BROWSER NO 227

DECEMBER 2025

Return address:
Busnet Computer Club Inc.,
22 Peel Terrace
Post Office Box 1109, Busselton WA 6280
Busnet.org.au, info@busnet.org.au
Busselton Senior Citizens' Club email address
manager@bscc.net.au
Web maintained by kg@kgweb.au

The Busselton Constitution is available on the Busnet website at busnet.org.au. This is a very useful and interesting site with lots of up to date information about our Club.

Table of contents:

Wishing you all a very happy, healthy and safe Christmas and New Year from your president and committee

This is my last browser. It has been a long time, about ten years since I took over from Nancy. I have enjoyed the journey and I hope you have found at least some of the articles of use and interest over that time.

Finding stuff has every month is a task I will miss—the cartoons as well as the articles about things we computer people want or need to know.

Thank you all for your long and kind support and friendship. I'm not leaving Busnet so hope to catch up in the New Year at meetings and coffee mornings for a long time to com.

Wishing you all a happy, healthy and safe Christmas and 2026.

Pam

You Can Delete, Change or Manage Your YouTube Search Results

https://www.google.com/search?q=how+to+view+and+change+your+youtube+history+

https://support.google.com/youtube/answer/95725?hl=en&co=GENIE.Platform%3DAndroid

Sometimes you get notifications of subjects you are no longer interested and don't want to receive them anymore. You can go to the website for two short videos in how to do this. Or you might want to make your YouTube

You can view your YouTube history by tapping your profile picture, then selecting "History" or "Manage all history," which takes you to a list of recently watched videos. To change your history, you can delete individual videos, clear your entire history, or pause history-saving through the "Manage all history" or "My Activity" page.

How to view your YouTube history

- **From the YouTube app:** Tap your profile picture (usually in the bottom right) and then tap "History" or "View all" next to "History" to see a list of videos you've watched. You can also find "Manage all history" under "Settings".

From a computer: Go to the YouTube homepage, click the three horizontal lines in the top-left corner to open the menu, and then select "History". Alternatively, go to My Activity, sign in, and click on "YouTube History" to see and manage your history.

This video shows how to view your YouTube watch history:

How to change your YouTube history

- ***Delete individual videos*:**
  - **In the app:** In your history list, tap the "X" or three dots next to a video and select "Remove from watch history" or tap "Delete" next to the video.
  - **On a computer:** Click the "X" next to a video in your history list to remove it.
  - **Clear all or a custom range of history:**
  - Navigate to "History" and tap or click the three dots in the top-right corner, then select "Clear all watch history".
  - From there, you may be redirected to your My Activity page where you can choose to delete videos from today, a custom time frame, or all time.
  - **Pause or manage history settings:**
  - Go to the "Manage all history" page via "Settings" in the app or by going to My Activity.

\(Continued on next page)

(Continued from previous page)

Here, you can turn off saving your watch history completely or set up automatic deletion for a specific period. This video explains how to clear your YouTube history:

Manage your recommendations & search results

There are several ways to influence your YouTube recommendations and search results. We give you the option to let us know when certain content might not be of interest to you, such as a video or a channel, and you can manage your Google Account activity, like videos, and more.

You can also edit, turn off, or delete your watch and search history to refine your recommendations. Learn more about how to manage your watch history and search history.

If you don't want video recommendations on Home, you can delete and turn off your watch history.

Tune your recommendations

One of the ways you can influence your recommendations is by tuning them to be more relevant to you and your interests. When you give us feedback, like when a video on your Home feed isn't interesting to you, it helps us improve your YouTube experience in the future.

Mark content as "Not interested"

There are several ways to influence your YouTube recommendations and search results, including letting us know when certain content might not be of interest to you, such as a video or a channel.

1. Click More next to the title of the video, playlist, or section on Home.
2. Click **Not interested** .

If it's a video, click **Tell us why** to share why you're not interested. You can select **I've already watched the video** or **I don't like the video** to further customize your recommendations.

Adjust channel recommendations

1. On certain pages, such as your Home and Watch Next pages, find a video from a channel that you don't want recommended to you.
2. Click More next to the video title.

Select **Don't recommend channel** .

Clear "Not interested" & "Don't recommend channel" feedback

If you don't want your "Not interested" and "Don't recommend channel" feedback to influence your recommendations, you can clear it.

Go to My Activity.You might need to sign in to your Google Account.

1. Find **Other Google activity** in the left-hand menu or under the My Activity banner.

Select **YouTube 'Not interested' feedback**, then select **Delete.**

See fewer Shorts

On certain pages, such as your Home and Watch Next pages, you may also be recommended Shorts to watch. You can choose to see fewer of these.

On the YouTube app, go to your Home feed.

1. Scroll to a grid of Shorts.
2. At the top of the grid, tap More .

Tap **Show fewer Shorts**.

Clear "Show fewer Shorts" response

If you opted to be shown fewer Shorts, you can clear this decision in My Activity.

Go to My Activity.

1. Find and select **Other activity** in the left-hand menu or under the My Activity banner.

Under "Show fewer Shorts," select **Delete**.

Manage recommendations from your Google Activity

YouTube may also use data from your Google Account activity to influence your recommendations, search results, in-app notifications, and suggested videos in other places.

\(Continued on next page)

(Continued from previous page)

You can view and control your activity at myactivity.google.com. Learn more about controlling activity for your Google Account.

Manage liked videos

Your recommendations and search results are also based on videos that you've liked. You can like, dislike, and remove liked videos to influence your recommendations and search results.

Explore recommended topics

If you only want to see recommended content about a specific subject, explore topics on the Home and watch pages. Topics are based on your existing, personalized suggestions and on content related to what you interact with. These topics are meant to help you find content you want to watch faster. For example, a topic called "Learning" may have educational videos.

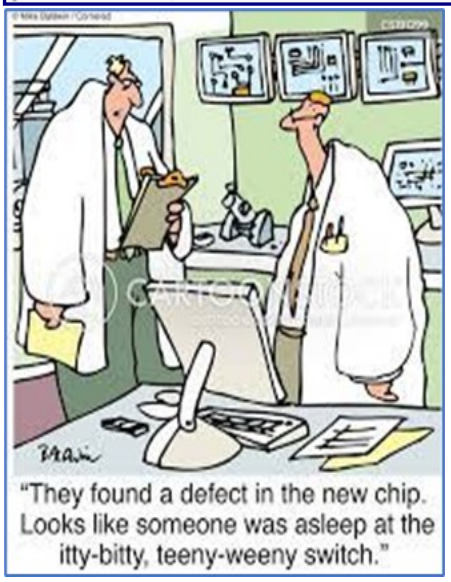
For all the graphics and videos please go to the websites listed above.

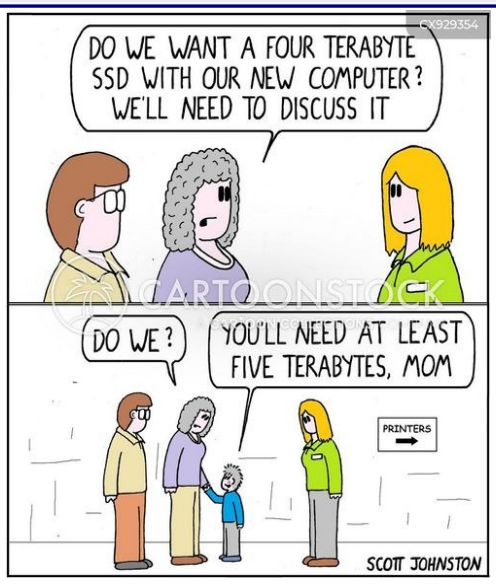
BUSNET COMPUTER CLUB INC

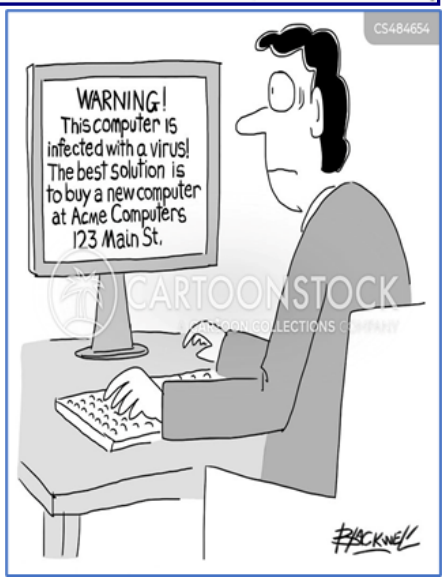
January 2026 ROSTER

DATE	DAY	Reception & Technician	DATE	DAY	Reception & Technician	DATE	DAY	Reception & Technician
	Monday			Wednesday			Friday	
		CLOSED		CLOSED			CLOSED	
05/01/2026	Monday	Kerry Mclements	07/01/2026	Wednesday	Heather Maclean	09/01/2026	Friday	Trevor Gray
		Peter Quinby			Bill Whipp			Bill Whipp
		Jake Challis			Tony Hill			Tony Hill
12/01/2026	Monday	Lois Ralph	14/1/26	Wednesday	Peter Ralph	16/01/2026	Friday	Jane Buckley
		Peter Quinby			Bill Whipp			Bill Whipp
		Jake Challis			Tony Hill			Tony Hill
19/01/2026	Monday	Maureen King	21/01/2026	Wednesday	Michelle Chaplin	23/01/2026	Friday	Ursula Hillman
		Peter Quinby			Bill Whipp			Bill Whipp
		Jake Challis			Tony Hill			Tony Hill
26/01/2026	Monday		28/01/2026	Wednesday	Heather Maclean	30/01/2026	Friday	Peter Ralph
	PUBLIC HOLIDAY				Bill Whipp			Bill Whipp
					Tony Hill			Tony Hill

Any changes to the Roster contact Peter on 0429 185 066 OR email treasurer.busnet@gmail.com

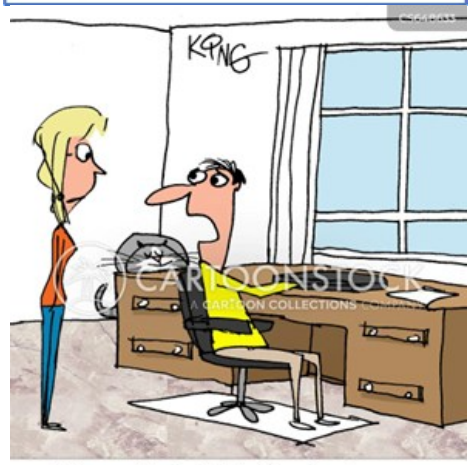






INFLOWS	
Activity Fees	167.20
Computer Sales	200.00
Home Visit	20.00
Membership	360.00
Printing	11.40
Raffle Sales	33.00
Refunds	-20.00
TOTAL INFLOWS	**771.60**
OUTFLOWS	
Bills & Utilities	
Internet	65.50
TOTAL Bills & Utilities	65.50
BSSC Rent & Internet	290.00
Insurance	114.07
Square Terminal	2.66
TOTAL OUTFLOWS	**472.23**
OVERALL TOTAL	**299.37**

"It's a phishing scam. Don't take the bait."



"When my laptop thinks I'm going to open a strange attachment, it automatically closes. It won't open until I promise not to do it again."

Google denies analyzing your emails for AI training - here's what happened

Lance Whiteney, 23/11/2025, https://www.zdnet.com/article/google-denies-analyzing-your-emails-for-ai-training-heres-what-happened/

You can opt out of the features in question if you're still concerned. Here's how.

Google is denying allegations that it has altered certain Gmail settings, which allow it to analyze private emails and other data to train its AI models without users' knowledge or permission. These allegations cropped up earlier this month in the wake of a class action lawsuit charging the company with privacy violations over this supposed change.

Referencing a discussion thread about this on X, security firm Malwarebytes published a blog post last Thursday, claiming that the change rolling out to Gmail users allows Google to view their private emails and attachments to train Gemini and other AI tools. Features cited in the allegations include Smart Compose, Smart Reply, and predictive text.

I contacted Google for comment, and a spokesperson sent me the following statement:

"These reports are misleading – we have not changed anyone's settings. Gmail Smart Features have existed for many years, and we do not use your Gmail content for training our Gemini AI model. Lastly, we are always transparent and clear if we make changes to our terms of service and policies."

In response to Google's pushback, Malwarebytes updated its blog post with the following commentary:

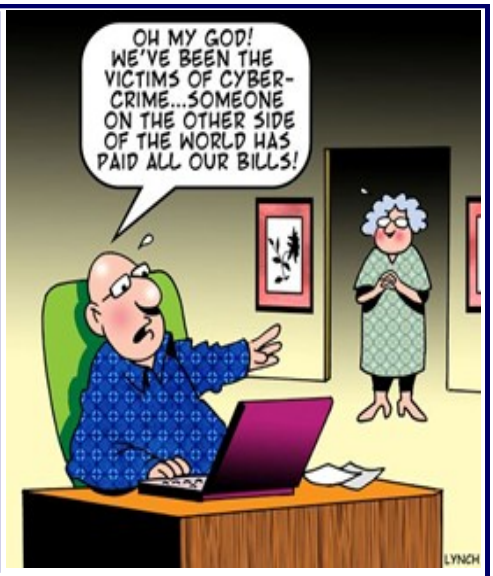
"We've updated this article after realizing we contributed to a perfect storm of misunderstanding around a recent change in the wording and placement of Gmail's smart features. The settings themselves aren't new, but the way Google recently rewrote and surfaced them led a lot of people (including us) to believe Gmail content might be used to train Google's AI models, and that users were being opted in automatically. After taking a closer look at Google's documentation and reviewing other reporting, that doesn't appear to be the case."

Malwarebytes further said that Gmail does scan the content of your emails to enable its smart features such as spam filtering, email categorization, and writing suggestions. But the security firm said that this is "normal" behavior and is different from using your data for AI training.

Yes, these smart features have been around for years. But even if they're not being used for AI training, they seem to

(Continued on next page))

Committee members for 25/26			
President	Peter Quinby	pquinby@protonmail.com	0419 047 714
Vice President	Colin Hartley	eehartley51@gmail.com.	427451252
Secretary	Lois Ralph	phylpeach@gmail.com	0400 787 789
Treasurer	Peter Ralph	treasurer.busnet@gmail.com	0429 185 066
Technicians	Bill Whipp	uuruu46@gmail.com	0435 651 488
	Peter Ralph	treasurer.busnet@gmail.com	0429 185 066
	Peter Quinby	pquinby@protonmail.com	0419 047 714
	Tony Hill	tonyhill@mac.com	0422 106 119
	Jake Challis	adude490@gmail.com	
Committee Members	Ron Grigg	ron2grigg@gmail.com	9752 4210
	Bill Whipp	uuruu46@gmail.com	0435 651 488
	Michelle Chaplin	michelle17@iinet.net.au	0417 189 394
	Tony Hill	tonyhill@mac.com	0422 106 119
	Heather Maclean	heathermaclean@outlook.com	0427 893 952
	Pam Shanks	pamela.shanks44@gmail.com	0418 898 207



(Continued from previous page)

be enabled automatically. The Verge reported that one of its staffers said they had opted out of some of the smart features but had been opted back in so that they were enabled.

What I found

I checked the three Gmail settings described by Malwarebytes in my own account as well as several other Google accounts, including two I created on the spot. For the two new accounts I set up, a Privacy and Terms page described some of the data that Google could collect. Here I could tell it to not save certain data, such as my web and app activity. However, there was no mention of potentially using my emails or other data for smart features.

In each of the accounts, all three settings highlighted by Malwarebytes were automatically enabled.

The first setting, "Turn on smart features in Gmail, Chat, and Meet," allows Google to use your content in these products to provide smart features and personalize your experience.

The second setting, "Smart features in Google Workspace," allows Google Workspace to use your Workspace content and activity to personalize your experience. Workspace includes apps for businesses and schools, such as Gmail, Chat, Meet, Drive, and more.

Specifically, enabling this setting means that Google can show events from Gmail in your calendar, such as flight itineraries and invitations. You're also able to run more personalized searches that use keyword suggestions, file suggestions, and more relevant results. Further, you can ask Gemini to summarize content, create drafts, find key information, and use other Gemini for Workspace features.

The third setting, "Smart features in other Google products," lets Google use your Workspace content and activity to personalize your experience in other products. These could include restaurant reservations and to-go orders in Maps, tickets and loyalty cards in Google Wallet, answers and reminders in Google Assistant, and suggestions and answers in the Gemini app.

About that lawsuit

What about the lawsuit that seemed to trigger the concerns and controversy? Filed on Nov. 11 in federal court in San Jose, California, the proposed class-action lawsuit alleges that Google secretly granted Gemini access to the private communications of Gmail, Chat, and Meet users. As reported by Bloomberg on Nov. 12, the suit charges that doing so without the consent of users and making it difficult to opt out may be a violation of the California Invasion of Privacy Act.

"On or about October 10, 2025, Google secretly turned on Gemini for all its users' Gmail, Chat, and Meet accounts, enabling AI to track its users' private communications contained in those platforms without the users' knowledge or consent," the lawsuit alleges. "As of the date of this filing, Google continues to track these private communications with Gemini by default, requiring users to affirmatively find this data privacy setting and shut it off, despite never 'agreeing' to such AI tracking in the first place "

Based solely on Google's explanation, most of the allegations in the suit seem to be without merit. But that doesn't mean there's no cause for concern. The biggest question is why Google is automatically enabling these settings, and seemingly without your knowledge or permission.

How to opt out

If you don't use the smart features and other options, you can certainly turn off any or all of the three key settings. Here's how.

(Continued on next page)

(Continued from previous page)

On the desktop, sign in to the Gmail website, click the Gear icon in the upper right, and then select the button to view all settings. At the General screen on the Settings page, look for the Smart features section. If the setting for "Turn on smart features in Gmail, Chat, and Meet" is turned on, click the checkbox to turn if off.

In the next section for Google Workspace smart features, click the button to manage Workspace smart feature settings. At the pop-up window, turn off the switches for "Smart features in Google Workspace" and "Smart features in other Google products."

In the Gmail mobile app, tap the three-lined icon in the upper left and select Settings. In the iOS app, tap the setting for Data privacy. In the Android app, tap the name of your Google account. Turn off the switch for Smart features. Tap the option for "Google Workspace smart features" and then turn off the switches for "Smart features in Google Workspace" and "Smart features in other Google products."

If you do turn off all three settings, keep in mind that certain smart features may no longer operate as expected, including Smart Compose and Smart Reply. But Gmail itself will still work normally. As always, it's a choice between convenience and privacy, and that's something only you can decide for yourself.

The Rise of Streaming Services: How They Are Changing the Film Industry

Ben Bradley, https://www.starburstmagazine.com/features/the-rise-of-streaming-services-how-they-are-changing-the-film-industry/

In recent years, the film industry has experienced a seismic transformation, propelled by the meteoric rise of streaming services. Platforms like Netflix, Amazon Prime Video, Disney+, and HBO Max have revolutionized how audiences engage with movies and TV shows. This revolution extends far beyond mere convenience, reshaping the entire landscape of film production, distribution, and audience interaction.

From altering viewing habits to redefining cinematic storytelling, streaming services are not just changing the game—they're rewriting the rules of the film industry as we know it. Join us on a

The Evolution of Content Consumption

On-Demand Viewing

One of the most significant changes that streaming services brings is the shift to on-demand viewing. Unlike traditional TV schedules or cinema release dates, streaming services allow viewers to watch content whenever they want. This flexibility has made it easier for audiences to fit movies and TV shows into their busy schedules, increasing overall viewership.

Binge-Watching Culture

Streaming services have also popularized binge-watching, where viewers consume multiple episodes or movies in one sitting. This new way of watching has influenced how content is produced, with many series now designed to keep viewers hooked for hours at a time.

Impact on Movie Theaters

Decline in Theater Attendance

The convenience of streaming services has led to a decline in theater attendance. While blockbuster films still draw large crowds, many viewers prefer the comfort of their own homes. This trend was accelerated by the COVID-19 pandemic, which forced many theaters to close temporarily and pushed more viewers toward streaming.

Hybrid Release Models

In response to these changes, some studios have adopted hybrid release models, where films are released simultaneously in theaters and on streaming platforms.

This approach aims to maximize audience reach and cater to different viewing preferences. If you want to know about the best Bitcoin poker sites, check out the detailed reviews and recommendations at Hudson Reporter. This dual-release strategy reflects a broader shift in the industry towards embracing digital platforms and catering to the diverse needs of modern audiences.

Changes in Film Production

Increased Investment in Original Content

Streaming giants have invested heavily in original content to differentiate themselves from competitors. Netflix, for example, spends billions of dollars yearly on original movies and series. This influx of funding has created more opportunities for filmmakers and resulted in a diverse range of content.

(Continued on next page)

(Continued from previous page)

Diversity and Inclusion

Additionally, streaming services have encouraged inclusion and diversity in the film business. They frequently take chances on endeavors that might not appeal to traditional studios, which results in the telling of a greater range of stories. As a result, underrepresented communities now have a voice, and the film industry has become more diverse.

New Opportunities for Filmmakers

Accessibility and Exposure

Streaming services have made it easier for independent filmmakers to get their work seen. Unlike the traditional film distribution model, which relies heavily on securing theatrical releases, streaming platforms offer a more accessible route to audiences worldwide. This has democratized the industry, allowing more voices to be heard.

Data-Driven Decisions

Streaming services use data analytics to identify trends and audience preferences. Thanks to their data-driven methodology, they can approve projects that have a better chance of success. Filmmakers can increase the likelihood that their movies will be picked up by using this information to customize their material to audience demands.

Shifting Marketing Strategies

Direct-to-Consumer Advertising

With the rise of streaming services, marketing strategies have shifted towards direct-to-consumer advertising. Platforms like Netflix and Amazon Prime Video can promote new releases directly to their subscribers through personalized recommendations and targeted ads. This approach is more efficient and cost-effective than traditional marketing methods.

Social Media Influence

Social media has become a powerful tool for promoting streaming content. Platforms like Twitter, Instagram, and TikTok allow studios and filmmakers to engage directly with audiences, creating buzz around new releases. User-generated content, such as reviews and fan theories, also plays a significant role in marketing and audience engagement.

The Future of the Film Industry

Continued Growth of Streaming Services

The popularity of streaming services shows no signs of slowing down. We can expect even more innovative features and improved user experiences as technology advances. Virtual reality (VR) and augmented reality (AR) are potential game-changers that could further revolutionize how we consume content.

Challenges and Adaptations

The traditional film industry faces several challenges as it adapts to this new landscape. Movie theaters must find ways to entice audiences back, perhaps by offering unique viewing experiences that cannot be replicated at home. Studios will have to balance between theatrical releases and streaming to maximize profitability.

Conclusion

The rise of streaming services has undeniably changed the film industry in numerous ways. From altering how we consume content to impacting film production and marketing strategies, these platforms have reshaped the landscape.

While challenges remain, the opportunities created by streaming services offer a promising future for filmmakers and audiences alike. As we move forward, the film industry will continue to evolve, driven by technological advancements and changing viewer preferences.

19 iPhone texting tricks that most people don't know

https://plandothrive.com/blog/27-iphone-texting-tricks/

These iPhone texting tricks are a mix of super-useful features that will help you communicate efficiently, get rid of some of those annoying problems with texting, and get things done. Plus, I've mixed in some fun! I learned a lot while compiling this list and am excited to use these tips in my day-to-day texting.

1. Mark messages as unread
2. Edit a sent message
3. Unsend a sent message
4. Schedule a text to send later
5. Reply to a specific message in a thread
6. Tag someone by name in a group message
7. Turn off notifications for unknown senders
8. Forward messages
9. Pin a conversation to the top of your list
10. Customize group messages with names, adding people, and removing people\
11. Mute a conversation
12. Use text search filters
13. Check in when you arrive to your destination
14. Share and view locations
15. Send messages via satellite
16. Bulk read, unread, or delete messages with a swipe
17. Format texts with bold, italic, strikethrough, and animated text effects
18. Customize your pinned apps within iMessage
19. Play games in iMessage

How Modern Browsers Keep You Safe (Without Telling You)

https://www.howtogeek.com/how-modern-browsers-keep-you-safe-without-telling-you/

On occasion, you might have seen a red warning from your internet browser when it blocks access to a potentially harmful website. Blocks like those are only one of the many, many security measures modern browsers have in place to keep you safe online.

Browsers Block Malicious Websites Before They Load

In the early days of the internet, browsers like Netscape Navigator and Internet Explorer only had minimal, if any, security features. That's why the spread of malware and phishing scams were way more common back in the day.

Today's browsers make the internet a much safer place than it once was. Google keeps a constantly updated database of malicious URLs by scanning every site it can access. This feature is called Google Safe Browsing.

Firefox, Brave, Chrome, Safari, and others use this database to warn you when you're trying to access one of those blacklisted URLs. Microsoft maintains its own version of this database called Defender SmartScreen, which Microsoft Edge relies on.

The database and the scans run locally on the device, and the browsers automatically fetch and update their local lists multiple times in an hour. Before loading a URL, the browser checks it against the huge list of unsafe URLs, and only loads the website if it's safe.

Google is constantly scanning billions of URLs for phishing sites (fake clones of real websites designed to steal your sensitive information). Machine learning algorithms look for signs of shady design and behavior in real-time and flag suspicious websites.

They Sandbox Tabs

"Sandboxing" an app lets it run in a secure environment where it can't affect the user space or the network. If you suspect an app has malware, you could test it inside a virtual machine. An isolated virtual machine would become a sandbox where the app can't access or infect the actual system.

Modern browsers do something similar with tabs. Every new tab you open runs in its own restricted sandbox. Each of these sandboxes is contained with strict restrictions and permissions.

That's why you can adjust cookies and other site permissions individually for every site you visit. You have to manually grant access when a site wants to access your location or camera, for example.

Even if one tab is exposed to malware, it's confined to that tab only. The sandboxing doesn't let it spread across other tabs or your local files on the system.

Before browsers adopted this sandboxing architecture, all tabs and extensions ran as a single whole process. If one tab was infected, it would crash the entire browser, and even compromise your entire system.

They Automatically Patch Vulnerabilities

Internet browsers update far more often than other types of software, even though you rarely ever see the browser update itself. At most, you'll get a prompt to restart the browser after a new update has been installed. That's because browser updates happen in the background, every two or four weeks.

Major updates that come with new features or upgrades are rolled out every month, but in between these major updates, browsers frequently get security patches.

The reason browsers need so many security patches is that vulnerabilities in these apps are constantly popping up. For example, you can find thousands of open bug reports for Chromium (the browser that powers Brave, Chrome, Edge, and others) on Chromium's issue tracker page. . The Mozilla Security page tracks the security fixes pushed for vulnerabilities in Firefox.

But why do browsers have so many vulnerabilities and bugs in the first place? The answer isn't developer error (although that is the culprit sometimes); it's because browsers are incredibly complex.

Browsers have to run code in a lot of different languages and not just render web content but provide a bunch of additional features like password managers and extensions. They're basically tiny operating systems with millions of lines of code, including third-party APIs. Bugs and vulnerabilities are basically inevitable.

In the early days of the internet, browsers had to be updated with a physical medium, like a floppy disk or CD. The companies themselves didn't push fixes for security vulnerabilities all that often. Modern browsers are far safer because of the automatic updates I mentioned and advanced bug bounty programs.

Your Connections Are Auto-Upgraded to HTTPS

There was a time when most of the data sent over the internet wasn't encrypted at any point. Anyone with access to your network could "sniff" your internet data packets. They would not only know which websites you visited, but also

(Continued on next page)

(Continued from previous page)

what you were doing on the website.

While it's now largely phased out, the Hyper Text Transfer Protocol or HTTP is how your browser and servers used to talk to each other. Your browser would send an HTTP request to get a file from a server, for example. The HTTP request was just a bunch of text specifying exactly what the browser was looking for. Then the server would respond with the content your browser requested—HTML code, image files, text or whatever.

Since neither step was encrypted, an attacker could intercept exactly what you're requesting and what the server is sending back, including sensitive info like login credentials. They could even tamper with what the server sent back.

Hyper Text Transfer Protocol Secure or HTTPS fixed that vulnerability. The request and response between the site and the browser are now encrypted and kept private. If a URL starts with https://, and you see a lock icon next to the loaded URL, it means the established connection is secure.

With HTTPs, no one can snoop on the data packets in transit, even if they are connected to the same network. The most they can see is which websites you're visiting, but not the data being sent back and forth

Even though HTTP is now being phased out and HTTPS is almost everywhere, you might end up clicking an old HTTP link at some point. Modern browsers are built to "prefer" HTTPS connections so they automatically redirect the URL to HTTPS. If the HTTPS alternative isn't available and the browser has to fall back on HTTP, it warns you that the connection is unsafe.

Those are only some of the ways modern browsers keep us safe online. There are even more defense systems always active in the background, and by choosing the right browser, you can make your online activity more secure than it already is.

For the complete article , graphics and recommendations of software please go to the website above.

How Your Smartphone Tracks Your Every Move—And How to Fight Back

https://www.howtogeek.com/how-your-smartphone-tracks-your-every-moveand-how-to-fight-back

We live in an era where the lines between our physical and digital lives are increasingly blurred. Smartphones are indispensable companions, seamlessly integrating into nearly every facet of our daily existence. However, that comes with a significant trade-off in the form of location tracking. Many of us operate under the assumption that we control our digital footprint, especially when it comes to our whereabouts, but that's not very accurate.

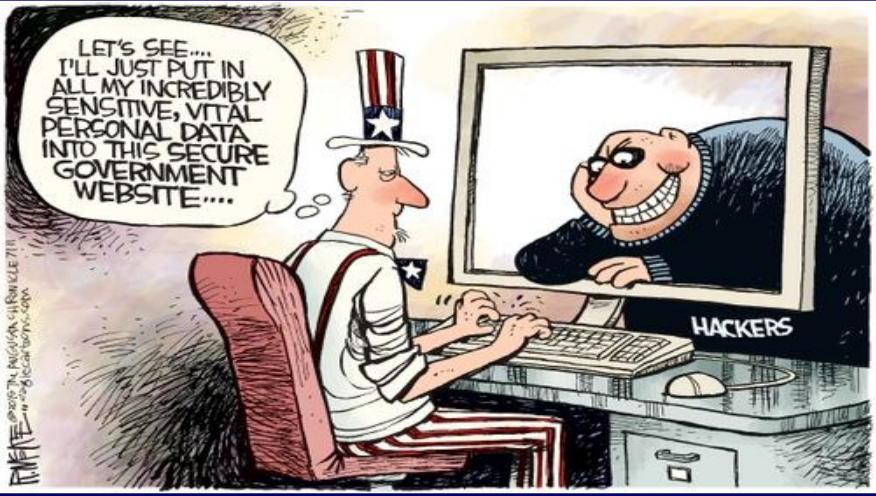
Understanding the underlying processes of how you are tracked is the first step toward reclaiming some semblance of control over your personal data. More importantly, you should be equipped with practical knowledge and actionable steps to fight back and improve your digital privacy effectively.

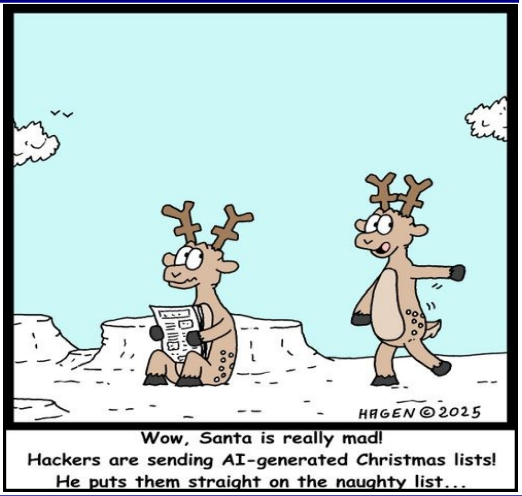
The Invisible Grid of Cell Tower Triangulation

The truth about owning a smartphone is that your location is constantly being broadcast, and it's completely tied to how the mobile network actually works. Cell Tower Triangulation is essentially a network-based method used to figure out where your mobile phone is. Unlike location tracking that comes from the apps on your device, this technique is non-intrusive and happens through the service provider's core infrastructure.

To successfully route your calls and data, cell towers have to listen for a signal from your device and constantly figure out which tower is the best one to communicate with. Your phone is always negotiating this connection, which basically means it's sending out a steady stream of "pings" to the network. Even when your phone is powered on but idle, it's sending out a signal just to keep in touch with nearby antenna towers, so service works.

For the remainder of this article please go to the website.





BROWSER NO 227

DECEMBER 2025

If unclaimed please return to PO Box 1109, Busselton. WA. 6280.

Postage paid

in Busselton

WA 6280