11 – Pureinfotech

LASTPASS: 'HORSE GONE BARN BOLTED' IS STRONG PASSWORD – The password manager service LastPass is now forcing some of its users to pick longer master passwords. LastPass says the changes are needed to ensure all customers are protected by their latest security improvements. But critics say the move is little more than a public relations stunt that will do nothing to help countless early adopters whose password vaults were exposed in a 2022 breach at LastPass. LastPass: 'Horse Gone Barn Bolted' is Strong Password – Krebs on Security

them regularly. **Enable two-factor authentication** wherever possible. See [DIGITAL LOCKDOWN] Authenticator Apps Protect Your Accounts. And **keep your software and systems up to date** by following my advice in Keep Your Software Updated (or else...).

F-Secure says these phishing campaigns are effective because users are already accustomed to receiving notifications... failure of delivery emails, alerts for hitting storage limits, requests for reactivation, or package delivery notfications, and 'update your password' emails.

Keep in mind that spam and phishing can take the form of text messages as well as email. I wrote about bogus "account services" and package delivery scams in [SCAM ALERT] Smishing is Getting Worse (what you need to know and do).

As software vulnerabilities are closed and anti-malware suites grow more capable, spam becomes relatively more effective compared to hacking and exploitation of software vulnerabilities. Spam still is infinitely scalable, too; it costs nearly nothing to blast out millions of spam emails from a compromised machine, and spambot networks of thousands of slave machines are commonplace.

While success still depends on spewing out millions of spam emails to get a handful of "bites," spammers are constantly refining their techniques and improving their batting averages.

Why Do People Click?
According to F-Secure, here are some clues as to what makes phishing spam successful:

- The probability of a recipient opening an email increases 12% if the email claims to come from a known individual
- Having a subject line free from errors improves spam's success rate by 4.5%
- A phishing email that explicitly states in its call to action that it is very urgent gets less traction than when the urgency is implied

Most users have finally learned not to click on email attachments sent by strangers, or any attachment that comes unexpectedly. So more phishing emails include URLs instead; people are still conditioned to click on links to see where they go, especially if the link says "click on this link..."

The link often does not lead directly to a malicious site, but to an innocuous site that redirects traffic to a malicious site. That way, the bad guy avoids detection by automated analysis software that previews links and compares them to known malicious URLs.

Here are some of the most common phishing tactics:

- The Fake Tech Support scam: An email arrives with a warning that your computer has been compromised with malware, and directs you to click a Norton or McAfee link to scan your computer, or call a bogus Microsoft Tech Support phone number.
- The Suspicious Activity scam: An email claiming to be from your bank says there is suspicious or unusual activity on your account. It may ask you to respond with your username and password.

Scams

Disaster Relief Scams

Humanity often unites to offer support and aid in the wake of natural disasters. Unfortunately, scammers also seize these moments to exploit the generosity of individuals. Whether it's a pandemic or natural calamities like the Japan Earthquake in January 2024, scammers tend to take advantage of this.

AI-Powered Scams

In 2024, Generative AI's meteoric rise isn't just impressive; it's a double-edged sword, exposing consumers to unprecedented risks. Scammers, ever the opportunists, will ride this AI wave, honing their deception skills to new heights. AI-powered scams will now play the role of digital chameleons, using sophisticated algorithms that blur the line between human-like and fraudulent behavior.

Tech Support Scams

Scammers pose as tech support agents, convincing individuals that their devices have issues and requesting remote access or payment for unnecessary services.

Text Scams

Just like phone scams, text scams have become increasingly sophisticated and pervasive in exploiting digital communication for deceptive purposes. These scams leverage the immediacy of text messages to trick individuals into divulging personal information or falling for fraudulent schemes.

Fraudulent Links

Phishing emails contain disguised links that, when clicked, redirect users to fraudulent websites designed to collect login credentials or install malicious software.

- The HR/IT scam: You get an email that appears to be from your employer's Human Resources or IT department. You may be directed to update employee information, or download an app.
- The UPS/Fedex/USPS scam: An email or text advises you that a package cannot be delivered due to incorrect shipping information. You are urgently advised to click a link or your package will be returned or discarded.
- The Amazon/Apple scam: A message informs you that you've ordered some expensive item from either Amazon or Apple, and asks you to login and confirm the purchase.

In every case, a careful examination of the sending address, or a phone call to verify the sender will reveal that it's unwise to continue. Never trust the phone number or email address provided in the message.

Another technique I've seen lately is a quick email asking "Sorry to bother you, do you order from Amazo n?" If you engage with this scammer, he or she will spin a tale of how they had a problem buying an Amazon gift card for a sick friend's birthday, and ask if you would kindly do so, with a promise that you'll be reimbursed. I can't imagine who would fall for that obvious scam, but apparently there really is a sucker born every minute.

A BIT OF HISTORY: I mentioned in the opening of this article that the first spam message was sent over 45 years ago. That happened in May 1978 when a marketing executive for Digital Equipment Corporation sent an unsolicited email to 397 ARPAnet addresses, with an invitation to a product demonstration. The term "spam" was not applied to unsolicited messages until April 1993, and according to Wikipedia, is thought to derive from a Monty Python comedy sketch "in which a group of Vikings sing SPAM, SPAM, SPAM... at increasing volumes." It was adopted to refer to "unsolicited commercial electronic mail sent to a large number of addresses, in what was seen as drowning out normal communication on the internet." So now you know.

F-secure includes tips for security-conscious people in its security blog. Some recent topics include ransomware, stalkerware, and account takeover. F-Secure predicts that the use of phishing tactics as a lure, using office documents as an infection vector, and the use of cloud services to host malicious content, will likely continue.

The good news is that with education and software, we have eliminated or limited many malware attack options to spam. The bad news is that spam still works. My best advice: Think twice before you click.

Your thoughts on this topic are welcome. Post your comment or question below...

From the website of Bob Rankin,
https://askbobrankin.com/
do_you_know_the_preferred_tool_of_online_criminals.html.

Virtual Tours

Ljubljana, Slovenia
Not content with 360° photos, Ljubljana opts for 360° videos. If you have a VR headset (like Google Cardboard for example), you can get a truly immersive experience. Otherwise, it's easy to spin around and enjoy what's on offer.
https://www.visitljubljana.com/en/visitors/explore/ljubljana-360-degree-sightseeing/

Wildlife of Canada live cams in various national parks
https://www.pc.gc.ca/en/nature/science/controle-monitoring/cameras

A virtual stroll in **old Quebec.**
https://www.youtube.com/watch?time_continue=12&=&v=9Gori011U4E&=&feature=emb_logo

Journey behind the **Niagara falls** virtual tour.
https://www.niagarafallstourism.com/vr/journey-behind-the-falls/

Visit the **Amazonas rainforest.**
https://www.conservation.org/stories/virtual-reality/amazon-under-the-canopy

Tour the **Guilin Mountain** in China.
https://www.airpano.com/360video/vr-guilin-china/

China glass bridge virtual tour
https://www.airpano.com/360video/vr-china-glass-bridge/

Tech Magazines, now Websites

By Dick Maybach
Brookdale Computer User Group

When PCs arrived in the 80s, bookstores were full of hobbyist magazines, such as PC Magazine, PC World, and Dr. Dobbs Journal. Now, most PC users consider their devices to be appliances rather than hobby equipment, and magazines have disappeared. However, a few enthusiasts remain, as do publications that support them, but most now as websites. These are not where you go to find problem solutions but to learn about new developments and tutorials. Here are a few examples.

PC Magazine appeared once or twice a month in my mailbox, and I would read every page. It now is a website, https://www.pcmag.com/, that covers **Macs and PCs**. The website covers more topics than its print predecessor and includes product, advice, and tech news reports. There is a search feature to help you find past articles that interest you. As with all websites, the content evolves continually, so if you see something interesting, you may wish to save the article or its URL. In addition, you can subscribe to special-topic newsletters (what's new, lab reports, tips, tricks, etc.), apparently at no cost.

PC World is also still alive and well, https://www.pcworld.com/. The topics are less wide-ranging than those on the PC Magazine site and are mainly limited to PCs. However, they also have free newsletters, and you can subscribe to their digital magazine for about $20 per year to relive the print magazine experience.

See Tom's Hardware, https://www.tomshardware.com/, for **information on PC components**. Unfortunately, this never appeared in print and is formatted as a traditional website rather than a periodical. You'll find detailed reviews of motherboards, CPUs, monitors, storage devices, other peripherals, and complete computers here. There are also tutorials on building and testing PCs and forums where you can ask questions and exchange views. Although the name implies, this is a one-person project, a sizable staff supports the site.

If you're looking for tutorials or help to **solve PC problems**, check Computer Hope, https://www.computerhope.com/tips/index.htm. Unfortunately, this, too, has existed only as a website. If you need information or help on specific topics, this may be a better site than the general-information ones above. In addition, its coverage includes Linux, while the first three above appear to be limited to Windows and Macs.

Full Circle Magazine, http://fullcirclemagazine.org/, is a 60 to 70-page monthly publication covering primarily **Ubuntu Linux**, although much of the material has a wider scope. Unlike the sites discussed above, this magazine began publication in 2007 and continues today. You can read or download the issues online as PDFs or EPUB files. The monthly issues cover Ubuntu primarily, but there are also special issues on such topics as the Python language and LibreOffice. But, like print magazines, once an issue is published, it doesn't change.

Raspberry Pi users have MagPi, https://magpi.raspberrypi.com/, a 100-page monthly, available as a download or in print. The first issue was published in 2012. Like Full Circle, you can read and download the issues for free, although they

Interesting Internet Finds
by Steve Costello
scostello@sefcug.com

How To Swap Out Your Wi-Fi Router Without Disconnecting All Your Smart Home Devices
https://www.theverge.com/23453354/keep-smart-home-devices-online-replace-wifi-router-how-to
If you are upgrading your Wi-Fi router or thinking about it, check out this post first to avoid potential problems.

New Send To Kindle Webpage Can Send EPUBs And Documents To Kindles
https://blog.the-ebook-reader.com/2022/11/17/new-send-to-kindle-webpage-can-send-epubs-and-documents-to-kindles/
The desktop apps still don't support EPUBs as yet. I have been using the webpage referenced in this post, which works well. It is much easier than opening my email to send the EPUB.

Why You Should Consider Using DuckDuckGo As Your Search Engine
https://www.makeuseof.com/why-consider-duckduckgo/
I use DuckDuckGo as my default search engine in all my browsers and the DuckDuckGo browser app on my Android devices. Check out this post to learn why you should be doing the same.

request a donation. Many articles describe hardware and software projects, often with a link to step-by-step instructions. This is an essential resource if you are working with a Raspberry Pi.

Arduino users should check the blog on the Arduino website, https://blog.arduino.cc/. This blog, not a magazine, is made of short articles describing Arduino projects with links to more complete descriptions. Since the content changes continually, you'll want to record the URLs of those that interest you.

This has been a sampling of some resources available to those interested in PCs, and many more may suit you better. With the decline of printed publications, it's easy to use the Internet only to find solutions to specific problems, which can narrow our focus. However, in the early days of PCs, print magazines continually exposed us to new products and ideas, which websites like those discussed here can do today. PCs are wonderful aids for exploring and growth; losing this resource would be a shame.

From the newsletter of www.bcug.com, n2nd@att.net.

* * * * * 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.

Cybersecurity Guru Mikko Hyppönen's 5 Most Fearsome AI Threats for 2024
AI giveth and AI taketh away   January 1, 2024

Mikko Hyppönen has spent decades on the frontlines of the fight against malware. The 54-year-old has vanquished some of the world's most destructive computer worms, tracked down the creators of the first-ever PC virus, and sold his own software since he was a teenager in Helsinki.

In the intervening years, he's earned Vanity Fair profiles, spots on Foreign Policy's Top 100 Global Thinkers, and the role of Chief Research Officer at WithSecure— the largest cybersecurity firm in the Nordics.

The ponytailed Finn is also the curator of the online Malware Museum. Yet all the history in his archives could be overshadowed by the new era in tech: the age of artificial intelligence.

"AI changes everything," Hyppönen tells TNW on a video call. "The AI revolution is going to be bigger than the internet revolution."

As a self-described optimistic, the hacker hunter expects the revolution to leave a positive impact. But he's also worried about the cyber threats it will unleash.

* * Jokes & Quotes Stolen from Everywhere * *

LIARS:

My wife told me she is a compulsive liar.
I'm not sure whether to believe her or not.

Ghosts are terrible liars.
You can see right through them.

Liars are just unbelievable!

Her: You're such a liar! You said you have between 10 and 15 million dollars.
Him: I didn't lie. I have 25 bucks.

"I told you Doc!! I've got fatigue and my heart keeps skipping a beat! Why do you keep calling me a liar?
Doctor: "Sir, I'll say it again, that's A Fib!"
Sorry, It's not a good hearted joke.

Getting quite tired of my friends calling me a pathological liar.
Being the head of the NSA during the week and captaining the International Space Station on the weekends can be very exhausting.

Soup lovers are all liars.
You can never put too much stock in them.

I have a problem with lying.
I just made that up.

I can always tell when someone is lying just by looking at them.
I can tell when they're standing too.

Today on the bus, I caught an absolutely disgusting low lying old pervert watching Porn..........
.......Over my shoulder!!!

At the dawn of 2024, Hyppönen revealed his five most pressing concerns for the year to come. They come in no particular order — although there is one that's causing the most sleepless nights.

1. Deepfakes
2. Deep scams
3. LLM-enabled malware
4. Discovery of zero-days
5. Automated malwareThe perilous path to AGI

Get the TNW newsletter
Get the most important tech news in your inbox each week.

Read the details on https://thenextweb.com/news/mikko-hypponen-5-biggest-ai-cybersecurity-threats-2024.

Researchers Create First Functional Semiconductor Made From Graphene

The technology could allow for smaller and faster electronic devices and may have applications for quantum computing.

By Catherine Barzler, Thursday, January 4, 2024

Researchers at the Georgia Institute of Technology have created the world's first functional semiconductor made from graphene, a single sheet of carbon atoms held together by the strongest bonds known. Semiconductors, which are materials that conduct electricity under specific conditions, are foundational components of electronic devices. The team's breakthrough throws open the door to a new way of doing electronics.

Their discovery comes at a time when silicon, the material from which nearly all modern electronics are made, is reaching its limit in the face of increasingly faster computing and smaller electronic devices. Walter de Heer, Regents' Professor of physics at Georgia Tech, led a team of researchers based in Atlanta, Georgia, and later in collaboration with colleagues at the Tianjin International Center for Nanoparticles and Nanosystems at Tianjin University in China, to produce a graphene semiconductor that is compatible with conventional microelectronics processing methods — a necessity for any viable alternative to silicon.

In this latest research, published in *Nature*, de Heer and his team overcame the paramount hurdle that has been plaguing graphene research for decades, and the reason why many thought graphene electronics would never work. Known as the "band gap", it is a crucial electronic property that allows semiconductors to switch on and off. Graphene didn't have a band gap – until now.

"We now have an extremely robust graphene semiconductor with 10 times the mobility of silicon, and which also has unique properties not available in silicon," de Heer said.

Wow! A major breakthrough.
https://research.gatech.edu/feature/researchers-create-first-functional-semiconductor-made-graphene.

Odds and Ends

Bionic Glasses 'seeing' Through Sound

Breakthrough technology is transforming the way people, who are blind or low vision, navigate the world around them.

What does a smile sound like? It's a question that's preoccupying some of the world's leading experts in the fields of machine and human perception — and now, it's driving the development of next-generation bionic glasses for people who are blind or low vision.

Called ARIA, the wearable technology has emerged from years of painstaking work by Sydney start-up ARIA Research and researchers from the University of Technology Sydney and the University of Sydney.

ARIA is a non-invasive device that can be worn like ordinary glasses. It's equipped with a camera and other sensors that collect data about the surrounding environment and objects within it; this information is transmitted via audio cues that help users visualise the world around them.

Imagine an ARIA user arriving for coffee at a friend's house. ARIA's audio information explains the layout and the user's position within the space, enabling them to navigate the environment independently.

https://www.uts.edu.au/ research-and-teaching/ research/explore/impact/ bionic-glasses-seeing-through-sound.

Inhalable Sensors Could Enable Early Lung Cancer Detection

The diagnostic, which requires only a simple urine test to read the results, could make lung cancer screening more accessible worldwide.

Anne Trafton | MIT News, January 5, 2024

Using a new technology developed at MIT, diagnosing lung cancer could become as easy as inhaling nanoparticle sensors and then taking a urine test that reveals whether a tumor is present.
The new diagnostic is based on nanosensors that can be delivered by an inhaler or a nebulizer. If the sensors encounter cancer-linked proteins in the lungs, they produce a signal that accumulates in the urine, where it can be detected with a simple paper test strip.

This approach could potentially replace or supplement the current gold standard for diagnosing lung cancer, low-dose computed tomography (CT). It could have an especially significant impact in low- and middle-income countries that don't have widespread availability of CT scanners, the researchers say.

"Around the world, cancer is going to become more and more prevalent in low- and middle-income countries. The epidemiology of lung cancer globally is that it's driven by pollution and smoking, so we know that those are settings where accessibility to this kind of technology could have a big impact," says Sangeeta Bhatia.

To help diagnose lung cancer as early as possible, the U.S. Preventive Services Task Force recommends that heavy smokers over the age of 50 undergo annual CT scans. However, not everyone in this target group receives these scans, and the high false-positive rate of the scans can lead to unnecessary, invasive tests.

Bhatia has spent the last decade developing nanosensors for use in diagnosing cancer and other diseases, and in this study, she and her colleagues explored the possibility of using them as a more accessible alternative to CT screening for lung cancer.

The researchers tested their diagnostic system in mice that are genetically engineered to develop lung tumors similar to those seen in humans. The sensors were administered 7.5 weeks after the tumors started to form, a time point that would likely correlate with stage 1 or 2 cancer in humans.

Read the whole article at https://news.mit.edu/2024/inhalable-sensors-early-lung-cancer-detection-0105.

Experimental System Uses Microwaves to Cook Crop Pests in Soil

By Ben Coxworth, December 18, 2023

Just like any other organisms, crop-destroying soil microbes die if they get too hot. With that fact in mind, scientists have developed a new system in which soil-heating microwaves are used to kill such pests. The technology could one day replace the use of environmentally harmful pesticides.

Developed by Dr. Sunshin Jung and colleagues at the Korea Electrotechnology Research Institute (KERI), the setup incorporates a proprietary antenna that emits microwaves down into the soil.

By selectively increasing or decreasing the wavelength and phase of those waves, it's possible to space them in such a manner that they meet and overlap at specific points underground. The amplitude of the waves is increased at those points, causing the moisture in the soil to heat to a temperature of 60 to 100 °C (140 to 212 °F) – the exact temperature can be adjusted via the antenna.

In its current form, the system is able to heat soil to a depth of 30 cm (11.8 in). Jung and his team believe that this should be sufficient for eradicating harmful microbes such as bacteria, fungi and nematodes which live on or near plants' roots – although unfortunately, beneficial microbes would likewise be affected. By contrast, a weed-killing microwave setup developed at the University of Melbourne only reaches down 5 to 10 cm (2 to 3.9 in).

The microwave apparatus could conceivably be towed through fields behind a tractor prior to seeding

Korea Electrotechnology Research Institute

The KERI technology is now in the process of being commercialized by industry partner Jooeun Care Farm Co. It could conceivably also find use in applications such as non-destructively killing termites in wooden structures, melting ice on winter roads, or cleaning oil-contaminated soil.

"We took advantage of the wave nature of microwaves, directing them to superimpose, not spread, and heat the soil underground," said Jung. "This technology helps to kill pests residing underground after harvest without the use of pesticides, their side effects and environmental pollution, and will contribute a lot to agricultural productivity and farmers' income."

<div align="center">Source: National Research Council of Science and Technology via Newswise</div>

CLUB and REGIONAL NEWS

For anyone who would like to do some additional reading about various topics ranging from software, or hardware and their implementations, you can check out Mark Zinzow's blog at **https://mszinzow.blogspot.com/**. He has given several presentations over the years (some by Zoom) and is a proponent of open software and security. The latter is a real battle today, with all the hackers and scammers out there trying to trick us into giving out our secret financial information. Additional places to find Mark, **https://www.zguru.us/**, **www.slideshare.net/msz**, and on **youtube** (search for Mark Zinzow).

If anyone else has a blog, let me know and it can be included in this newsletter.

WOW! The new Maker Space at RIT, called The SHED (Student Hall for Exploration and Development) was dedicated on 1/18/24 and is incredible. Three floors with 45+ 3D printers, lazer cutters, electronics galore, quilting machines, industrial fabrication, and rooms for arts, dance, and clubs.

Our Meeting Place
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**

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