




Significant Bits

Journal of Brisbug PC User Group Inc.



Vol 39 No 09

17 November 2024

Page	Article	Author	Position	Club
3	From the President's CPU	Keith Catts	President	
5-9	Johns Jots	John Tacey	Q&A	
10-19	APCUG Articles	As Noted	Various	APCUG
			Secretary	

Meeting Timetable

Mitchelton Library Helios Parade Mitchelton

9:30am	Q&A	John Tacey
11pm	Exploring win 11 to Linux	Fred
	Lunch -- GM - Report to the Club	Keith
1:00pm	Linux Ubuntu Mate Workshop	Keith All

If you have a question that may need a bit of a look up, let me know before the meeting

Presentation can be done using Power Point and shared screens.



Significant Bits

Journal of Brisbug PC User Group Inc.

SIGNIFICANT BITS

the Journal of
BRISBUG PC USER GROUP INC.
*A Computer Club for users of
PC-type computers*
Telephone No. 07 3353 3121

Web Address:
<https://www.brisbug.asn.au>

President

Keith Catts 07 3353 3121
E-mail: president@brisbug.asn.au

Treasurer

Ross Skyring 07 3261 4781
E-mail: treasurer@brisbug.asn.au

Secretary

Gary Woodforth 07 3399 7939
E-mail: secretary@brisbug.asn.au

Webmaster

Keith Catts 07 3353 3121
E-mail: president@brisbug.asn.au

Newsletter Editor

Christine Haydock 07 3350 1573
or 0412 678 598
E-mail chaydock@powerup.com.au

CLUB NOTICES

CLUB INFORMATION LINES

Info Line (07) 3353 3121

The Members' Web Page

Meeting Days

17 November 2024

22 December 2024

19 January 2025

16 February 2025

16 March 2025

20 April 2025

18 May 2025

15 June 2025

20 July 2025

17 August 2025

21 September 2025

19 October 2025

16 November 2025

21 December 2025

Magazine

Editor
Chris Haydock

Proof-reader
John Tacey

Submission Deadline

Friday 8 November 2024

Please use e-mail if possible

COPYRIGHT

Material in this magazine may usually be copied by PC User Groups without fee. This is provided that the copyright rests with the Brisbug PC User Group Inc., so please first check with us to avoid possible infringement. This permission is also on condition that the copy is not used for commercial advantage and that the origin of the material and this permission to copy are acknowledged in the reprinted item.

LIABILITY

Although it is policy to check all published material for accuracy and usefulness as far as possible, no warranty is offered against any loss resulting from the use of any material in this magazine. All content reflects the opinions and experience of the author and does not necessarily reflect the policy of the Brisbug PC User Group Inc. Most hardware, software and products mentioned are registered names and trademarks of the vendors or makers concerned. Brisbug will not be held responsible for claims made by advertisers, and advertisers are not to be bound by errors and omissions in publication.

Hi All,

I have been trying out another way of getting Win 11 on old hardware. It follows a standard install but has some download and language matching of the existing win install. Then a setting up a folder from which to install and doing that by some command line stuff. It has worked on a couple of computers and it is update to 24H2. As with material from Fred's presentations the life of such a process is not known and subject to being crippled by some future update. At the best they may last out to the next full feature update.

Linux is of course an alternate option for many of us and depends on just how wedded we are to Windows and Office apps, along with the many programmes loaded on the platform. As Fred has pointed out much of what we do can be done using a Linux operating system. Much of our use is the apps that let us do our thing.

It will be cleared as we progress with the linux workshop and get some familiarity and comfort.

To really move would be to have a Linux computer in use. How to do it.

One those with access to a second box we can load it with Linux. I think for those that want to try it out, I propose the set the next meeting for loading Linux on to your computers so bring them in if you have an old laptop all the good, or if you can bring in say the Toshiba's you received from the club or your desktop if you can do that.

This will get past the loading Linux up stage and then you can learn at the club and work with it at home.

All for now

See you at the meeting

Keith

**PLEASE · PAY · YOUR ·
MEMBERSHIP · RENEWAL · VIA ·
DIRECT · FUNDS · TRANSFER**

**Brisbug · PC · User · Group ·
Inc**

BSB · No: · · 034 - 083

Account · No: · 185711

**Remember · to · enter · your · name ·
and · membership · number · in · the ·
comment · field**

Reports

Presentation and Education

Presentation:

Morning 11am. Win to Linux with Fred.

After Afternoon 1pm: Linux Ubuntu Mate workshop

Membership Report - Gary Woodforth

We had 10 members at the September meeting. With 1 visitor, who has joined us. Say hello to Tim Lummis and make him welcome.

Treasurer's Report

October 2024

Opening Balance at 01/10/24 2155.51

Income

Bank Interest 0.01

New Member Tim Lummis 30.00

Total Income 30.01

Expenses

Office of Fair Trading 62.10

Total Expenses 62.10

Month's loss 32.09

Balance at 31/10/24 2123.42

Ross Skyring

Treasurer



John's Jots

Q&A - October

Privacy and Security

For the Operating System and Application Programs check the Options or Settings for a section covering Privacy and Security.

Work your way through the list turning On or Off the various entries as appropriate.

Firefox 131.0.3

Application Menu

General

Home

Search

Privacy & Security

Thunderbird 128.3.1

Thunderbird Menu General

Composition

Privacy & Security

Microsoft Edge

Ellipsis (...)

Privacy, search & searches

Backup Slows Down

Browser Cache from WordWeb Dictionary:-

2. (Computing) RAM memory that is set aside as a specialized buffer storage that is continually updated; used to optimize data transfers between system elements with different characteristics.

Web Browsers store a historical list of sites, including their URLs, of all the pages visited. This facilitates returning to a previous site.

Each entry is equivalent to a Bookmark or Favorite

e.g. Name: calibre - E-book management Location: <https://calibre-ebook.com/>

Browser Cache

Limit size or empty cache on closure

Depending on the particular browser, it may be possible to have the History/Cache cleared on closure or limit the size of the Cache.

Outlook.com Account Won't Send

Thunderbird, existing account added with OAuth2 authorisation.

Works fine with incoming mail. Will not send mail.

Error messages:-

Sending of message failed:

An error occurred while sending mail: Outgoing server (SMTP) error.

The server responded: Cannot connect to SMTP server 3.33.257.168 (3.33.257.168 : 587). connect error 10060.

The message could not be sent because connection to outgoing server (SMTP) failed. The server may not be available or refusing SMTP connections. Please verify that your outgoing server settings are correct and try again.

Note: This record of the Q&A session topics relies on my biological volatile memory (a.k.a. the 'forgettery').

Gleanings from e-newsletters and other sources.

Reviews

Proton VPN

By Chris Stobing Oct 24, 2024

The best VPN gets even better

Bottom Line

Proton VPN rises above the competition with an excellent collection of features, a high-performance server network, and a nearly peerless free subscription option, making it the top service we recommend.

<https://au.pcmag.com/vpn/57676/protonvpn>

The Best Android Antivirus for 2024

By Neil J. Rubenking Oct 23, 2024

More phones run Android than any other mobile OS, and there's a correspondingly large variety of malware. Our testing shows these are the best Android antivirus apps for keeping your devices safe.

<https://au.pcmag.com/antivirus/51688/the-best-android-antivirus-apps>

The Best Authenticator Apps for 2024

By Kim Key Oct 22, 2024

Stay protected with the best multi-factor authentication apps we've tested.

<https://au.pcmag.com/security/106845/the-best-authenticator-apps-for-2024>

The Best Password Managers for 2024

By Kim Key Aug 07, 2024

Stop using the same password everywhere. The top password managers we've tested create a unique and strong password for each of your online accounts and alert you to potential data leaks.

<https://au.pcmag.com/password-managers/4524/the-best-password-managers>

Qualcomm's 8-Core Snapdragon X Plus, Tested: A Competitive, Cheaper Chip

By Rob Pegoraro Oct 28, 2024

The eight-core Snapdragon X Plus laptop processor is Qualcomm's latest bid to lower the starting price of mobile CoPilot+ PC Windows systems with its new chips.

<https://au.pcmag.com/processors/107987/qualcomm-s-8-core-snapdragon-x-plus-tested-a-competitive-cheaper-chip>

Snap Spectacles '24 First Look: AR Glasses That Aren't Vaporware

By Rob Pegoraro Oct 26, 2024

You do, however, have to join a developer program to try out a pair.

<https://au.pcmag.com/wearables/107968/snap-spectacles-24-first-look-ar-glasses-that-arent-vaporware>

The Best Malware Removal and Protection Software for 2024

By Neil J. Rubenking Jun 03, 2024

We've tested more than 100 anti-malware apps to help you find the top malware protection and removal software for all your devices.

<https://au.pcmag.com/antivirus/48370/the-best-malware-removal-and-protection-software>

The Best PC Brands for Tech Support

By Eric Griffith Oct 25, 2024

Not everyone is comfortable troubleshooting or fixing the devices they own. If tech support and repair options are a consideration in your technology purchases, these are the brands our readers recommend.

<https://au.pcmag.com/news/107945/the-best-pc-brands-for-tech-support>

Ultraloq Bolt Fingerprint

By John R. Delaney Oct 22, 2024

The best smart lock gains HomeKit compatibility

Bottom Line

The Ultraloq Bolt Fingerprint is one of the most versatile smart locks we've tested, offering numerous ways to lock and unlock your door and third-party support across multiple platforms.

<https://au.pcmag.com/smart-locks/107882/ultraloq-bolt-fingerprint>

New Releases

Avast Free Antivirus

License: Freeware

File name: Avast_Free_Antivirus_v24.9.6130 (Web Installer)

File Size: 0.25 MB O/S: Windows

Publisher: Avast Software s.r.o.

URL: <https://www.avast.com/antivirus>

Glary Utilities 6

License: Freeware

Release Date:

File Name: Glary_Utilities_v 6.17.0.21.exe

File Size: 26.48 MB

Platform: Windows 11, 10, 8, 7, 2000, XP, Vista. 32/64bit version.

Publisher: Glarysoft Ltd

Languages: 44 Languages [Help Translate]

URL: <http://www.glaryutilities.com/>

Release Notes:

Optimized Disk Cleaner: added support for 'Corel VideoStudio Pro x9' and 'SketchUp Make 2014'

Optimized Tracks Eraser: added support for 'Corel VideoStudio Pro x9' and 'SketchUp Make 2014'

Optimized Software Update: optimized the version comparison algorithm, and increase the comparison speed by 30%

Optimized Empty Folders Finder: add folder delete validation to prevent accidentally deletion of non-empty folder

Minor GUI improvements

Minor bug fixes

Glary Utilities is a freeware with registry and disk cleaning, privacy protection, performance accelerator and amazing multifunctional tools. It can fix dogged registry errors, wipe off clutters, optimise Internet speed, safeguard confidential files and maintain maximum performance.

It is designed for both novice and professionals. User-friendly interface shows clear & detailed directions. For novice, all work can be done with just 1 or 2 clicks, while for professionals, abundant options are available.

Key features:

Optimise, clean and boost the speed of your Windows.

Protect your privacy and security.

Block spyware, trojans, adware, etc.

Fix certain application errors.

Simple, fast and user friendly interface.

For private use only.

URL: <http://www.glaryutilities.com/>

Google Chrome (32bit) 130.0.6723.70

License: Freeware

File name: ChromeSetup.exe

File Size: 108.24 MB O/S: Windows

Publisher: Google

URL: <https://www.google.com/chrome/>

Java Runtime Environment (32bit)

License: Freeware

File

name:Java_Runtime_Environment_(32bit)_v8.0.4310.10.exe

File Size: 60.78 MB O/S: Windows

Publisher: Oracle

URL: <http://www.java.com/>

Keepass

License: Freeware

File name: Keepass-2.57.1-Setup.exe

File Size: 4.32 MB O/S: Linux, Windows

Publisher: Dominik Reichl

URL: <https://keepass.info/>

LibreOffice

License: Freeware

File name: LibreOffice_24.8.2_Win_x86.msi

File Size: 329 MB O/S: Windows

Publisher: The Document Foundation

Comments: Contains the functions:-

Writer

PDF

Presentation

Spreadsheet

URL:

https://mirror.freedif.org/TDF/libreoffice/stable/6.2.0/win/x86/LibreOffice_6.2.0_Win_x86.msi

Mozilla Firefox

License:Freeware

File name: Mozilla_Firefox_(32bit)_v132.0.exe Update

File Size: 61.69 MB O/S: Windows 7 to 10

Publisher: Mozilla Corporation

Comments:-

To force a manual update:-

Menu Button > ? Button > 'About Firefox'

URL: <https://www.mozilla.org/en-US/firefox/new/>

Mozilla Thunderbird 128.3.3 60.73 MB

License: Freeware

File name: Thunderbird Setup 128.3.3GB).exe

File Size: 60.73 MB O/S: Windows XP SP2 to 10

Publisher: Mozilla Corporation

URL: <http://www.mozilla.org/en-GB/thunderbird/>

Want more? See the New Releases list:

<http://ct.com.com/>

Want more? See the New Releases list:

<http://ct.com.com/>

Tips etc.

How to Download YouTube Videos

By Eric Griffith, David Paiz-Torres Jul 26, 2024

There are dozens of different ways to download YouTube videos so you can view them offline. Here are a few of the easiest and most effective methods

<https://au.pcmag.com/how-to/28663/how-to-download-youtube-videos>

Done With Google Maps? 18 Reasons to Try Apple Maps

By Lance Whitney Sep 11, 2024

The Apple Maps app has matured over the years and is now an effective navigation tool when you need to get somewhere or explore your destination.

<https://au.pcmag.com/iphone-apps/90712/done-with-google-maps-12-reasons-to-try-apple-maps>

How to Uninstall a Windows Update If Your Computer Is Acting Up

By Whitson Gordon, Jason Cohen Oct 23, 2024

If your computer is freaking out after you installed a Windows update, here's how to uninstall the patch and roll back to an earlier version of the operating system.

<https://au.pcmag.com/windows-xp/67708/computer-acting-up-how-to-uninstall-a-windows-10-update>

TSMC Chip Found in Latest Huawei AI Processor, Sparking Action Against Buyer

By Kate Irwin Oct 24, 2024

TSMC is investigating how Huawei has obtained its chips after one was found in the Huawei Ascend 910B.

<https://au.pcmag.com/processors/107943/tsmc-chip-found-in-latest-huawei-ai-processor-sparking-action-against-buyer>

Cellular Starlink Powered 'Hundreds of Thousands' of Texts After Hurricanes

By Michael Kan Oct 24, 2024

In an earnings call, T-Mobile CEO Mike Sievert also dismissed concerns about radio interference from cellular Starlink satellites.

<https://au.pcmag.com/networking/107940/cellular-starlink-powered-hundreds-of-thousands-of-texts-after-hurricanes>

Hacker May Have Breached Hot Topic, Stolen Data on Millions

By Michael Kan Oct 24, 2024

A security firm uncovers evidence that the hacker hit Hot Topic by targeting an employee at a third-party retail analytics platform.

<https://au.pcmag.com/security/107921/hacker-may-have-breached-hot-topic-stolen-data-on-millions>

Cloudflare: Latest Record-Breaking DDoS Attack Hits 4.2Tbps

By Michael Kan Oct 24, 2024

It comes after an 'unprecedented surge in hyper-volumetric DDoS attacks' in recent months.

<https://au.pcmag.com/security/107926/cloudflare-latest-record-breaking-ddos-attack-hits-42tbps>

Claude AI Can Now Control Your PC, Prompting Concern From Security Experts

By Kate Irwin Oct 24, 2024

Security pros suggest hackers could trick Claude's 'computer use' into deploying malware. 'I'm majorly crossing my fingers that Anthropic has massive guardrails,' one expert says.

<https://au.pcmag.com/ai/107925/claude-ai-can-now-control-your-pc-prompting-concern-from-security-experts>

15 NASA, US Defense Contracts Got Sub-Standard Cybersecurity

By Kate Irwin Oct 23, 2024

The US hits Penn State University with a \$1.25 million fine to settle allegations that it failed to adequately secure data tied to government contracts.

<https://au.pcmag.com/security/107915/15-nasa-us-defense-contracts-got-sub-standard-cybersecurity>

How to Delay Windows Updates and Tell Microsoft to Leave You Alone

By Whitson Gordon & Jason Cohen

Updated October 15, 2024

Are you concerned that the latest and greatest updates to Microsoft's Windows 10 or Windows 11 might be a little buggy? Certain versions of the operating system allow you to pause the updates.

<https://au.pcmag.com/how-to/57455/how-to-delay-windows-10-updates>

What's New in the Windows 11 24H2 Update?

By Michael Muchmore Oct 11, 2024

New core code, convenience features, and eye candy, along with exclusive Copilot+ PC bonuses make the latest version of Windows 11 worth a look. Here's everything you get.

<https://au.pcmag.com/operating-systems/107486/whats-new-in-the-windows-11-2024-update>

Opera Rolls Out Big Browser Update: 5 Reasons to Try Opera One R2

By Kate Irwin Oct 23, 2024

Check out split-screen tabs, new themes, continued ad-block support, and more.

<https://au.pcmag.com/browsers/107912/opera-rolls-out-big-browser-update-5-reasons-to-try-opera-one-r2>

New Quantum Computing Chip Deals Could Aid US, Canadian National Security

By Kate Irwin Oct 23, 2024

North America's semiconductor industry gets a boost as Nord Quantique taps an R&D center to produce custom quantum computing chips in Quebec. But the quantum industry is still trying to solve its biggest technical challenge.

<https://au.pcmag.com/processors/107916/new-quantum-computing-chip-deals-could-aid-us-canadian-national-security>

Meta Revives Facial Recognition to Fight Scams and Account Hijacking

By Michael Kan Oct 22, 2024

The goal is to help Facebook and Instagram crack down on so-called 'celeb-bait ads,' but facial-recognition tech will also be available for those looking to recover lost accounts.

<https://au.pcmag.com/security/107896/meta-revives-facial-recognition-to-fight-scams-and-account-hijacking>

8 Ways to Protect Your Smart Home From Hackers

By Stephanie Mlot, Jason Cohen Oct 26, 2024

Smart homes offer convenience and security risks. Here's what you can do to stop hackers from taking control of your smart speaker, thermostat, doorbell, and other connected devices.

<https://au.pcmag.com/smart-home/102123/stay-safe-8-ways-to-protect-your-smart-home-from-hackers>

Intelsat Satellite Mysteriously Breaks Up in Earth's Orbit

By Michael Kan Oct 22, 2024

About 20 pieces of debris from the Intelsat 33e satellite have been spotted in geostationary orbit.

<https://au.pcmag.com/networking/107883/intelsat-satellite-mysteriously-breaks-up-in-earths-orbit>

Police: Thousands of Hackers Used RedLine, Meta Malware to Attack PCs

By Michael Kan Oct 30, 2024

After a Monday crackdown, US and European law enforcement offer more details about the two malware strains, which were used to steal millions of login credentials from PCs.

<https://au.pcmag.com/security/108017/police-thousands-of-hackers-used-redline-meta-malware-to-attack-pcs>

10 Tips for Safer Online Shopping

By Eric Griffith, Kim Key Oct 29, 2024

Follow these tips to keep criminals out of your accounts while shopping online.

<https://au.pcmag.com/security/105529/10-tips-for-safer-online-shopping>

Putin Asked Elon Musk Not to Deploy Starlink in Taiwan

By Kate Irwin Oct 25, 2024

Musk and Russian leader Putin have reportedly been in frequent contact.

<https://au.pcmag.com/networking/107967/putin-asked-elon-musk-not-to-deploy-starlink-in-taiwan>

Wii U Owner Warns: Plug in Your Console to Ward Off Memory Corruption

By Adrianna Nine October 22, 2024

At 12 years old, the Nintendo Wii U is at risk of 'dying' for good, this gaming enthusiast reports.

https://www.extremetech.com/gaming/wii-u-owner-warns-plug-in-your-console-to-ward-off-memory-corruption?utm_source=email&utm_campaign=whatsnewnow&zdee=gAAAAABjNL8ST42l80nl07cPB3qfRUi6ntgUgOTESLESDIZFhs8z4qnmoLs_AknqwLVhZpQWW_ldjicVknAoSBZ5elt2gM0-Tu64aKwciwXzXGx5QU6ZfE%3D&lctg=24359534815

How to Update Your Computer's BIOS/UEFI

By Whitson Gordon Oct 22, 2024

Your computer's Basic Input/Output System or Unified Extensible Firmware Interface shouldn't need to be updated that often, but a hardware bug or compatibility issue may require it.

<https://au.pcmag.com/components/86226/how-to-update-your-computers-bios>

Here Endeth John's Jots

APCUG ARTICLES

These APCUG articles are republished with permission of APCUG. All copyright rests with APCUG and/or the original writer.

Clean Your Dirty Laptop

David Kretchmar, Hardware Technician. Sun City Summerlin Computer Club
<https://www.scscclclub>

After being used regularly for months or years, our laptops accumulate dust, grime, skin oils, sneezes, and who knows what else. Your laptop is most likely due for a cleaning, and I'm going to pass along some suggestions for how to do it effectively without harming this delicate piece of equipment.

You know your laptop is filthy. You can see the dirt and grime on your screen and keyboard. You might also be able to see grime accumulated on your trackpad. So, it's time for a cleaning.

A shining, newly cleaned laptop should be a joy to use; the keys are clean, and the screen is free of smudges and splatters. These cleaning suggestions might also be helpful if you buy a used laptop since the previous owner doesn't always leave it in pristine condition.

Your Supplies

You don't need much to clean a computer: rubbing alcohol, a mild dish detergent, soft lint-free cloths (microfiber cloths are ideal), Q-tips, and canned air. Ninety percent or higher isopropyl alcohol is what you want since it won't damage the internal components. And if you have some particularly embedded dirt, a Mr. Clean Magic Eraser (or other melamine sponge) can also work wonders. However, it should be an absolute last resort since it's abrasive and can leave permanent scratches.

Don't waste your money on specialty cleaners you see at Amazon or big box electronics stores like Best Buy. They work just fine but no better than what you already have at home.

Start With the Inside

Starting with that dirt on the keyboard and screen might be tempting, but you should start with the internals. Canned air will blow dust and dirt everywhere, so if you start cleaning the screen, you'll have to clean it again after you've used

canned air. Start by blowing out the dust, then move on to the outside.

You shouldn't have to open your laptop to clean the inside. Turn off the laptop, unplug the power cable, and remove the battery if it pops out (removable batteries are becoming a thing of the past). Give it a quick burst away from the laptop to eliminate condensation, and then start blowing air into any cracks and crevices: the keyboard, the vents, and even the USB and other ports. Blow in short bursts since longer sprays can cause moisture to accumulate inside your computer. You can also damage the fans by making them spin too fast.

You probably won't see a significant change after doing this. The goal is to prevent dust buildup over time, which can cause your laptop to overheat and possibly spontaneously shut down. If you can see dust bunnies in the vents, you've let it go too long without a cleaning. If you see dust stuck behind the vent that you can't dislodge by blasting it with compressed air, consult your user manual to open the case. Be sure you remember which screws went where for the reassembly. Snap a picture or two of your laptop for reference before opening the case, and be super-organized with the screws as you remove them.

Smokers and pet owners should take special care to clean the inside often since you'll likely experience a much quicker buildup of dust, smoke, hair, and other dirt. Computers exposed to smokers can have their useful life cut by as much as half.

Wipe Down the Outside

Remember, when cleaning a laptop (or desktop) computer, apply the cleaning product to the tool you're using to clean, NEVER directly onto the computer. So, grab your microfiber cloth, pour a little alcohol onto it, wring it out so it isn't dripping wet, and wipe down the surface. Cotton swabs and alcohol are helpful for the keyboard keys and the small spaces between them. (If there are marks that won't come off, you can try rubbing them with a Mr. Clean Magic Eraser or other cleaner very lightly, but again, they're mildly abrasive, which can alter the surface's finish.)

It may take a few passes to get all that grime off, but you should notice a dramatic difference once

you do. If your laptop is particularly old, you may not be able to get rid of the shine on the keys; some of us may have worn down the top layer of plastic and even the letters on the keys. There's not much you can do about that.

You should be able to wipe fingerprints off your screen with a dry microfiber or soft terry cloth. If you need more cleaning power, a slightly damp cloth that has been thoroughly wrung out first can help. Some manufacturers, including Dell and Lenovo, even say you can use a 50:50 mixture of isopropyl alcohol and water to remove tough dirt. Avoid household cleaners with harsher chemicals like ammonia or Windex on the screen.

Get Rid of Bad Smells

Let's say you have a particularly terrible case of a gross laptop, and even after the above steps, your laptop still carries the essence of whatever it has been exposed to. I've seen many laptops that smelled like smoke, and getting rid of that is challenging or impossible. Cleaning the surface can help, but many of those smells may also be inside the computer. For that, you can turn to a natural deodorizer: charcoal. Don't go digging through your grill for briquettes! Cooking charcoal is different from activated charcoal. Activated charcoal is made with much more (micro) surface area to be more absorbent. Another common household item is kitty litter. It's a great odor eliminator because most kitty litter formulas have activated charcoal to neutralize litter box smells.

Seal the laptop in a bag or closable bin with a cup or so of the activated charcoal or litter and leave it for at least 24 to 48 hours. If you don't have a cat, people also had good luck with diaper pail deodorizers, which are neat little packets of charcoal you can throw away when you're done. The longer you leave the computer in the bin, the better.

Cyber Security

By David Kretchmar, Hardware Technician. Sun City Summerlin Computer Club
<https://www.scsccl.com>
dkretch@gmail.com

Recently, SCSCC Vice President Tom Burt provided members with a link to an interesting

article from *Malwarebytes* about cyber security: <https://www.malwarebytes.com/blog/news/2023/10/the-3-crucial-security-steps-people-should-do-but-dont>

Malwarebytes (2-week free or trial version) is an excellent product that other SCSCC technicians

“Everyone’s afraid of the internet and no one’s sure what to do about it.”

and I frequently use to search for malware and other potential PUPs (potentially unwanted programs) on computers. *Malwarebytes professional* is their paid-for real-time protection sold for \$30 - \$45 per computer per year.

The essential point of the article was that many internet users employ "dismal cybersecurity practices" and are too lax in implementing and using security measures designed to keep them safe and secure. Some experts estimate that one-third of individuals experienced a security breach within the past year. This sounds reasonable based on my personal experience. Still, I also find it comforting that older adults (Baby Boomers) are estimated to be four times less likely to experience a security issue than younger users. I'm unsure if we are more careful than younger users or if we do less online.

While anything that makes people aware of the dangers that stalk all of us online is valuable, I disagree with two of the three primary points raised in the article. *Malwarebytes* provided the article, and since they sell subscriptions to their products to stay in business, it is arguably in their interest to frighten people, who then will be more likely to become customers.

In the following paragraphs, I will discuss the essential three points made in the article that I find misleading, outright untrue, and primarily true (multi-factor authorization).

1. "Just 35 percent of people use antivirus software."

I call BS on this. It is rare for me to come across a computer that has no antivirus software running. Microsoft Windows Defender runs by default on Windows computers and does not have to be

turned on by the user. This is by far the antivirus software utilized by most individuals, and it has the advantage of having no cost beyond what a user initially pays for a Windows PC.

In addition to being "free," the Microsoft Windows Defender program code is updated at least monthly. The monthly security update release is scheduled for the second Tuesday of each month. The Microsoft Windows Defender virus intelligence database is updated almost daily in case of newly discovered threats, also known as a 0-day or zero-day vulnerabilities. The term zero-day refers to the fact that the vendor has just learned of the flaw – which means they have zero days to address it.

It might be that only 35% of users subscribe to an antivirus software tool other than Microsoft Windows Defender. Certainly, *Malwarebytes* would like you to buy their product, but the article states an untruth when it says that only 35% of computers are protected.

I believe Microsoft Windows Defender provides excellent protection for most users. The modern version of this security package was implemented with Windows 10 in 2015 and is further improved with Windows 11. I have examined hundreds of computers since 2015 and have never had to remove a virus protected by Microsoft Windows Defender. Before 2015, our club's hardware technicians spent as much as half our time at our Tuesday Repair SIG removing viruses from systems, but this work is no longer necessary.

2. "Just 15 percent of people use a password manager."

Again, I call BS on this. It is common for club members who come to the Tuesday Repair SIG when asked for their password to, for instance, their Google account to state, "I don't have a password; I just click on Gmail, and it appears." They are unknowingly and effortlessly using a password manager.

Without a password, you cannot use an application such as Gmail or any other mail program. Many users set up a password for Gmail or any other applications when they initiate use of that service or have this done for them by whomever is helping to set up their device.

Many users forget they have the required password because their browser's built-in password manager enters it automatically and seamlessly. Google, Edge, Firefox, and Safari all have integrated password managers with features like autofill and a password generator. They can also store credit cards and other personal information, which makes your online life more manageable. Smartphone operating systems on the Apple iPhone, Samsung Galaxy, etc. also store user credentials.

A password generator will create a unique password, such as "8X!4tZ7pas@vFyY" which is impossible to guess and memorize. A password manager best utilizes this bizarre string of characters. I have seen people write down and manually enter a generated password, but obviously, it is tedious and often takes multiple tries.

Are passwords saved by browsers secure?

Google states, "Google Password Manager and the passwords it generates are considered safe compared to similar password managers. Google uses military-grade encryption to protect your usernames, passwords, and payment information."

Microsoft states, "Microsoft Edge stores passwords encrypted on disk. They're encrypted using AES, and the encryption key is saved in an operating system (OS) storage area."

Firefox states, "Firefox Desktop uses simple cryptography to obscure your passwords. Mozilla cannot see passwords, but Firefox Desktop decrypts the password locally so that it can enter them into form fields."

In other words, the "free" password managers built into browsers and operating systems use security schemes that are like paid password managers. Naturally, marketers of these paid-for third-party services, such as Nordpass, Norton, OneLogin, and LastPass, claim built-in password managers are vulnerable.

Unfortunately, third-party password managers have been hacked, severely compromising user information. OneLogin was hacked in 2017, and LastPass was hacked in 2022. In March 2023, LastPass stated that the breach resulted in

unauthorized and unknown users gaining full access to customers' vault data, including personal information like usernames and passwords.

Yet third-party password managers urge users to buy their product rather than depend on the security built into browsers and operating systems. But any account or device can be hacked.

Unless you write down your passwords using a pencil and paper, you must trust someone and use a password manager. I would rather trust a massive entity like Google, Microsoft, or Apple over a relatively tiny software provider. Even more prominent entities, such as Norton, have been subject to internal dishonesty and theft of client data.

3. *Use multi-factor authentication (MFA)*

This is NOT BS. Multi-factor authentication (MFA) requires users to provide at least two of three categories of authentication to access an account.

- **Knowledge:** a password or PIN code,
- **Possessions factor:** a secondary device (i.e., Smartphone) or account you have, in addition to a knowledge factor.
- **Biometrics:** any part of the human body that can be offered for verification, such as fingerprints or facial recognition.

I only have one account, Interactive Brokers, that *requires* MFA. When I want to access my account, a notification is sent to my iPhone, which opens the Interactive Brokers application on my phone and identifies me using facial recognition. Thus, all three factors of MFA are utilized, which is about as good a set of authentications as you will find today.

Disadvantages of MFA

The second factor, the secondary device or account, is much stronger when a separate device is utilized. Many MFA schemes send a code to an email account, which is useless when that happens to be the account you are attempting to access. Using only an email account for secondary

authentication rather than a discrete device, such as your Smartphone, provides weaker security.

MFA can lock you out of your account when your discreet device (phone) is unavailable, runs out of juice, or lacks an internet or cellular connection.

Conclusions and Recommendations

Microsoft Windows Defender runs by default on Windows computers and does not have to be turned on by the user. Microsoft Windows Defender provides excellent antivirus protection.

The password managers provided by browsers and operating systems are reasonably secure. I believe they are similar in security compared to password managers offered by third-party vendors, maybe better. These credentials operate seamlessly with the operating system or browser, making for a much smoother internet experience.

Multi-factor authentication is the way to go if you want absolute internet security. Using the three categories of authentication, knowledge, possession, and biometrics provides some of the best security available today.

Default Apps: Where and What are they?

By Phil Sorrentino, Secretary & Newsletter Contributor, Sun City Center Computer Club,

<https://sccccomputerclub.org/>

philsorr@yahoo.com

Default Apps is a choice in the Apps section of Settings. To get there, click the Start button, then click "Settings," then "Apps," and finally, "Default apps." This is where you can choose what Apps will be used for certain types of files. Windows 10 and Windows 11 both have this feature, but the screens look a bit different. It looks like Windows 10 scratches the surface of this feature, and Windows 11 expands on it. But as an example, let's first look at the more straightforward Windows 10 screens. Let's look at one of these choices, probably familiar to most computer users, "photo viewer" (the fourth item on my list). Below the choice "photo viewer" is the icon and the name of an App. In my case, it is "Photo Gallery." By default, this App will be used when the user

attempts to open a photo file type, like a .jpg file.



Microsoft Photos Gallery Icon

Just a bit of background. Many file types (extensions - the letters in the file name after the period) have been defined, and many are commonly used daily. FileInfo.com maintains a searchable database that contains over 10,000 file extensions. They are used for documents, databases, graphic images, disk images, presentation software, email, virtual environments, file encoding, and other purposes.

Many of these file types are defined and used by specific software and are not often encountered by the average computer user. However, we usually use a few categories of file types in our daily computing lives so frequently that operating systems have identified some categories and provided specific folders for their use, such as documents, pictures, videos, and music. In this same order, you can think of these categories as Text-based, Image, Video, and Audio files. So, now that some basic categories have been defined, we can see what file types might fit into these categories. Some common file types like .docx, .xlsx, .pdf, .html, .odt, .pptx, .zip, and .txt are document file types. .jpg, .jpeg, .jpe, .png, .tiff, .gif, .heic, and .raw are image file types. .mp4, .wmv, .avi, .mov, .flv, and .mkv are video file types. And finally, mp3, .ogg, .wma, .wav, .aac, and .flac are music file types. (If this doesn't make sense, you may not see the file type extension part of your file names. Windows defaults not to show extensions. To change this, in File Explorer, click "View" and then check the "file name extensions" checkbox.) Additionally, there are categories for file types for specific uses like email, maps, and web browsers, which Windows puts into categories for convenience. For example, .msg, .pst, .edb, .ost, and .eml are email file types. .shp, .shx, .kml, .kmz, and .gpx are map-oriented file types. .html, .xps,

.css .asp, and .php are web browser-oriented file types.

So Windows provides control over the Application (or App) that will be called upon to open and/or process a file. When you attempt to open a file by double-clicking it, the "Default" App associated with the double-clicked file type will be used. For example, if you try to open a Photo document (.jpg file type, for example), the Default App (in my situation) Microsoft Photos Gallery will be used. There may be other Apps on your computer that can also do the job. If you want to see what Apps could do the job and maybe even change the Default App, click the current Default App, in my case, the "Photo Gallery" Icon, and you will see a list of the other Apps on your computer that can be used. When I clicked the "Photo Gallery" Icon, I was presented with a "Choose an App" list that included "Photos," "Faststone Image Viewer," "Microsoft Office Picture Manager," "Movie Maker," "Paint," "Paint 3D" "Photoshop Elements 13 Editor", "Snip & Sketch," and "Look for an app in the Microsoft store." (Microsoft is always anxious to provide or even sell solutions.) This list indicates the apps that could be set as the default apps for photo files. The list on your computer may be shorter or longer depending on the Apps you have installed on your computer. To change the Default App to an App in the list, click the Name of the App and the Default will be changed. Notice that below the Default Apps choice is an option to "Choose default apps by file type." Clicking this allows you to set default Apps for every file type on your computer. My computer's list of file types is quite long, totaling around 500, going from .386 to .zpl. Changing these entries is probably unnecessary, at least not for the average computer user. However, if you have specific and maybe expensive software you want to use for certain file types, this would be the place to make that choice.

Windows 11 "Default Apps" is similar but a little different. When you select Default Apps (under Settings-Apps) instead of a list of a few categories, like "mail," "maps," or "photo viewer," there is a list of all of the Apps on your computer. If you select an app, you will see a list of all the file types associated with the

App chosen. At this point, you can change the "Default App" used for the selected file type. This is similar to the "Choose default apps by file type" in Windows 10. As such, in either version of the OS, there is an attempt to give the user complete control over what App is used by default when attempting to open a specific file type.

Do You Use Two-Factor Authentication?

By Phil Sorrentino, Secretary & Newsletter Contributor. Sun City Center Computer Club

<https://sccccomputerclub.org/>

philsorr@yahoo.com

If not, you might want to consider it for specific accounts if it is offered. Two-factor authentication is a way of adding an additional level of privacy to a computer account. When you set up an account, typically on a computer server, you assign a "User Name," which is not private, and a Password, which you are advised to keep private. This provides a certain level of privacy because to access your account, you must provide the User Name, which is not private, and the password, which is, hopefully, known only to you. This is probably all you need to do for most of your accounts. However, adding another level of privacy would be prudent to guarantee that you can access the account only for specific accounts. These accounts would be those that you would be very unhappy if someone else, or some other computer, could access and download or manipulate its contents. An account that contains very personal information or an account at a financial institution might be just this type of account.



Client-Server Architecture

Keep in mind the internet employs a Client-Server Architecture. Using this architecture, your account is on a server computer, not your

home computer, tablet, or phone. These (client) devices only provide the ability to connect to the server and manipulate the account contents. So if someone else knew your User Name, which is not protected, and knew or stole or guessed your Password, which is hopefully protected, they could access the account and manipulate the contents. If it's a financial account, they could probably manipulate its value. Unfortunately, no matter how diligent you are in protecting your password, sometimes passwords become known to the bad guys, such as "hackers." If hackers get into your financial account, they can possibly use it for fraudulent financial transfers or payments, or worse, a password alone may not be enough. Even many services that don't offer two-factor authentication have instituted various checks on the computer attempting to use a particular server account, like sending an email to the email of record indicating a new computer is trying to access the account and asking, "Is this you?". If you are concerned about this, google "What happens if someone accesses my account" and see the possibilities. Nowadays, many services employ two-factor authentication to help guarantee that only the account owner can access a particular account.

Two-factor authentication is not a new concept. Banks have used a second form of identification for years, using ATMs to secure access to safe deposit boxes. When a bank customer visits a local automated teller machine (ATM), one authentication factor is the physical ATM card that the customer slides into the machine ("what you have"). A second factor is the PIN the customer enters through the keypad ("what you know"). When you want to get into your safe deposit box, you have to provide the account number ("what you know") and a key ("what you have") before they will let you into the box.

Fortunately, many, if not all, financial institution servers provide the ability to use two-factor authentication. Two-factor authentication requires a second form of identification, which you typically have. Two-factor authentication increases the probability that the requester is who he says he is. The more factors used, the higher the likelihood that the requester is the account owner. Two-factor authentication is sometimes confused with "strong

authentication," but these are different strategies. Soliciting multiple answers to challenge questions may be considered strong authentication. However, unless the process also requires "what the user has" or "what the user is," it would not be regarded as two-factor authentication.



What you know + What you have = Positive Authentication

In general, authentication can be done by "what you know," like a password or pin, or "what you have," like a badge or a smartphone, or "what you are," like a fingerprint or iris eye-print. (Some highly classified systems may require all three for authentication, which would involve possessing a password and a physical token used in conjunction with biometric data, such as a fingerprint, a voiceprint, or a retina scan.)

For most typical internet servers, the second form of identification is "what you have." The "what you have" can be a code sent to you by text, email, or phone; the account owner usually makes the choice. The code is typically a one-time-use series of six or so digits. Once the code is sent, you will have enough time to enter it into the screen that starts the authentication process. If email is selected, the server will send an email with the code to your email address of record on that server. Once you provide the correct code, you will be granted access to the account. If a voice phone call is selected, the call is made to the phone number on the record on that server. Once the phone call is answered, the digits are announced, and you can enter them on the screen that starts the process. If a text is selected, the text will be sent to the phone number of record on that server (ensure the phone number can receive texts). The code in the text can then be entered into the screen that starts the process.

Two-factor authentication adds an extra step to your login process, and depending on how the service has implemented it, it can be a minor

inconvenience or a major annoyance. (And it also depends on your patience and willingness to spend the extra time to ensure higher security.) However, in the long run, using two-factor authentication improves the security of your private information, which is undoubtedly something we all want. So, take the time to set up two-factor authentication on at least all of your financial and very private accounts.

