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. 43, No.6 web: www.rcsi.org Rochester, NY June, 2024

June 11, "Human-Computer Interaction", "What are Chiplets", "Latest Tech Products"

*** * July and August, summer hiatus – No Meetings * ***

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.

In This Issue

Will AI Replace Search Engine Optimization	Caleb Peter
Safeguarding Your Finances	BrandPoint
Faheem A Zaidi	
Craigslist, Scammers and Schmeckpepers	Bob Rankin
Windows 11 Will Soon Be Encrypted by Default	Arol Wright
Scammers Are Bombing Apple Devices	Simon Batt
Bits and Pieces in the News	RCSI editor
Mercedes Becomes First Automaker to Sell Level 3 Self-Driving Direct to US Consumers	
NASA's Proposed Plasma Rocket	
Unlocking the True Power of Clean Geothermal Energy	
Club and Regional News	
Humans are the Nuts and Bolts of RIT Robotics Research	

Will AI Replace Search Engine Optimization (SEO)?

By Caleb Peter, March 12, 2024

The proliferation of search engines like Google and Bing has provided new business opportunities. Businesses no longer spend a lot of money on display advertising.

Ranking on these search engines is almost free but requires a lot of effort. Some of the effort you must make is to adapt to regular changes.

Since 2020, Google has made over 30 core updates to its ranking algorithm. A core update introduces major changes to how the search engine ranks webpages in its index. That means when a core update is made, you're likely to either be swept under the carpet or even improve your rankings overnight. To sustain your rankings in search

"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:
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

engines like Google, you must remain updated about these core updates.

Now, forget about the need for staying updated about Google's core updates. There are other factors you can't ignore to sustain your rankings. Other technological innovations are taking place that directly affect your Google search rankings. One of them is artificial intelligence (AI).

The launch of ChatGPT and Google's Gemini have paved the way for the proliferation of AI tools. Many people are rushing to enroll in AI courses to stay updated with current technological developments. And of course, search engine optimizers have not been left behind. They are also worried about whether AI will replace them.

Since mid-2023 onwards, one of the questions I have been encountering as someone directly engaged in managing content solution services at Scribble Bridge is, 'Will AI replace SEO?' This is a question commonly asked by our writers and SEO experts. Some clients have also asked me the same question.

It shows that people are anxious about the impact of AI on SEO. Content creators who specialize in SEO fear being replaced, and content marketers fear being blind to the role and effect of AI on SEO.

To address this anxious situation, I embarked on researching the impact AI has already had on SEO. I engaged in a deep reflection session and contacted top content managers, marketers, and some top content writers.

Now, before I mention how AI is shaping SEO, it is important to pay attention to the fact that AI has been around for some time now. Google introduced an AI-based algorithm called RankBrain in 2015. This algorithm is capable of understanding user intent in search queries. This update further eliminated the need for traditional keyword optimization, where it was initially recommended to place the exact keyword in your content after every 50-100 words. Nowadays, if your article answers the user's question or addresses their intent, regardless of keyword placement, you can still be valuable in the eyes of Google. When we ask whether AI will replace SEO for content marketers and managers, it's probably because we're looking for ways in which AI can enhance our SEO efforts. When I've talked to content managers and marketers like you, they've told me some of the ways they're using AI for SEO:

- Developing content briefs and outlines.
- Proofreading content and improving engagement with the target audience.
- Optimizing keyword placement within the content.
- Analyzing SEO trends and predicting the future to stay ahead.
- Writing meta-info sections of their websites, like meta-descriptions and meta-titles.
- Using AI and machine learning algorithms to track user behavior on their websites and improve user experience, a positive SEO signal.

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:
By Judy Taylour
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/

These ways in which content managers and marketers use AI for their SEO efforts have revealed something to me based on my 15 years of experience in the content writing industry. If you're a content creator like me, you'll almost certainly agree that AI cannot and will not replace SEO anytime soon. Why? Because AI is more of a tool than a human complement. SEO is extremely complex, and AI only automates a few tasks.

So, the answer to the question "Will AI Replace SEO?" is a resounding no. AI has made significant improvements to search engines like Google, helping them better understand users' search queries and delivering the best content. Today, content marketers and managers are using AI, such as ChatGPT, for simple SEO tasks like generating content briefs and outlines, proofreading, optimizing keyword placement, and writing meta-information.

Some companies have integrated AI solutions into their platforms to improve user experience, as user experience is one of the many SEO ranking factors. Therefore, in my observation, as content creators, we shouldn't worry about being replaced. Instead, we should embrace AI and start integrating it into our tasks.

I am the founder of Scribble Bridge, a content writing agency in London.

END OF ARTICLE # #

Safeguarding Your Finances: A Guide to Protecting Yourself From Fraud

BrandPoint

In today's digital age, the growing portion of our lives taking place online has led to an increased risk of fraud. Cybercriminals are getting smarter and constantly finding new ways to exploit vulnerabilities. In fact, 2023 was the worst year ever for scams, causing people to lose $10 billion according to the FTC.

Yet, that doesn't mean you need to panic! New technologies are helping protect individuals from scams before they even happen. And by taking a few simple steps, you can ensure your transactions and personal information are kept secure.

Here are some best practices you can adopt to safeguard yourself from fraud:

Keep Your Devices Updated:

One of the fundamental steps in fortifying your defense against fraud is to ensure that your devices, including smartphones, tablets and computers, are running on the latest operating system and software updates. Developers regularly release security patches and updates to address vulnerabilities, and by keeping your devices up to date, you minimize the risk of falling victim to known security loopholes.

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, 9/24

Jan Rothfuss 347-6020
Membership & Help's Half Hour
jan_rothfuss@hotmail.com, 9/26

Tony Dellelo 734-6149
Programs & Monitor editor
tonydel@techie.com, 9/25

Got Questions?:

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

Planning Meeting

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

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

Avoid Public Wi-Fi for Online Shopping:

Public Wi-Fi networks, while convenient, are hotspots for potential security breaches. Cybercriminals can easily intercept data transmitted over unsecured networks, putting your sensitive information at risk. It's advisable to avoid making online purchases or accessing your financial accounts when connected to public Wi-Fi. Instead, use a secure and private connection, such as a personal hotspot or a trusted home network, to conduct sensitive transactions.

Use Your Smartphone's Digital Wallet:

Your smartphone's digital wallet isn't just super convenient, but it's also a more secure way to pay. By setting a unique passcode (that isn't your address, birthday or phone number) and biometrics (such as facial recognition or fingerprint), your digital wallet will be even more secure than your physical one! Also, be on the lookout for enhancements to wallets that will provide even more features to keep you secure, including by letting users verify identities and manage their data all in one place.

Shop at Reputable Vendors:

When shopping online, it's crucial to stick to reputable vendors and well-known e-commerce platforms. Be wary of unfamiliar websites that may lack the necessary security measures to protect your personal and financial information. Look for websites with secure payment options, indicated by "https://" in the URL, and familiarize yourself with the vendor's reputation by reading reviews from other customers.

Use Multi-Factor Authentication:

Enhance the security of your online accounts by enabling multi-factor authentication (MFA) whenever possible. MFA adds an extra layer of protection by requiring users to verify their identity through a secondary method, such as a one-time code sent to their mobile device or email. This additional step makes it significantly more difficult for unauthorized individuals to gain access to your accounts, even if they have your login credentials.

Zero-Liability Has Your Back:

Financial institutions that issue Mastercard cards won't hold consumers responsible for "unauthorized transactions," provided they are promptly reported and the cardholder used reasonable care in protecting the card from loss or theft. As a Mastercard cardholder, Zero Liability applies to your purchases made in the store, over the telephone, online, or via a mobile device and ATM transactions. With protections like that, paying with your card brings more peace of mind than paying with cash or check.

Mastercard has an entire suite of solutions dedicated to fighting fraud and helping approve genuine transactions. That includes identity solutions that validate you are a genuine person; ID Theft Protection, which provides proactive monitoring and resolution of identity theft threats for U.S. Mastercard cardholders; SafetyNet, which leverages AI and machine learning to detect and address fraud more accurately and more quickly than ever before, and more.

Tidbits of probably useless information

Yes, the rumors are true – **apples** do contain deadly cyanide, or at least the compound to lead to its production. However, don't get too worried about your favorite fruity snack. Apple seeds contain amygdalin, which can turn into cyanide when digested. **Throw the seeds away!** The seeds of other fruits, including apricots and pears, also contain the same chemical. People can eat these fruits safely by avoiding the seeds, pits, or kernels.

The largest population of **camels** in the wild, estimated at more than 1 million individuals as of 2023, is found in neither Arabia nor Mongolia, the traditional homelands of genuinely wild camels, but instead in the Australian desert.

Believe it or not, if you have a wound, pour some **sugar** on it. Better yet, after bleeding has been controlled, use sugardyne (3 parts powdered sugar to 1 part cooking oil).

Though **blood vessels** are relatively small, the network is amazingly long. In fact, if they were laid out in a line, they would measure more than 60,000 miles in length, the U.S. National Institute on Aging (https://www.nia.nih.gov/) (NIA) calculates. Considering that the circumference of the Earth is 24,873.6 miles, according to NASA, that means your blood vessels could circle the globe more than twice.

Protecting yourself from fraud requires a combination of awareness, vigilance and proactive measures. By keeping your devices updated, avoiding public Wi-Fi for financial transactions, choosing reputable vendors, using multi-factor authentication and paying securely with your card, you can significantly reduce the risk of falling victim to fraudulent activities. Stay informed, stay cautious and take the necessary steps to fortify your digital defenses in the ever-evolving landscape of online security. Learn more about all the ways Mastercard protects cardholders at https://www.mastercard.us/en-us/personal/get-support/safety-security.html .

END OF ARTICLE # #

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

Craigslist, Scammers and Schmeckpepers

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

Craigslist is a free online classified ads site that's been around almost 30 years. It's a popular way to buy, sell, and trade goods or services locally. It's also used as a dating service, a job-hunting and recruiting tool, and much more. Lots of people use it every day for legitimate transactions, but if you're not careful, you could end up getting scammed by a Schmeckpeper. What's a Schmeckpeper? Read on for the answer, and learn about some Craigslist traps to avoid...scam, bogus money order, Western Union scam, overpayment scam.

Be Aware of Common Craigslist Scams

Craigslist itself warns users that they're entirely on their own when it comes to vetting their trading partners. Craigslist makes no attempt to screen advertisers. Instead, it relies on "flagging" of unsavory listings by the user community. If a listing receives too many flags from other users, it is taken down automatically. But this self-policing does not catch all scams. And of course it can't catch the creeps and crooks who respond to the legitimate ads.

The number one thing you can do to protect yourself is "deal locally with people you can meet in person." That advice comes from the Craigslist FAQ about scams. If you send money or goods to someone far away, there is very little you can do if you get nothing in return. By dealing face to face, you will avoid 99% of scam attempts.

Unlike eBay, Craigslist offers no verification of sellers' and buyers' identities; no "buyer protection" in case the goods are not delivered; no escrow service; and no guarantees of any transaction. It's 100% buyer beware. Craigslist advertisers who ask you to send money in advance via Western Union or bank wire transfer should be avoided, and flagged. There is no way to get your money back when you pay via these methods, and in most cases you will not get anything in return.

Windows & Android Tips

by Judy Taylour

YOUR ANDROID DEVICE IS TOO OLD TO RECEIVE UPDATES, NOW WHAT?

If you own a relatively new or high-end Android smartphone, it'll most likely get at least four years of software updates and support. Older devices, however, may already be at the end of their lifecycles. So, what happens once your Android is too old to receive updates? Read more at Your Android Device Is Too Old to Receive Updates, Now What? (howtogeek.com)

EXCEL OPENING BLANK DOCUMENTS? TRY THESE TIPS TO FIX THE PROBLEM – Microsoft Excel opening blank documents for you? Problems like a corrupted Excel workbook, a hidden sheet, interference from add-ins, and other factors can lead to this issue. Try these How-To Geek fixes to identify the leading cause and resolve the problem. **Excel Opening Blank Documents? Try These Tips to Fix the Problem (howtogeek.com).**

DO YOU NEED TO WIPE YOUR PRINTER BEFORE YOU GET RID OF IT? – We all know it's important to remove personal data before selling or discarding a PC or smartphone. But what about your printer after it spits out its last page? Here's how to securely dispose of it. Read this PCMag article to find out how. Do You Need to Wipe Your Printer Before You Get Rid of It? | PCMag

If you're selling on Craigslist, it may seem safe to accept cashier's checks or money orders through the mail. But counterfeit cashier's checks and money orders can come back to bite you weeks after your bank told you the funds had cleared. Sometimes it can cost you a lot more than the face amount of the check.

My Personal Craiglist Scam Story

I posted several items for sale on Craigslist. And within minutes, I started getting emails from people with strange sounding names, asking if the item was still available. One person's name was (I kid you not) "Schmeckpeper Ayuso". I responded to that person, and got this in reply:

"i would have love to come and see it, but my scheduled is very tight. I will mail out yor payment once you provide your full name, phone number and addresse. I can only pay via money order as am on a business trip now, pls let me know where to send your payment to because i wouldn't want to lose it to some else. I don't mind adding ($50) dollars so you can keep it in my favor. i will appreciate if you can get the ad off craigslist so i can be sure you are keeping it in my favor. Please let me know as soon as you receive it so i can start making arrangement for the pick-up."

Turns out the wording of this reply is almost identical to other messages commonly sent by overseas scammers. Here's how the scam often plays out:

One Craigslist seller received a check for $2,500 from a foreign buyer, instead of the $250 they had agreed upon. The buyer said there had been a "terrible mistake" made by her bookkeeper, and asked the seller to wire back the excess funds. She even told the seller to keep an extra $100 for the trouble. The check, of course, was counterfeit, and the seller would have been scammed out of $2150 if they had wired funds to the crook. I'm sure I would have been Schmeckpepered if I had gone ahead with that sketchy deal.

Beware of any seller who requests personal financial information such as a bank account number, credit card number, or Paypal email address. Identity theft is often one of the objects of Craigslist scams.

Likewise, if you are applying for a job listed on Craigslist, **do not cooperate in any background or credit check** until you have had a face-to-face interview and verified that the employer is legitimate. The information you provide to enable a background check may be used to steal your identity.

Housing rentals are another favorite Craigslist scam. It's amazing how many people hand over hundreds or thousands of dollars in deposits and rent without ever seeing the inside of a rental property. A lot of people have rented homes from scammers who didn't even have the right to rent the properties! They show up and

Scams

By AARP

Multistage grandparent scam -

This is a new, more sophisticated version of the old grandparent scam, in which crooks call and pretend to be a grandchild who's been arrested and needs bail money to get out of a nonexistent legal jam. In the past, grandparent scammers were often small-timers who would plead for a few hundred dollars. But these days, Foss says, they often set up call centers staffed with young people who are paid a few bucks for every grandparent that they can connect with. After posing as grandchildren who've been jailed after a car accident, they'll provide a case number and instruct the target to call their defense attorney or the local prosecutor. "When Grandpa calls up, they say, 'Oh, do you have the case number?'" Foss explains. It's actually a subtle psychological trick to see whether the grandparent is compliant and will follow their instructions to send thousands or even tens of thousands of dollars.

Some scammers have a third conspirator pose as a courier and go to a grandparent's home to pick up the money in person, according to Steve Baker, a former Federal Trade Commission official who now publishes the Baker Fraud Report newsletter.

find the home or apartment is already occupied, and the scammer is long gone.

A friend of mine warned about a Craiglist scam where **the "buyer" emails the seller a link** to view a web page or watch a video "to make sure it's the item I want to buy." Don't click... or you'll wind up a victim of some nasty virus that will wreak havoc on your computer.

If a buyer offers to pay MORE than the asking price, run away fast. But likewise, **if a seller is offering a price that's way too LOW, that's another big red flag.** I've seen scams on Craisglist, Facebook Marketplace, and Nextdoor in which a car is offered for sale at a price that's just ridiculously low. The seller may claim they're being deployed for military service, or the car belonged to their ex-husband and they just want to get rid of it. THey'll make up some reason why you can't see the car in person, and try to persuade you to send a money order. But these cars do not exist.

Be wary also of concert or event tickets sold on Craigslist. It's too easy for scammers to offer fake tickets that look like the real thing. Instead go to Ticketmaster or StubHub where the tickets are validated and guaranteed to be legitimate.

Employment and Freelance Job Scams: Job offers promising unrealistic salaries may tempt job seekers, but in this scam, the applicants are told they need to pay for training or background checks. These jobs don't actually exist. On the flipside, some scammers will post ads for freelance workers. After the job is completed, they refuse to pay, claiming that the work was incomplete or unsatisfactory.

Poor spelling, confused grammar, odd-sounding names, and long rambling replies are a hallmark of Craigslist scammers. Beware of anyone who wants to pay with a money order or a check, even a certified check, as they can be easily forged. And if you're buying or selling something that costs a significant amount of money, always have a friend with you when meeting the other party, and do it in a public place where video cameras are present. Some police stations encourage people to use their facilities for this purpose. See SafeTrade Stations to find a safe trading location near you. There are hundreds of SafeTrade locations listed there, including one at North Pole, Alaska! A scammer is much less likely to participate in a fraudulent deal if they know they're being watched.

Finally, be aware that some scammers go so far as to send **fake emails or voicemails purporting to be from Craigslist.** The message may say that Craigslist has approved the transaction as safe, and mention a buyer's protection service. If you see something like this, it's a big red flag that a scam is in the works.

Many of these same scams can play out on Facebook Marketplace, or sell-your-stuff sites such as Letgo, OfferUp or Poshmark. The bottom line is "buyer (and seller) beware" if you don't want to get Schmeckpepered.

END OF ARTICLE # #

Virtual Tours

ITER, initially known as the International Thermonuclear Experimental Reactor (*iter* meaning "the way" or "the path" in Latin).

We offer virtual visits for groups and for individuals, both in English and in French.

Virtual visits will last about **90 minutes**. They include a presentation on the ITER project, a video and an immersive virtual tour of the ITER work site.

Virtual visits are **free of charge** and there is **no age restriction.**

The ITER Organization requires a certain number of personal information of its visitors, in order to ensure the appropriate level of safety and security. For more information, see our data privacy and data protection page.

Please contact us at visit@iter.org.

Curious about ***Wind for Industry***? Take a tour of a Wind for Industry project. Walk through the North Findlay Wind Campus, where the One Energy headquarters sits directly beneath the eight wind turbines helping to power factories owned by Whirlpool Corporation and Ball Corporation in Findlay, Ohio.

There's nothing quite like taking a walk under these massive structures, climbing to the top of a turbine, and seeing the view for yourself. Watch this 34-minute video for the same tour we would give you on-site. Plus, climb a wind turbine with us! https://youtu.be/odY_vyb27UQ

Windows 11 Will Soon Be Encrypted by Default

By Arol Wright, May 9, 2024

There are some (tricky) workarounds. Over the past few years, device encryption has transitioned from being something optional in most cases to being mandatory. With hardware advances, encryption no longer has the same performance penalty it once had. It has also become required in devices such as smartphones—Android phones made encryption a must years ago. Now, Microsoft will be mandating encryption in Windows 11, although you do have workarounds if your device is too old for this.

Microsoft is making significant changes to its device encryption policies in Windows 11. The upcoming 24H2 update will enable device encryption by default on both Pro and Home editions for new installations and system resets. This change has already been observed in preview builds. Microsoft also confirmed the policy shift, stating it aims to increase the adoption of device encryption. The feature utilizes BitLocker technology to encrypt system drives, safeguarding data. One thing you must take into account if you're going to accept this change is that you must back up your BitLocker recovery key—losing access to this key could mean losing access to your entire PC.

The good part is that you shouldn't suddenly have your PC encrypted with a future update as a result of this change. From what we understand, this is a change that applies only to new installs, not existing ones. Even then, there are concerns about how users might handle the recovery key or lose access to their Microsoft account, as both things could prove fatal if you happen to have an encrypted PC.

While Windows 11's hardware requirements generally ensure compatibility with BitLocker, users who wish to disable automatic device encryption have a few options. For one, a registry modification during installation can prevent device encryption. Tools like Rufus can also create Windows 11 installation media that bypasses system requirements and disables BitLocker. However, we don't really recommend doing this unless your PC is really too old to handle encryption without a significant performance penalty. Keeping your PC encrypted can be vital to keep your PC and the contents of your hard drive safe from prying, unauthorized eyes. Make sure to keep that key safe, though.

Reprinted from https://www.howtogeek.com/microsoft-encryption-by-default-windows-11/.

Scammers Are Bombing Apple Devices With Two-Factor Password Resets: Here's How to Avoid It

By Simon Batt , Mar 29, 2024

Do you get waves of two-factor authentication requests? Don't panic or give in; it's exactly what the scammer wants.Key Takeaways

- 2FA bombing attacks target iOS devices to gain access to accounts through constant 2FA requests and phone calls.

Penguin Platform

By *"Free John" Kennedy*

The Linux operating system has a lot of fans for good reason. The open-source operating system is free, offers a lot of customization, and is very stable. It also has a reputation for being safe from malware attacks.

While it's true that it's free, flexible, and stable; **Linux is not immune to malware attacks**. Security experts say attacks against Linux systems have increased by 60% in recent years.

Malware can infect Linux systems through various means, including email attachments, software downloads, and malicious websites.

Here are a few tips to help protect your Linux system:

1. Update your software regularly: Make sure to install the latest updates and security patches for your Linux distribution.
2. Use a firewall: A firewall can help block unauthorized access to your system.
3. Install antivirus software: Although Linux is less susceptible to viruses than other operating systems, installing antivirus software is still a good idea.
4. Be careful when downloading software: Only download software from trusted sources.

By taking the necessary precautions and implementing security measures, you can protect your Linux system from malware and enjoy a safe and secure computing experience.

Linux OS vulnerable to attacks (cynmackley.com)

- Scammers pretend to be Apple Support after bombarding victims with 2FA notifications to obtain 2FA codes.
- To avoid falling victim, decline suspicious 2FA requests, don't give codes over the phone, and verify with Apple if in doubt.

If you or someone you know owns an iOS device, watch for en-masse password reset spam. If it happens, you're on the receiving end of a two-factor authentication (2FA) bombing attack.

While the attack may seem scary, you're completely in control of the situation. As long as you know how 2FA bombing works, the scammer can't access your account.

What Is 2FA Bombing?

2FA bombing (also known as "MFA bombing" or "MFA fatigue") is when an attacker gets a hold of somebody's account information and tries to log in with it. If the account has two-factor authentication protection and doesn't use a separate authenticator app or device, it will send a text, email, or phone notification to the account holder, asking if they want to log in.

Usually, this is the end of the story. However, with 2FA bombing, the attacker bombards the user with 2FA requests in hopes that they will either accidentally allow it or accept it to stop the messages from coming in.

How does the iOS 2FA Bombing Attack Work?

2FA bombing can be effective, but it's very easy to defend against. You just need to reject the requests or change their 2FA confirmation method, and the scammer won't get in. However, a new strain of 2FA bombing that affects iOS users has appeared.

The attack starts as normal. The scammer sends a wave of iOS 2FA notifications asking you to let them in. After a few minutes, the scammer stops sending 2FA notifications and calls your phone.

When you pick up, the scammer pretends to be from Apple support. They'll claim the wave of notifications was due to a hacker trying to gain access to their account. They will then ask you for some information under the guise of protecting them.

What's worrying is that the scammer will already have a lot of information about you. This is because some services collect data on people, including tying personal information to phone numbers. This means the caller will know sensitive data like your name, date of birth, and address.

The scammer aims to get a hold of your 2FA code, which you receive via text. Once you hand over the code, the hacker will access your account.

How to Avoid an iOS 2FA Bombing Attack

As scary as this attack may sound, you have complete control over the situation. If you notice your iPhone blowing up with 2FA requests, don't panic; that's exactly what a scammer wants you to do. Remember, they cannot access your account if you do not accept the request.

Decline all 2FA requests you receive that you did not ask for. If someone calls you asking for a code, do not give it to them. If you're concerned that the call is real, see if you can spot telltale signs that the person calling you is a scammer. You can also hang up and call

* * Jokes & Quotes Stolen from Everywhere * *

Dumb Jokes:

My dream job would be to clean mirrors. I could really see myself doing that.

A man walks into lawyer's office and asks, "How much for a consultation?" "Three questions for $150 bucks." "Kinda steep, isn't it?" "Yeah, now what's your last question."

Why did the scarecrow get an award? He was outstanding in his field.

What do Alexander the Great and Winnie the Pooh have in common? Same middle name.

Did you hear about those new corduroy pillows? They're making headlines!

Why do cows have hooves? Because they lactose.

What did the baby corn say to mama corn? "Where's popcorn?"

I just burnt my Hawaiian pizza. I guess I should have put it on aloha temperature.

What happened to the exorcist's car? It got repossessed.

What's the leading cause of dry skin? Towels.

My wife found out I was cheating on her after she found all the letters I was hiding...she got mad and said she's never playing Scrabble with me again.

I caught my son chewing on electrical cords, so I had to ground him. He's doing better currently and now conducting himself properly.

Apple support yourself to double-check if something really is wrong with your account.

Unfortunately, changing your password will not work because the scammer can send you 2FA notifications by just entering your phone number. As such, you can either change the number on your account or ride it out until Apple comes up with a solution. You can also stop scam calls on your iPhone to prevent the scammer from phoning you.

2FA bombing attacks can be scary and mentally draining, but that's exactly what the scammer wants. As long as you decline the notifications and ignore any calls from Apple, you won't risk losing your account.

From the web, https://www.makeuseof.com/scammers-bombing-apple-devices-two-factor-password-resets/.

* * * * * 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.

Mercedes Becomes First Automaker to Sell Level 3 Self-Driving Direct to US Consumers

By Adrianna Nine April 22, 2024

Drivers who enable Drive Pilot in their 2024 EQS and S-Class sedans no longer have to keep an eye on the road.

Level 3 and Level 4 autonomous driving—what most of us imagine when we think of "self-driving"—has historically been reserved for "robo-taxis" like Waymo. But after becoming the first automaker in the United States to secure Level 3 autonomous driving permits last year, Mercedes-Benz is selling the technology directly to American consumers. EQS and S-Class sedan drivers can enable "Drive Pilot" through an annual subscription that allows them to divert their attention from the road.

Mercedes began obtaining government approval for Drive Pilot last year. Because Nevada law allows all levels of autonomous driving on public streets, Mercedes simply "self-approved" its software in January 2023, then submitted documentation for California approval a few months later. In June, California's Department of Motor Vehicles (DMV) issued Mercedes a Level 3 self-driving permit that allowed the German automaker to begin selling Drive Pilot in the state.

Level 3 and Level 4 autonomous driving—what most of us imagine when we think of "self-driving"—has historically been reserved for "robo-taxis" like Waymo.

Read more at https://www.extremetech.com/cars/mercedes-becomes-first-automaker-to-sell-level-3-self-driving-direct-to.

Odds and Ends

Watch Out! Hackers Now use Google Calendar to Steal Your Data

Natalia Kudryavtseva, 02/27/2024

Hackers have uncovered a novel method to exploit Google Calendar for their malicious activities, posing a significant cybersecurity threat to numerous Internet users.

Traditionally, cybercriminals have relied on a command and control (C2) infrastructure to execute malicious commands on infected endpoints. This infrastructure often involves compromised servers, but it has a major flaw: cybersecurity professionals are typically quick to detect these connections and halt them.

However, hackers are now leveraging legitimate resources, such as **Google Calendar**, as **C2** infrastructure. This approach significantly complicates the task of security experts who must identify and effectively counter these attacks. Google has already issued a warning to the entire security community about a proof-of-concept exploit known as "Google Calendar RAT" (GCR), circulating on the dark web.

Google has taken measures to disable Gmail accounts controlled by the attackers and used by the malware.

https://ccm.net/apps-sites/11825-watch-out-google-calendar-is-the-new-target-for-hackers-delivering-you-malware/.

NASA's Proposed Plasma Rocket Would Get Us to Mars in 2 Months

By Passant Rabie

The space agency is investing in the development of a propulsion system that uses nuclear power to create plasma bursts.

PublishedWednesday 1:35PM

The future of space travel depends on our ability to reach celestial pit stops faster and more efficiently. As such, NASA is working with a technology development company on a new propulsion system that could drop off humans on Mars in a relatively speedy two months' time rather than the current nine month journey required to reach the Red Planet.

NASA's Innovative Advanced Concepts (NIAC) program recently selected six promising projects for additional funding and development, allowing them to graduate to the second stage of development. The new "science fiction-like concepts," as described by John Nelson, NIAC program executive at NASA, include a lunar railway system and fluid-based telescopes, as well as a pulsed plasma rocket.

The potentially groundbreaking propulsion system is being developed by Arizona-based Howe Industries. To reach high velocities within a shorter period of time, the pulsed plasma rocket would use nuclear fission—the release of energy from atoms splitting apart—to generate packets of plasma for thrust.

The new propulsion system has the potential to revolutionize crewed spaceflight, helping humans make it to Mars without the toil of the trip itself.

Continue this article on https://gizmodo.com/nasa-pulsed-plasma-rocket-advanced-concept-mars-1851463831.

Unlocking the True Power of Clean Geothermal Energy

MIT spinout Quaise Energy, is working to create geothermal wells made from the deepest holes in the world. There's an abandoned coal power plant in upstate New York that most people regard as a useless relic. Paul Woskov, a research engineer in MIT's Plasma Science and Fusion Center (PSFC), notes that the plant's power turbine is still intact and the transmission lines still run to the grid. He's hoping it will be back online, completely carbon-free, within the decade. In fact, Quaise Energy, the company commercializing Woskov's work, *believes if it can retrofit one power plant*, the same process will work on virtually every coal power plant in the world. Quaise's founders have set an ambitious timeline to begin harvesting energy from a pilot well by 2026.

Quaise is hoping to accomplish those lofty goals by tapping into the energy source below our feet. The company plans to vaporize enough rock to create the world's deepest holes and harvest geothermal energy at a scale that could satisfy human energy consumption for millions of years. Quaise's drilling systems center around a

microwave-emitting device called a gyrotron that has been used in research and manufacturing for decades.

Our work is a necessity, not an option.

Deep geothermal energy is at the core of an energy-independent world. Our mission is to bring this inexhaustible, renewable, clean energy source to future generations. This is the profound power of deep geothermal. We are unlocking energy for all. Our approach uses the established workforce, assets, supply chains, and regulatory frameworks of the fossil fuel industry. We don't need to create infrastructure from scratch. Geothermal has the power density and scalability of fossil fuels, allowing us to put clean energy on the grid very quickly.

Checkout the future at https://www.quaise.energy/.

CLUB and REGIONAL NEWS

*** * July and August, summer hiatus – No Meetings * ***

Humans are the Nuts and Bolts of RIT Robotics Research

Story by Michelle Cometa

At RIT, robots are learning to read the room—especially rooms with humans.

Robots work with individuals everywhere, from storerooms to operating rooms. These robots can see pupils dilate, detect sweat on a brow through biosensors, and perceive heart rates going up. Using this bio-information to adapt to humans—rather than the other way around—robots are becoming sophisticated enough to predict behaviors and act on them.

Improved communication between robots and people is part of the human-centered philosophy that anchors much of RIT's work in robotics.

"Industry wants robot systems that work collaboratively with humans, that are safer and have more flexibility in how they interact together to solve problems no matter what field," said Ferat Sahin, department head of RIT's electrical and microelectronic engineering programs. "We are teaching robots to understand human qualities. Our students use this information to build solutions for people and the work they are doing."

To develop the best human-robot partnerships, RIT researchers are refining how robots measure and detect signals from humans.

For his Ph.D. project, Subramanian is adding facial recognition information into the AI system for a UR-10 collaborative robot. He has developed a way to determine human emotion from facial images of people working with robots.

Read more of this ground breaking technology at https://www.rit.edu/news/human-robotics-research.

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

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**