



OTTAWA

PC NEWS

Volume 41, Number 6

JUMBO SUMMER ISSUE

June 2024

PRODUCT REVIEW

PDFgear

by Chris Taylor

Why would anyone use anything but *Adobe Reader* to view PDF files? As I outlined at the May 1st Q&A session, Adobe Reader is the Typhoid Mary of the Internet with an endless stream of security flaws. Sophos's *Naked Security* blog reported in 2018 *Adobe fixes 85 serious flaws in Acrobat and Reader*. In a single update! SonicWall reported that 1/5 of all new malicious files are PDFs. The combination of Adobe's atrocious security record and the prevalence of malicious PDFs led me to remove *Adobe Reader* from my computers. I started using the free *Foxit Reader* many years ago.

The other reason one might look for a replacement PDF program is a need to edit PDF files. Some vendors have capable PDF editors, at prices far below *Adobe Acrobat's* perpetual licence at \$470 or subscription at \$17/month! However, there are not many free PDF editors available.

I received word about a free PDF editor: PDFgear. I was skeptical. The PDFgear website wanted me to click a big orange button labelled *Free Download*. I have often found this to be code for *Free Demo Version*. But a little research proved this to be wrong. PDFgear is truly a full featured, totally free PDF editor. The company intends to bring out a paid version in the future that will include premium features.

What do you get for the cost of a free download? A substantial array of interesting features. Along with some rough edges.

Using PDFgear as a PDF reader

When I compared how PDFgear and

Foxit Reader render PDF files, I found that both generally did a very good job at displaying PDF content. However, there were a few cases where PDFgear did it better.

Sometimes, Foxit Reader does not indicate if text is a hyperlink. While you can hover your mouse over the link and the cursor will change, just looking at the text does not show a link exists. PDFgear always displays links in blue text. I could not figure out why Foxit Reader sometimes highlighted links in blue and sometimes didn't.

Text as it appears in Foxit Reader

Typefaces: Lato, Epilogue
Read more in our article "Exploring typefaces with multiple weights or grades."

Even better: It has multiple widths

An often-overlooked variation within a single type family is width. From a narrow typeface that allows us to fit more words per line, to an extra wide face that adds personality, multiple widths offer the typographer more ways to work with type without the need to use more than one family.

The same text displayed in PDFgear

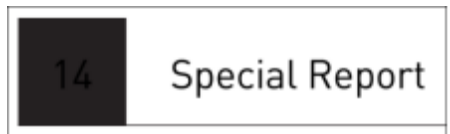
Typefaces: Lato, Epilogue
Read more in our article "Exploring typefaces with multiple weights or grades."

Even better: It has multiple widths

An often-overlooked variation within a single type family is width. From a narrow typeface that allows us to fit more words per line, to an extra wide face that adds personality, multiple widths offer the typographer more ways to work with type without the need to use more than one family.

Foxit Reader is far more configurable in its *Preferences* dialogue box, but this can be a double-edged sword. At some point, when trying to get Foxit Reader to follow my Windows choice for *Show accent colour on title bars and windows borders*, I must have chosen the option *Replace document colors > Use Windows color scheme* and all text was being displayed as black. If you have a PDF with white text on a black background, this is a real problem!

White text on black in Foxit Reader



White text on black in PDFgear



By the way, PDFgear honours my choice to display the title bar in my chosen accent colour. Foxit Reader always displays the title bar in white, making it more difficult to know which window has the focus. Programs overriding the choice for the title bar colour is a long-standing gripe of mine.

While both Foxit Reader and PDFgear do a very good job of rendering PDF files, I give a slight nod to PDFgear.

(Continued on page 13)

Inside this issue:

Next Meeting / Coming Up / Calendar	2
PDFgear	1
Transferring Files Over Wi-Fi	4
AI – What Next?	5
Cyber Security	7
Two-Factor Authorization Fiasco	9
Wi-Fi Hotspot and USB Tether	11
Stranded Alaskan Snowmobiler	12
Contact Information	15

PIZZA NIGHT: **WEDNESDAY, June 12th, 2024**

Next Meeting

Annual Pizza Night

Wednesday, June 12, 6 PM
Britannia Park Trolley Station

(see [article next page](#))

Once again we are fast approaching the end of our OPCUG season, and once again we'll celebrate it with pizza, drinks and desserts. This event is free for OPCUG members and their guests.

We will have four door prizes to give away at the pizza party:

2 Reactor Socket Shelf Ultra
2 OPCUG Travel Mugs

The sockets have six wide-spaced AC outlets with surge protection, two 3.1 amp fast-charging USB Type-A ports, an LED night light, and two shelves.

Only members are eligible to win a door prize.

The event will be, as always, on the second Wednesday of June, that is June 12, 2024, starting at 6 PM. It will be at the Britannia Park Trolley Station (see images below), under a sheltered area in case the weather does not cooperate, with free parking and bathroom access. Unfortunately, for those who like beer or wine with their pizza, alcohol is not permitted in the park. Pop and water will be provided.

To help with planning, we're asking you to register by email at pizzaparty@opcug.ca. Tell us if you are bringing guests and how many, your pizza preference (e.g. combo, special, meat lover, vegetarian, gluten free, etc.), and if you need a ride or can offer a ride.

We look forward to seeing you all in great numbers!

This is our last monthly meeting until September, but our [Q&A weekly sessions](#) will continue through the summer and there are [OPL Presentations](#) through July.

Coming Up...

11 SEPTEMBER

[BUILDING A WEBSITE – NO CODING REQUIRED!](#)

Speaker: Alan German, OPCUG

09 OCTOBER

[OTTAWA PUBLIC LIBRARY SERVICES](#)

Speaker: Carol Pearson, OPCUG

(details to follow)

13 NOVEMBER

[ARTIFICIAL INTELLIGENCE](#)

Speaker: Brett Martensen, founder of [Adaptron](#)

(details to follow)

OPL Presentations:

Thursday, 30 MAY, 6:00 pm - 7:00 pm

ARMCHAIR TRAVEL: NEWFOUNDLAND

Alta Vista Branch

Saturday, 01 JUN, 2:00 pm - 3:00 pm

ARMCHAIR TRAVEL: THE DANUBE

Nepean Centrepont

Saturday, 01 JUN, 2:00 pm - 4:00 pm

KEEPING PASSWORDS SAFE

Cumberland Branch

Monday, 03 JUN, 6:00 pm - 8:00 pm

HOW TO SECURE A HOME WIRELESS NETWORK

Rosemount Branch

Tuesday, 04 JUN, 6:00 am - 8:00 pm

HOW TO BUY A PC

Sunnyside Branch

Thursday, 06 JUN, 2:00 pm - 4:00 pm

TIPS AND TECHNIQUES FOR BETTER PHOTOS

Blackburn Hamlet Branch

Visit <https://opcug.ca/mec-category/opl-presentations/> for the full list of OPL presentations.

2024 CALENDAR

Meetings	Date	Time and Venue
Next Monthly Meeting	Wednesday, June 12 th	Pizza Night, 6-9 PM, Britannia Park Trolley Station To see all scheduled events, visit https://opcug.ca/#upcoming
Next Q&A Session	Wednesday, May 22nd	Until further notice, Q&A sessions are no longer held after regular monthly meetings. Join us on all other Wednesdays for weekly Q&A .
Next OPL Presentations	(see Upcoming Events)	Visit https://opcug.ca/mec-category/opl-presentations/ for the full list of OPL presentations.

ANNUAL PIZZA NIGHT

Pizza Time! Wednesday, June 12, 6 PM, Britannia Park Trolley Station

Once again we are fast approaching the end of our OPCUG season, and once again we'll celebrate it with pizza, drinks and desserts. This event is free for OPCUG members and their guests.



We will have four door prizes to give away at the pizza party:
2 Reactor Socket Shelf Ultra
2 OPCUG Travel Mugs

The sockets have six wide-spaced AC outlets with surge protection, two 3.1 amp fast-charging USB Type-A ports, an LED night light, and two shelves.

Only members are eligible to win a door prize.

The event will be, as always, on the second Wednesday of June, that is June 12, 2024, starting at **6 PM**. It will be at the **Britannia Park Trolley Station** (see images below), under a sheltered area in case the weather does not cooperate, with free parking and bathroom access. Unfortunately, for those who like beer or wine with their pizza, **alcohol is not permitted** in the park. Pop and water will be provided.

To help with planning, we're asking you to **register by email** at pizzaparty@opcug.ca. Tell us if you are bringing guests and how many, your pizza preference (e.g. combo, special, meat lover, vegetarian, gluten free, etc.), and if you need a ride or can offer a ride.

We look forward to seeing you all in great numbers!

Britannia Park Trolley Station
 (click image for more photos):



Map of Britannia Park
 (click image to open in Google Maps):



Sky view of Trolley Station and parking
 (click image to view larger):



PRODUCT REVIEW

Transferring Files Over Wi-Fi

by Alan German

It's often useful to be able to transfer files between a Windows computer and an Android smartphone. Normally, I use the combination of Software Data Cable and FileZilla to achieve this task. Software Data Cable establishes a link from my smartphone to my Wi-Fi network. The Filezilla FTP client on my computer is then used to make the connection and transfer files between the two devices. For those who are not familiar with the use of FTP, there is now an alternative Wi-Fi program – *LocalSend* – that makes a direct connection between instances of the app running on multiple devices.

LocalSend is open-source software that is released under the MIT license. This license permits unrestricted use of the software but, in contrast to the GPL, does not require modified versions of the code to be released into the public domain. For most of us, this means that we can just download and use the program as it is provided.

LocalSend is multi-device and multi-platform. It is installed on the devices between which files are to be transferred, e.g. a smartphone and a PC. Versions of the software are available for Windows, Linux, Android, macOS and iOS.

Once installed the basic choices are Receive and Send. There is also the option to customize the file transfer operations through a variety of settings. These include choices for themes and colours, file download location, and device name.

The basic choices when selecting the Send option on a device are to specify the files or folders to be transferred using a file manager. The program scans for nearby devices and will display any that are available. On my system, my smartphone has the default name of *Patient Pumpkin*, and my PC is named *Special Blueberry*. Figure 1 shows the program window with the image file *user_penguin.jpg* selected to be sent. Simply clicking the mouse on the *Patient Pumpkin* tile in the display window starts the file transfer process.

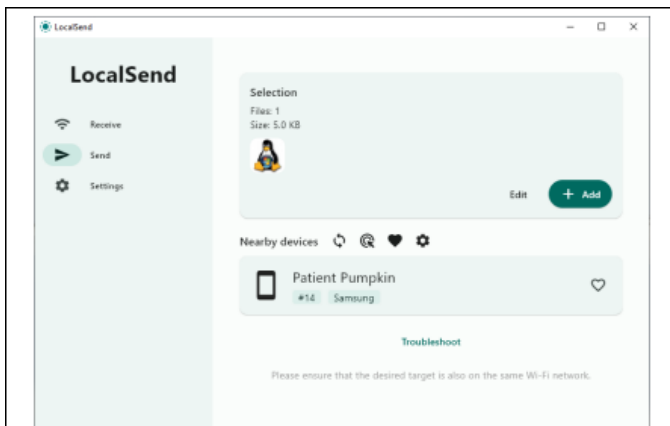


Figure 1. LocalSend ready to transfer a file.

On the smartphone, a dialogue box (Figure 2) requests permission to accept the transferred file, which is followed by confirmation that the file transfer has been completed (Figure 3).

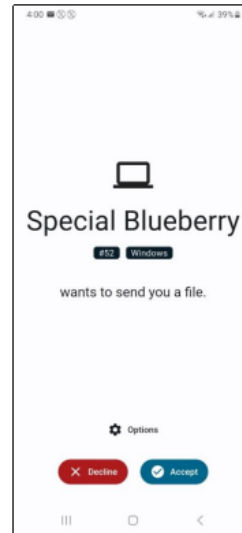


Figure 2. Accept/Decline the file transfer.

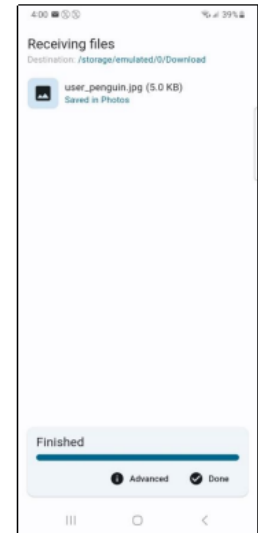


Figure 3. File transfer complete.

The transferred file is stored in the default download folder for the receiving device (unless otherwise specified in the optional settings).

LocalSend makes file transfer between a smartphone and a PC very simple. No more searching for that hardware data cable or needing to know how to drive an FTP client. Just run this app on the two devices and point-and-click to transfer files between them.

Bottom Line:

LocalSend (Open source)
Tien Do Nam
<https://localsend.org>



(see all OPCUG reviews [here](#))

Quick Tip 64: Accessing tray icons with keyboard

by Chris Taylor

I have always been a fan of keyboard shortcuts. Way back in [Quick Tip 3: Two-key program launch](#), I wrote that you can press the Windows key and a number to launch programs pinned to the taskbar.

You can also access icons in the system tray (those at the right side of the taskbar) using the keyboard. Press Win+B and a box will appear around left-most tray icon.

Use the arrow keys to move the box to the icon you want and press Enter. This will act as if you had clicked the left mouse button in it. What happens depends on the program. It might open a context menu or the full program. In some cases, it might do nothing (for programs that expect you to double-click or right-click on the icon).

If you press Win+B and want to switch back to your active program, press Alt+Tab.

AI – What Next?

By Tom Burt, Vice President
Sun City Summerlin Computer Club
<https://www.scscclub.com>
tomburt89134 (at) cox.net

(APCUG article. Reprinted with permission)

I recently came across an article from TechRepublic reviewing Intel's new Core Ultra and Xeon CPU chips with onboard support for AI. Here's the link to that article:

<https://www.techrepublic.com/article/intel-ai-everywhere-event-2023>.

I shared the article with our Tuesday Kaffee Klatch group. A friend replied, "Really interesting! What's Next?" In this article, we'll explore that question.

My first thought was, "What is AMD doing?" I ran a quick web search and immediately found that AMD has a family of Ryzen AI CPUs offering AMD's XDNA architecture. Here's a link to AMD's web page:

<https://www.amd.com/en/products/processors/consumer/ryzen-ai.html>

My next thought was, "What is ARM doing?" Sure enough, ARM also has CPU chips with onboard support for AI. ARM CPUs are the dominant chips on cell phones, tablets, and recent Apple devices. Here's a link to ARM's web page:

<https://www.arm.com/markets/artificial-intelligence>

So, all the major CPU chip families used in servers, PCs, laptops, and mobile devices incorporate onboard AI support. AI apps like ChatGPT, Bard, and Claude can run on your PC, laptop, or mobile device rather than on a cloud-based server farm. As this technology rolls out over the next few years, it will augment the available worldwide AI processing power by several billion devices.

Futurism

Usually, I avoid trying to predict the future, especially with technology. Reality tends to outstrip even "far-out-there" predictions. However, I'll have to make a few SWAGs in a "What's Next?" article, especially since I'm writing this at the beginning of the new year. However, I'll probably look at this a few years from now and laugh wryly at my naiveté. Let's look at areas where this new onboard CPU support for AI may significantly impact.

Speech Recognition and Generation

Speech recognition has come a long way since my software engineering days at Citibank's Transaction Technology Insti-

tute in the mid-1980s. Today, we are at the point where humans can talk to machines using natural, colloquial language and be understood. Even accented speech can be understood. Further, machines can now speak in natural voices and be easily understood by humans.

Machines can also translate textual content from one language to another. Combining translation with voice recognition and synthesis brings us to the realization of the science fiction concept of a universal translator.

A quick search on Google turned up two Android apps and an iOS app that offer this functionality today:

https://play.google.com/store/apps/details?id=com.speakandtranslate.voicetranslator.alllanguages&hl=en_US&gl=US

https://play.google.com/store/apps/details?id=com.erudite.translator&hl=en_US&gl=US

<https://apps.apple.com/us/app/itranslate-voice/id522626820>

For desktop computer users, Google Translate can recognize speech and translate it.

Currently, these apps, while very capable and well-rated, seem to depend on cloud-based servers for the actual translation intelligence. This means their ability to function depends on having an Internet connection. As the new CPU chips mentioned above become commonplace in mobile devices, look for more of this functionality to operate on the mobile device itself with better performance.

If you're a regular Zoom user, you've likely come across its live captioning and transcription features. Zoom can do real-time voice recognition of all the voices on a Zoom session and display the speech as text in a running window at the bottom of the screen. This is a huge aid to hearing-impaired participants. Similar technology is now providing captioning for online videos and other audio streams. For Android and iOS smartphones, there are Live Transcription apps:

<https://play.google.com/store/apps/details?id=com.google.audio.hearing.visualization.accessibility.scribble>

<https://apps.apple.com/us/app/live-transcribe/id1471473738>

Looking ahead, with advanced CPU chips in smart TVs, it becomes feasible for the TV to automatically generate live captions of any incoming audio stream and do on-the-fly translation of the source audio stream language to another language.

(Continued on next page)

AI - What Next? *(Continued from previous page)*

Customer Service

Customer service is a fertile area for applying voice recognition and synthesis. Consider a service application that can run on your smartphone, tablet, laptop, or desktop or a service kiosk, displaying a photo-realistic human face and torso, that can converse colloquially with you in any language and has a vast knowledge of the business's products, services and policies, federal, state and local regulations and has the reasoning and operational skills needed to resolve virtually all classes of customer support problems.

Customer Service is a huge cost for all businesses, a large part of which is recruiting and training service representatives. The service activity often has a high turnover rate, meaning the training expense is recurring. Also, policies and products may change frequently, requiring training updates for existing staff. An essential virtue of a "smart" customer service application is that only one master copy of the application needs to be updated, and those updates can be replicated automatically and nearly instantly in all instances of the application. Another virtue is that a "smart" service application is tireless – it will work 24 hours/day, 365 days/year, and doesn't get sick, take vacations, or lose patience with demanding customers.

Every business is somewhat different; consequently, its customer service applications must be customized. Having on-chip AI support in the CPUs of the business's in-house servers will make it easier to keep this customization and give better performance than depending on cloud-based servers. It also gives the business greater control over what data stays "in-house."

AI Companions

AI companions are an evolution of "smart" assistants like Siri, Alexa, and Cortana. Here are two articles that discuss the state of AI companion services:

<https://cybernews.com/tech/ai-companions-explained/>

<https://theweek.com/tech/the-pros-and-cons-of-ai-companions>

These systems today run on cloud servers, but with advanced AI CPUs, they should evolve to run directly on users' devices. This will provide better performance and prevent some concerns about personal information learned by these companions from being in the cloud.

Merging of AI and Robotics

In the past few years, there have been significant advances in robotics. Robots can now "see" via cameras, radar, and lidar and "hear" via microphones. This has helped in factory automation and many other repetitive actions. Self-driving vehicles are a reality, though they still need refinement.

There's also a lot of work on humanoid robots – robots with a head, torso, arms, hands, and feet that can perform tasks traditionally done by humans. These robots have been research projects but are beginning to be deployed in manual labor settings. Here are two links that survey what's current in the field. The YouTube video is quite remarkable.

<https://builtin.com/robotics/humanoid-robots>
<https://www.youtube.com/watch?v=gFp18nW7p34>

The humanoid robotic form has some challenges: The mechanical and software algorithms to keep the robot upright, especially on stairs and uneven terrain, are complex. The many small actuators needed to animate the robot's limbs draw a lot of power, which requires a large battery pack and regular recharging every few hours.

With advanced AI support in the CPU chips powering robots of all types, the robots should have more autonomy; they won't need to access the Internet cloud as much to provide their "intelligence." We can foresee a time not very far in the future when humanoid robots may serve as effective caregivers, nannies, servants, and companions in home and institutional settings. This could significantly improve the quality of life for aging seniors who are often alone and frail.

Final Thoughts

As is often the case, I've barely scratched the surface of the vastness of artificial intelligence. I kept thinking of more things to discuss as I wrote this article. I'll return to this topic now and then in 2024, both in articles and in a few of my monthly seminars.

Robotics and AI are not without concerns. Human workers, especially those in lower-skilled manual and clerical jobs, will likely be displaced. Even in creative professions, AI may be able to replace many workers by automatically synthesizing new works of art. Society must have a plan for repurposing these displaced workers.

AI will affect business, generally making it more efficient and productive. However, it can also make it easier for companies to manipulate consumers.

AI can amplify the power of government for good and evil. In the hands of despots, AI could become the ultimate tool for imposing tyranny. Used for good, AI may vastly elevate happiness and prosperity worldwide.



Cyber Security

By David Kretchmar, Hardware Technician
 Sun City Summerlin Computer Club
<https://www.scscc.club>
 dkretch (at) gmail.com

(APCUG article. Reprinted with permission)

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>

"Everyone's afraid of the internet and no one's sure what to do about it."

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

virus 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.

(Continued on next page)

Cyber Security *(Continued from previous page)*

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.

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.

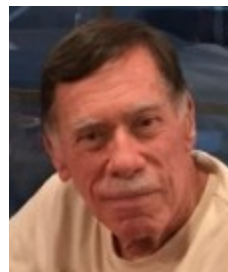
MFA can lock you out of your account when your discreet device (phone) is unavailable, runs out of juice, or lacks an internet or cellular connection.

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.



Two-Factor Authorization Fiasco

Greg Skalka, President

Under the Computer Hood Users Group Home
(uchug.org)

leditor101 (a) uchug.org

(APCUG article. Reprinted with permission)

If you are accessing a personal account or app on the web, you should be concerned about that account's security. Bad actors (and I don't mean those who can't get a job in Hollywood) constantly search for our login credentials, hoping to access our accounts and steal money or personal information. The best ways to protect online accounts include using strong passwords and protecting them, resisting attempts by others to gain access to those accounts through scams and phishing communications, and using two-factor authentication on those accounts.

Two-factor authentication, or 2FA, requires at least two identification items of different types to log into an account. It is a subset of multi-factor authentication (MFA). This can be enabled for most online accounts; some account providers now require it. It typically requires providing two or more identifying items from three categories for account access. These categories are something you know (like a password, birthdate, or the answer to a security question), something you have (could be a specific phone, computer, or email account, or a security key, fob, or dongle), and something you are (a biometric like a fingerprint).

To get money from an ATM (assuming you are not trying the big truck with a chain approach), you must provide something you have (an ATM card) and something you know (a PIN). With a 2FA-enabled online account, to gain access, you would typically need something you know (a password) and something you have (either a smartphone or computer that can receive a security code through text message or email). Entering the correct code sent to the device that presumably only you have validates your identity in a second way (in addition to the password).

Your account provider may be using 2FA, and you don't even realize it. Even if you only enter a password for access, the provider may look at the IP address or other identifying information from your device's connection to validate that it is really you (something you have). If you usually log in from one device and then suddenly use another, the account provider may ask for additional verifying information, like the answer to a security question.

It should be evident that trying to make it more difficult for others to access your accounts could also make it more difficult for you. Going through additional steps, like entering a six-digit code you were sent through a text message, takes time and opens up the possibility of being denied access. If you lose your phone, have phone communication problems, have a malfunction in your fingerprint scanner, or lose control of your email account, you may not be able to get timely access to your accounts.

I was a little apprehensive about 2FA at first due to concerns about my being denied access due to some problem outside of my control. I don't remember if I started using 2FA because I enabled it or if some account I already had started requiring it. I have used 2FA for several years on most of my critical accounts. Whenever I am asked to enable it, I look to enable it on some accounts (I have found some that did not support it then; I'm starting to think less of those companies). I typically use my phone as the second form (something I have); I need to ensure I have my phone handy when I want account access on my computer. Receiving a code as a text on a phone is supposed to be more secure than receiving it in an email. It may be a little more work, but I have had a few problems with it denying me access when I needed it.

Recently, however, I have had a few instances of being denied access to accounts through 2FA. My first instance was about a week ago when I was trying to access my Scripps online medical account on my computer to perform an electronic check-in for a medical appointment. Of course, I was in a hurry, trying to do this late at night, just before bed for an appointment the next day, and I would not have time to do it later.

After successfully entering my username and password on the MyScripps web login page, a page was provided to select the method for sending a code: email or text. I have found that my phone usually receives the text in just a few seconds. This time, however, the text did not come right away as expected. I waited maybe 60 seconds (remember, I wanted to finish this and go to bed) and then clicked "Send code again." Again, I waited, this time a little longer. I checked my phone to see that it was on and not in airplane mode or something else that would turn off reception.

(Continued on next page)

Two-Factor Authentication *(Continued from previous page)*

After waiting longer than I wanted, I finally selected email to deliver the code. Then, I had to start Thunderbird (my email program) to access my Juno email on my computer. Fortunately, the email with the code was there, and I successfully logged into Scripps and completed my task. At the time, I thought it was strange, but I didn't consider the problems I had any further. The following day, I found that the texts had come in at night.

A few days later, I tried to log into my US Bank online banking account from my computer; I again needed to check my account balance with some urgency. The US Bank 2FA code enter screen comes up right after entering a valid username and password; I may enable only texts to my phone for this. Again, I was used to having the text with the code pop up on my phone immediately, but I waited several minutes without receiving the text message. I now remembered my Scripps incident. There was no email delivery selection on the 2FA code entry screen on the US Bank website, but there was a link to "verify another way." I had hoped it would lead to verification through an email, but instead, it asked me to enter my debit card PIN.

I don't use a debit card for any of my accounts; I may have been sent one by the bank years ago, but I never activated it and had no way to get its PIN. This lack of access to my account was beginning to make me angry.

I canceled out of that screen (the only option) and tried going into the login page to get another code sent, but no code text message came to my phone. Finally, the bank locked me out of online access for too many unsuccessful attempts. I would need to change my password to get access again, and the first step for that was to send me a code that I'd need to enter. Good grief! I searched their website and finally found a number to call for online access support (they don't make things like this very obvious on their site).

While still on their site, I called the number and started my way down their automated phone menu system. Suddenly, while listening to the next set of options, I heard the sound of text messages being received on my phone. I found a bunch of texts from US Bank with 2FA codes that had just come through on my phone. I hung up the call and returned to the web page, but after entering the code from the last text, it said the code had expired, and a new one would be sent. Again, no code text was received. I called the US Bank support number again and found that action again appeared to trigger the receiving of text

messages on my phone. Again, I was too late to enter these codes, but I now saw a pattern.

I returned to the bank website and asked for a code to change my password. I then immediately called the US Bank support number, and after a few entries in their audio menu, a text arrived on my phone. I could enter this code in time, change my password, and regain access to my online accounts.

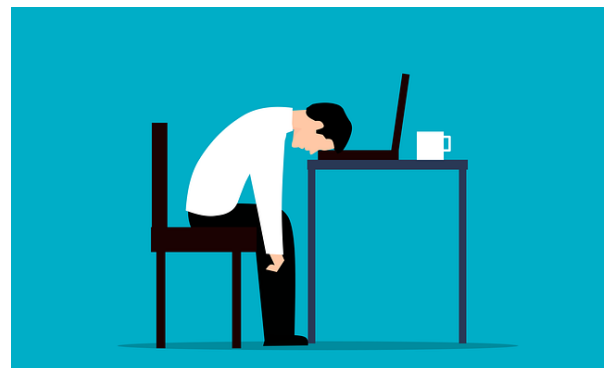
I finally got the information I needed off the website, but I was concerned about what I had to go through to get it. Why were my texts not coming through right away? It seemed like making the phone call (or pressing phone keys) triggered the reception of texts that appeared stuck somewhere.

This seemed like a problem, so I cycled power on my phone and then tried logging into my US Bank online account. This time, the text message with the 2FA code was received right after my password was accepted, just as it had been.

Something in my phone went awry, and cycling the power fixed it. I try to

remember to do that periodically; I need to be better at making that a part of my tech management routine.

I still understand that online security is essential, but I also know how it feels to be locked out due to some malfunction in the system. The lesson in resiliency to take away is not to decrease security to prevent being affected by such a failure. Still, instead, I plan so I'm not doing things at the last minute and making myself vulnerable to problems when something inevitably breaks down.



Wi-Fi Hotspot and USB Tether

If you use a smartphone Wi-Fi hotspot to provide an internet connection to a single computer, the tether option may provide advantages.

By John Krout, Presenter and Newsletter Contributor
Potomac Area Technology and Computer Society www.patacs.org

(APCUG article. Reprinted with permission)

Introduction

Many environments do not provide either reliable Wi-Fi or high-speed Wi-Fi. In those environments, some find that the only way to provide internet access for a computer is to enable a smartphone to provide a Wi-Fi hotspot.

From the viewpoint of the computer user, that hotspot is just like any Wi-Fi service. The hotspot shows up in the computer's list of available Wi-Fi services. Connection to the hotspot usually requires a password; you can find that password on the smartphone's screen.

Any Wi-Fi hotspot does face issues affecting its performance.

First, the Wi-Fi hotspot drains the smartphone battery at an increased rate, more rapidly than when the smartphone hotspot is disabled.

Second, the smartphone's Wi-Fi hotspot offers no competition for a Wi-Fi router. A router typically has two or more antennae and supplies much greater Wi-Fi signal power than a smartphone Wi-Fi hotspot.

Since a smartphone's Wi-Fi signal is weaker than a router's signal, the distance between the smartphone hotspot and the computer is critical. Put the phone as close as possible to the computer. Move the smartphone a bit farther away, and the speed of the Wi-Fi connection available to the computer declines.

Third, due to the weak Wi-Fi signal from a smartphone, the Wi-Fi signal strength and, therefore, the internet speeds may vary because of intermittent nearby interference beyond anyone's control.

In short, tether options overcome those three issues.

If your smartphone already enables you to create a Wi-Fi Hotspot, then your smartphone likely provides one or more options to use a tether.

Bluetooth tether

Both recent iPhones and recent Android phones also include Bluetooth tethering capability. However, since Bluetooth involves no cable, the capability is better described as a Bluetooth hotspot.

Again, like Wi-Fi hotspots, your carrier contract may or may not allow your use of Bluetooth tethering. Also, like Wi-Fi hotspots, Bluetooth has disadvantages. For example, Bluetooth usage accelerates smartphone battery drainage. Also, Bluetooth range for useful internet data rates is quite limited and degrades over distance.

USB Tether advantages

USB tether simply means that the smartphone provides internet service to the computer through a USB cable. The Windows 10 and 11 operating systems automatically recognize that the USB tether provides an internet connection.

The USB cable connection provides power from the computer to the smartphone, reducing battery drainage. In addition, USB cable communication requires less power than Wi-Fi or Bluetooth, reducing battery drainage.

How to enable an Android phone's USB Tether

First, attach the smartphone to a USB cable, then connect that USB cable to a USB-A socket on a computer. Most recent smartphones support USB3, so plug that cable into a USB3 socket on the computer.

After that, you use Settings on your smartphone to enable the USB Tether behavior.

Here I will show you how to enable USB Tethering behavior on my Samsung Galaxy S10 smartphone running Android 12. The main Settings app screen, shown in **illustration 1**, is the place to start. Then, on that screen, tap **Connections**, which is circled in the illustration.

In **illustration 2**, you can see the Connections screen. On that screen, tap **Mobile Hotspot and Tethering** is circled in the illustration.

Illustration 1

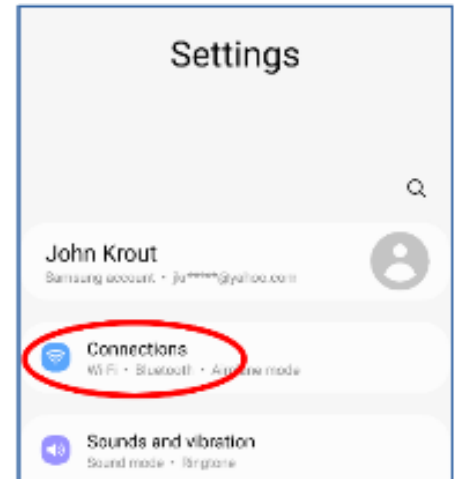
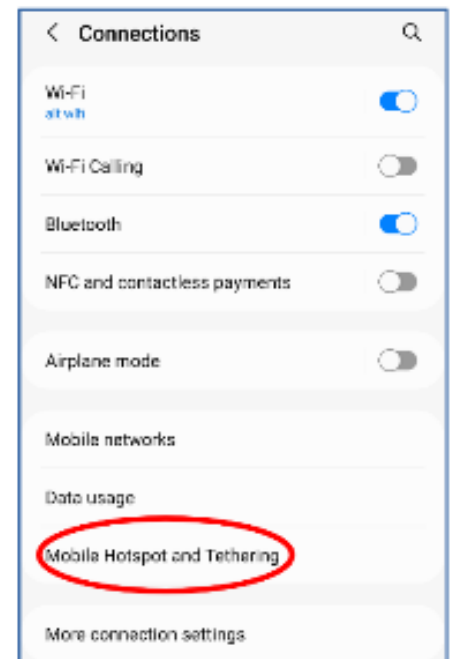


Illustration 2



In **Illustration 3** (next page), you can see the Mobile Hotspot and Tethering screen. As shown, the USB Tethering switch is disabled. However, if a USB cable connects your smartphone and the computer, that USB Tethering switch will be enabled, like the Mobile Hotspot switch in the illustration.

(Continued on next page)

Wi-Fi Hotspot (Continued from page 11)

Illustration 3



After connecting the USB cable to the smartphone and the computer, tap the enabled USB Tethering switch to turn it on.

When you do so, the computer should recognize the available internet connection via the connected USB cable within a few seconds.

How to enable an iPhone's USB Tether

On my iPhone X, the equivalent Settings screen sequence to turn on a hotspot are **Settings→Cellular→Personal Hotspot**. Unfortunately, my iPhone is not currently on a carrier contract. Therefore, Cellular is ghosted (disabled) in Settings, so I cannot enable and test an iPhone personal hotspot.

The iPhone user's manual ebook on my iPhone does not document a USB tether capability. However, USB tether documentation on this iPhone support web page seems to indicate that a USB tether connecting an iPhone running iOS 15 to a computer can be accomplished without turning on any Settings switch: support.apple.com/en-us/HT204023

Ethernet tether

You might think: my smartphone cannot connect to an Ethernet cable! On the contrary, perhaps it can, but you must spend some money to make it happen.

As you can see in illustration 3, my Samsung Galaxy S10 phone supports an Ethernet tether. To use that Ethernet tether, a smartphone must support On-The-Go (OTG) capability. The existence of that Settings Ethernet Tether switch may indicate that OTG is, in fact, supported. I happen to know by testing my S10 phone that the phone does support OTG. To use OTG with Ethernet, you must obtain a 3-way OTG adapter and a USB-to-Ethernet

adapter. With the OTG connected to the phone to power, the USB side of the USB to Ethernet adapter, and an Ethernet cable connected to the Ethernet adapter and to a computer, the Ethernet Tether switch will be enabled.

Most of us already have the USB cable for a USB tether, so the USB Tether method is essentially more straightforward and cost-free than Ethernet Tether. Therefore, I suspect that the USB Tether method will be preferable for all readers of this article.

Final Notes

A smartphone hotspot or tether will **never be any faster than the available speed provided by the nearest cell tower**. The very nature of cell towers means that factors beyond the control of any one person will cause the download and upload speed to vary. I have measured the 4G download speed from the cell tower about two blocks away from my suburban home a few times. The speed has been as high as 12 megabits per second and as low as 1.8 megabits per second.

Carrier companies claim that 5G will improve the speeds, but there are still caveats: 5G runs at a rate greater than 4G only if you are close to a 5G-compatible cell tower. Also, for maximum speed, the cell tower must not be overloaded. Unfortunately, that condition is beyond the control of anyone other than the carrier company. Nevertheless, carrier companies are marketing 5G hotspots to businesses to use as an alternative to wired Internet connections. If that marketing succeeds, then 5G-compatible cell tower overloading may become the new 5G normal in cell towers serving residential and commercial customers.

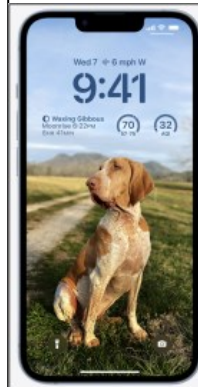
ABOUT THE AUTHOR: John Krout has been writing about the creative uses of personal computers since the early 1980s and now writes about the creative uses of smartphones, tablets, and digital cameras. He is a retired software engineer who spent his career collecting requirements, developing designs, coding in C and C++, and writing documentation for systems large and small used by Federal government agencies. He lives in Arlington, VA, and is a member of the APCUG Speaker's Bureau.



Stranded Alaskan Snowmobiler Saved By iPhone's Emergency SOS Via Satellite Feature

By Kurt Jefferson, Editor, Central Kentucky Computer Society <https://ckcs.org/lextown2> ** gmail.com

(APCUG article. Reprinted with permission)



In early December, the Alaska Department of Public Safety issued a **brief report** about a man stranded on a snowmobile in a remote part of the state.

The man pulled out his iPhone 14 and used the Emergency SOS via Satellite feature to call for help. The Emergency

Apple's new iPhone 14 offers a feature called Emergency SOS via Satellite. It automatically calls Apple's Emergency Response Center when cell phone or Wi-Fi service is unavailable and a 911 call is placed. A snowmobiler stranded in a remote area of Alaska is the first person to use this service according to the Apple Emergency Response Center.

Courtesy: Apple

SOS via Satellite service is automatically triggered on all iPhone 14 models when an

attempt is made to call 911, and cell service or Wi-Fi is unavailable.

This was apparently the first time the iPhone's satellite phone feature was used to rescue a stranded individual.

From the Alaska Department of Public Safety report (according to [9to5Mac](#)):

"On December 1, 2022, at around 2:00 am, the Alaska State Troopers were notified that an adult male traveling via snowmachine from Noorvik to Kotzebue had activated an Apple iPhone Emergency SOS via satellite on his iPhone after becoming stranded. Working with local search and rescue teams, the Apple Emergency Response Center, and the Northwest Arctic Borough Search and Rescue Coordinator, the NWAB SAR deployed four volunteer searchers to the Nimiuk Point area directly to the GPS coordinates provided by the Apple Emergency Response Center. The adult male was located and transported to Kotzebue by the volunteer search team. There were no injuries reported to Troopers."

(Continued on page 14)

PDFgear (Continued from page 1)

And PDFgear can do something Foxit Reader does not even attempt: edit PDF files.

The ability to edit PDF files is a stand-out feature, especially in free software. Unfortunately, PDFgear offers a very mixed bag. While the website says you can *Edit PDF text like in Microsoft Word*, the reality is somewhat less than the promise.

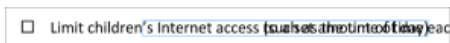
What PDFgear struggles with

PDFgear allows you to edit any text within a PDF file. But with complex layouts, it is an exercise in frustration. I could drag a text placeholder to a different location on the page. If I added text, the placeholder would extend vertically, but I couldn't change the width of any placeholder.

Choosing *Edit Text* allowed me to do in-line edits. Choosing *Edit Object* allowed me to select strange snippets of text in blocks scattered throughout the page. In the example below, moving the mouse around caused the blue box showing 's Internet access to appear. Why this selection was part of a sentence in the middle of a paragraph is a mystery. I chose the option to Edit and the text opened in an edit box rather than allowing me to edit in-line like in *Microsoft Word*! I added the text (*such as the time of day*).



After clicking the *OK* button, I ended up with the following:



Suffice it to say, simple small edits *may* be possible without ending up with a total mess, but don't count on it.

Given PDFgear can convert PDF files to several formats, including Microsoft Word, I thought maybe I could convert the PDF to Word, edit the text there, and save it back as a PDF file. Unfortunately, PDF files with any sort of complex layout tend to convert into Word documents that are a total mess. In most cases, Microsoft Word itself does a

more credible job opening a PDF file and allowing you to edit it. But complex layouts in PDF files will stymie Word too.

PDFgear can convert a lot of document formats, such as Word and PowerPoint files to PDF. It generally does a decent job, but I found using the *Microsoft Print to PDF* virtual print driver built into Windows always did at least as good a job and sometimes much better. In the following example, a PowerPoint text box with graduated background and bevelled edges shows correctly when using *Microsoft Print to PDF*.

Two-way firewall problem

If you use a two-way firewall

- you may get a popup asking if a program should be allowed to access the Internet
- and you won't know the right answer

But when converted by PDFgear, the shading & beveling are lost, and the text is not aligned well.

Two-way firewall problem

If you use a two-way firewall

- you may get a popup asking if a program should be allowed to access the Internet
- and you won't know the right answer

When filling forms, PDFgear did not honour data type restrictions. On a CRA fillable tax form, while Foxit Reader would not allow alphabetic characters in the SIN field, PDFgear didn't care. Then I discovered that filling in the PDF form using a web browser (Edge, Firefox, Chrome, or Opera) also allowed letters in the SIN field. Go figure.

I filled out the CRA T1 tax form in PDFgear, saved it, then opened it in Foxit Reader and all the fields I had filled in were blank! Opening the PDF file in a browser displayed form data correctly. Chalk this one up to a problem with Foxit Reader...I guess?

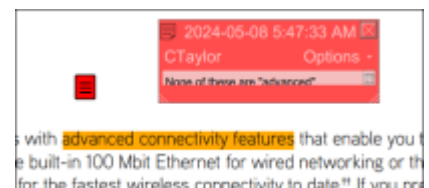
What PDFgear does well

PDFgear has strong annotation features. You can easily highlight text, add lines, stamps, and more. Unfortunately, while it allows handwriting, it doesn't support pens. Rather than using the pen with my Wacom Cintiq display, I had to write *WOW* in the example below using a mouse, with the expected poor result!

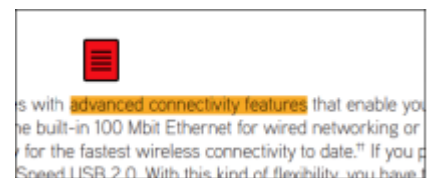


I found an issue with *Comments*. While the comment box labelled *CTaylor* above looks nice, when I opened the PDF file in other programs the comment box was far less attractive. I don't know if this is the fault of PDFgear or the other readers.

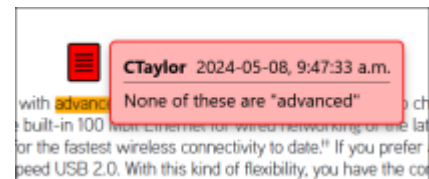
Foxit Reader



Comment missing in Edge



Comment overlays text in Firefox



PDFgear allows you to easily move pages around, insert additional pages from other PDFs or Word documents, and extract images & entire pages. You can insert and edit hyperlinks. You can even crop and rotate pages.

The program can perform optical character recognition of text within images, but I found it to be somewhat hit and miss. If you use the feature, be sure to proof what it produces.

PDFgear can compress PDF files with three different compression levels. It resulted in impressive size reductions with resulting files between 15% and 50% the size of the original file. The

(Continued on next page)

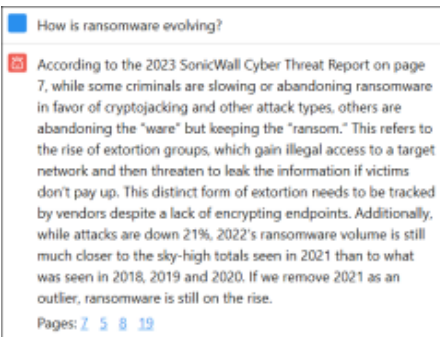
PDFgear (Continued from previous page)

quality of embedded images was virtually indistinguishable from the originals when using low compression. There were noticeable artifacts when using high compression.

You can add watermarks and headers & footers. I ran into a problem with headers and footers when trying to have page numbers formatted as *Page x of y* on the right for odd pages and on the left for even pages: a common enough thing. It put *Page 1 of 17* at the right of page 1, *Page 1 of 17* at the left of page 2, *Page 2 of 17* at the right of page 3, *Page 2 of 17* at the left of page 4, etc.

Copilot

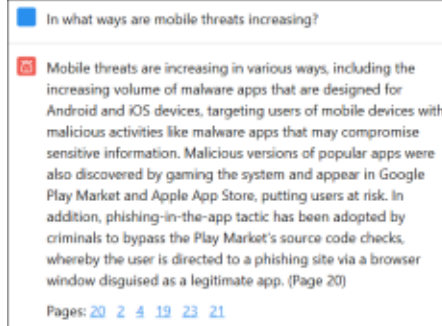
Every program wants to include AI features and PDFgear is no exception. Clicking the Copilot icon that appears in the bottom-right of the program window opens the Copilot pane and the document is analysed. You can ask Copilot to do things like *Summarize this PDF file* or query about things that may be in the document such as the following in a security threat report. It finds related information anywhere in the PDF, pulls it all together, and provides links to the relevant sections.



On occasion it threw its hands up in defeat yet still linked to pages that had the information:



Rephrasing the question returned better results:



When I asked Copilot to *Add a bookmark called "Ransomware" to page 7*, it responded *Would you like to add an annotation to current view?* It appears Copilot is a work in progress.

Late breaking news: Microsoft is set to replace the code in Edge that allows it to read PDF files with the Adobe engine. I highly recommend you make sure Edge is **not** the default to read PDF files!

I had one final issue with Foxit Reader. They sell *Foxit PDF Editor*, so when you install or update Foxit Reader, an option to *Install a free 14-day trial of Foxit PDF Editor* is "helpfully" preselected for you. Of course, if PDFgear releases a premium, paid version, they may pull the same stunt.

Conclusions

PDFgear and Foxit Reader render PDF files well. While I had some minor issues with Foxit Reader, if my only aim was to display PDF files, I probably would not have changed to PDFgear.

The ability to edit text in PDF files is hit and miss. Simple layouts don't cause many problems, but complex layouts are guaranteed to frustrate.

Features including annotation, hyper-linking, rearranging pages, and extracting pages & graphics, are all quite good, even though there are some rough edges.

When it works, Copilot can do a stellar job of helping you find relevant information in a PDF file.

Bottom line:

PDFgear v2.15

Price: free

Website: <https://www.PDFgear.com/>

(see all OPCUG reviews [here](#))

(return to page 1 [Table of Contents](#))

Stranded (Continued from page 12)

MacRumors **reports**: "Apple's Emergency Response Center worked with local search and rescue teams and the Northwest Arctic Borough Search and Rescue Coordinator to send out volunteer searchers directly to the GPS coordinates relayed to Apple using the emergency function. The man was rescued successfully, and there were no injuries.

However, the area where he was located is remote and on the fringes of where satellite connectivity is available. Apple says satellite connectivity might not work in places above 62° latitude, such as northern parts of Canada and Alaska, and Noorvik and Kotzebue are close to 69° latitude."

Business Insider reports authorities located the man at Nimiuk Point and was taken to Kotzebue by the rescue team at 6 am 9to5Mac writes the emergency satellite service is available in iPhone 14 models because of a new radio chip included in those phones.

Garmin, a long-time maker of smartwatches and exercise apps, launched a similar service in 2011 called inReach Messenger.

As of October 2022, Garmin reported that its emergency service had helped 10,000 people who needed immediate assistance.

Garmin says its service is often used to help other folks who don't own the device make the emergency call. In addition, Garmin lists the top five reasons people have used its emergency service over the past eleven years:

1. Injury
2. Medical issue
3. Vehicle accident
4. Stranded/Stuck
5. A vehicle problem

The top five incidents requesting emergency help from Garmin:

1. Hiking/Backpacking
2. Driving
3. Motorcycling
4. Climbing/Mountain climbing
5. Boating



OTTAWA PC NEWS

Ottawa PC News is the newsletter of the Ottawa PC Users' Group (OPCUG), and is published monthly except in July and August. The opinions expressed in this newsletter may not necessarily represent the views of the club or its members.

Member participation is encouraged. If you would like to contribute an article to Ottawa PC News, please submit it to the newsletter editor (contact info below). Deadline for submissions is three Sundays before the next General Meeting.

To receive the monthly newsletter by email, send an email to:
opcug-newsletter+subscribe@googlegroups.com (leave subject and body fields blank)
 You do **not** need to create a Gmail or Google Groups account.

To subscribe to other OPCUG Google Groups member services, go to:
<https://opcug.ca/google-groups-how-to/>

Group Meetings

OPCUG meets on the second Wednesday in the month, except July and August, at the Riverside United Church, 3191 Riverside Drive, Ottawa. Parking is free at the church. OC-Transpo bus #90 stops nearby. Details at <https://opcug.ca/venue/>.

NOTE: Until further notice, all our events are via video conference.
 Details at <https://opcug.ca/venue/>

OPCUG Membership Fees: \$20 per year
Mailing Address: 3 Thatcher St., Nepean, Ontario, K2G 1S6
Web address: <https://opcug.ca>
Follow us on Facebook: <https://www.facebook.com/opcug>
Follow us on Twitter: <https://www.twitter.com/opcug>

President and System Administrator		
Chris Taylor	chris.taylor@opcug.ca	613-727-5453
Meeting Coordinator		
Vacant	meetings@opcug.ca	
Treasurer		
Alan German	alan.german@opcug.ca	
Secretary		
Gail Eagen	gail.eagen@opcug.ca	
Membership Chairman		
Mark Cayer	mark.cayer@opcug.ca	
Newsletter		
Brigitte Lord (editor/layout/e-distribution)	brigitte.lord@opcug.ca	
Public Relations		
Vacant	PR@opcug.ca	
Facilities		
Bob Walker		613-489-2084
Webmaster		
Brigitte Lord	webmaster3@opcug.ca	
Privacy Director		
Wayne Houston	privacy2@opcug.ca	
Special Events Coordinator (Mr.) Jocelyn Doire	jocelyn.doire@opcug.ca	
Director w/o Portfolio		
Karen Wallace-Graner	karenwg@opcug.ca	
Director w/o Portfolio		
Bob Herres	bob.herres@opcug.ca	

© OPCUG 2024.

Reprint permission is granted* to non-profit organizations, provided credit is given to the author and *The Ottawa PC News*. OPCUG requests a copy of the newsletter in which reprints appear.

*Permission is granted only for articles written by OPCUG members, and which are not copyrighted by the author. Visit <https://opcug.ca/copyright-and-usage/>.



Q&A HAS GONE ON-LINE! WEEKLY!

Because of the pandemic, the OPCUG is holding weekly Q&A sessions in Zoom video-conferences.

Join us every Wednesday (except on regular monthly meeting nights) at 7:30 pm to discuss computer issues. Questions (and answers) on any computer-related issue are welcome. Or, do you have a favourite computer program or topic that you would like to share with the group? Send your questions, answers, or the details of what you would like to share to:
SuggestionBox@opcug.ca

Everyone is welcome to attend Q&A sessions and to ask questions about their specific computer-related problems. Join us at: <https://tinyurl.com/opcug-meeting> (if you use the Zoom client, the meeting ID is 924 9556 0898 and the password is **opcug**).

OPCUG



Users helping users
 for over 40 years