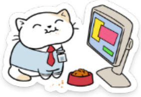
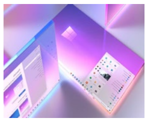
# Club Bytes



Brought to you by the Lake Gaston Computer Club

## Word of the Month

"SMTH"  It's not really a word or an acronym. It's a contracted version of something.  It's similar to other contractions, like "SRSLY" and "NVM," which mean "seriously" and "never mind," respectively.



## Windows 10 Sun Valley Update ditches Windows 95 icons for Modern versions

By **Mayank Parmar**

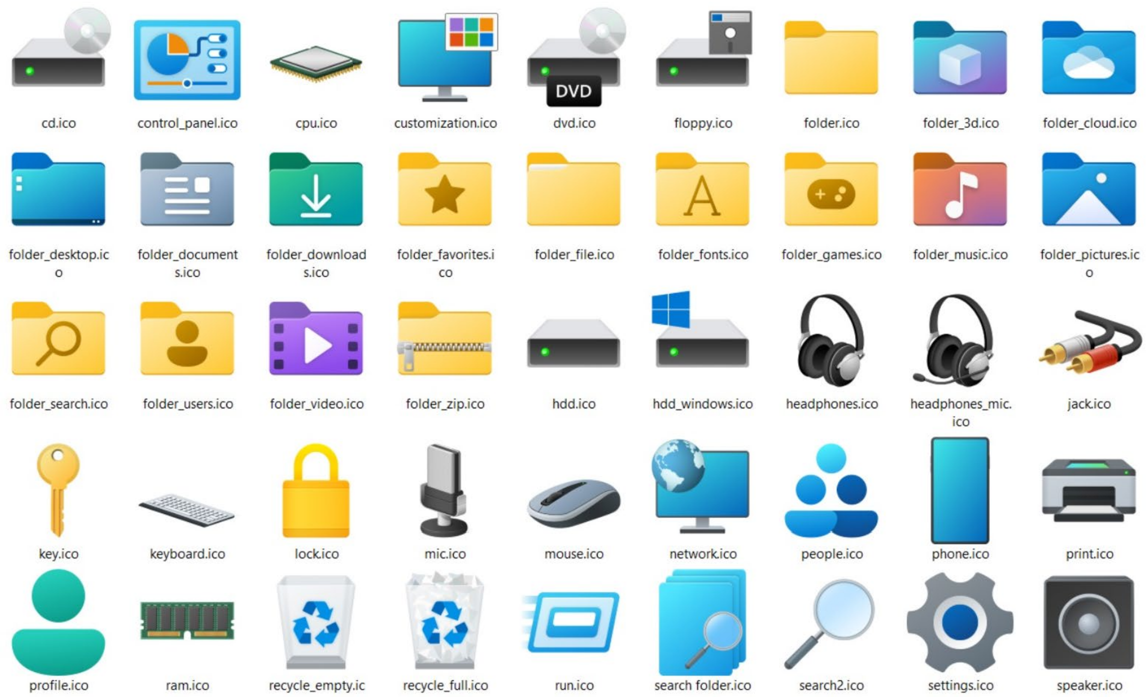
For those of you who like to play around with the icons, your wishes will come true with the new modern versions.

Later this year, Microsoft is planning to deliver a "sweeping visual rejuvenation" with Project Sun Valley, giving testers in the Insider program an early look at changes that will be introduced on Windows 10.

Windows 10's big interface refresh is codenamed "Sun Valley" and it's reportedly coming in October/November, with reports suggesting that the feature update will hit the RTM (release to manufacture) status in June. In the latest preview builds, we've now caught a glimpse of new icons for features from Windows 95-era.

Here is a glimpse at some of the new icons.

Microsoft is using different colours (rather than yellow and blue look) and these changes are in line with Fluent Design.



The icons for Recycle, Windows Run, Settings, and even floppy disk have been modified with a have a touch of Fluent Design.

## How to Create an Automatic Outline in Microsoft Excel

Excel has some automatic grouping and outlining features in their software. Math was never my best subject, so I got lost in this explanation, but for those of you who are wizards in Excel and understand this stuff it looks like a really great feature. Take a look. Ctrl + Click to follow the article. https://www.howtogeek.com/724558/how-to-create-an-automatic-outline-in-microsoft-excel/ Ctrl + Click to follow the article.

## How to Take a Screenshot on iPad

**BENJ EDWARDS** @BENJEDWARDS
MAY 6, 2021, 8:00 AM EDT | 2 MIN READ

Taking a screenshot on an iPad is as easy as pressing two buttons at once on your device—or you can use an alternative onscreen method. Here's how to do it.
Ctrl + Click to follow the Article.
https://www.howtogeek.com/724508/how-to-take-a-screenshot-on-ipad/

## How to Opt out of Google FLoC in Chrome

**JOHN BOGNA** @JBOGNA

You ask what in the world is FLoC? It is the Federated Learning of Cohorts which is supposed to take the place of cookies, or maybe not. Read the article to find out what is really going on and see if you need to change your settings. Ctrl + Click to Follow the article.
https://www.howtogeek.com/724783/how-to-opt-out-of-google-floc-in-chrome/

## How to Make Firefox Tabs Open at the End of the Tabs List

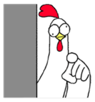
**BENJ EDWARDS** @BENJEDWARDS APR 28, 2021, 9:00 AM EDT | 1 MIN READ

Since I don't use Firefox, I didn't know the tabs don't open at the end of the tabs list anymore. I guess It was a new feature once upon a time that changed life as we used to know it. However, if you want to have it back, read this article. Ctrl + Click to follow the article.
https://www.howtogeek.com/719839/how-to-make-firefox-tabs-open-at-the-end-of-the-tabs-list/

## The Problem With Passwords is People

**DAVE MCKAY** @thegurkha APR 28, 2021, 8:00 AM EDT | 6 min read.

The only thing I can tell you is after reading this article is if you have a password of 123456 on any PC, Phone, Printer, Extender, or router you need to change it. Ctrl + Click to follow the article. https://www.cloudsavvyit.com/10819/the-problem-with-passwords-is-people/



## Your 6 Strongest Practical Password Techniques, Ranked

Password approaches, from best to worst, with examples:

1. Long with random characters: SBH2F%b^xDCUQf5frqBR
2. Long with multiple random words: *drying karen ruth afoot sauce*
3. Medium-length words with padding: *-*-*breakfast pancakes*-*_*
4. Medium-length words with random characters: l)ws7.BOZ1
5. Shorter with padding: *4*iforgot*4*
6. Shorter with random characters: (8dQ,]a

Regardless, use different passwords on every site and use a password vault to track them all.

To view the AskLeo video, copy and paste this link into your browser: https://www.youtube.com/watch?v=V7wlUTEeKb0

## How to Update Mozilla Firefox

**BENJ EDWARDS** @BENJEDWARDS
MAR 23, 2020, 8:30 AM EDT | 1 MIN READ

Keeping your browser updated is essential for internet security. Mozilla regularly updates Firefox to cover any emerging threats. Updates are free, so here's how you can install them and stay safe. Ctrl + Click to follow the article. https://www.howtogeek.com/661458/how-to-update-mozilla-firefox/

## Special Interest User Groups

The club has two groups that are back in the swing of things since Covid disrupted us last year: Genealogy and Apple User Groups. Check out the club calendar on the website https://www.lakegastoncc.org/ for days and times.

There has also been some interest in forming some more groups, i.e., Investment and Quicken/Quick Books. If you are interested, please let me know. Or if you have any other "SIG's" you think you would like to have, please think about it, and let me know. communications@lakegstoncc.org
Thank you.

## How to Update Your Amazon Kindle **HARRY GUINNESS**

Amazon regularly updates the Kindle software with bug fixes, improvements, and even new features like book-cover screensavers. Here's how to make sure that yours is always up to date.
Ctrl + Click to follow link.
https://www.howtogeek.com/725610/how-to-update-your-amazon-kindle/

## How to Add an Image to a PDF with Preview on Mac

MAHESH MAKVANA The Preview app on the Mac doesn’t make it easy to add an image to a PDF file, but there’s a clever workaround you can use with Preview itself, and we’ll show you how to do it.

Ctrl + Click to follow link.

https://www.howtogeek.com/722971/how-to-add-an-image-to-a-pdf-with-preview-on-mac/

## How to Use Multiple Page Orientations at Once in Google Docs SANDY WRITTENHOUSE

When you’re creating a document that could benefit from both portrait and landscape page orientations, consider Google Docs. You can mix both views throughout your document for the perfect format. Elements like tables, charts, graphs, and even images can often look better in landscape view. Luckily, a feature to switch page orientations in a single document was added to Google Docs.

Ctrl + Click to follow the link.

https://www.howtogeek.com/726950/how-to-use-multiple-page-orientations-at-once-in-google-docs/

## What Is Satellite Internet? FERGUS O'SULLIVAN @FERGUSOSULLIVAN

Satellite internet is known for being slow and expensive. Traditionally, it was used by people in remote rural areas and at sea. Let’s take a look at the problems associated with satellite internet—as well as

how several players, like Elon Musk's Starlink, are working on solving its problems.
Ctrl + Click to follow article.
https://www.howtogeek.com/728452/what-is-satellite-internet/

## What is SpaceX and Starlink?

SpaceX was founded in 2002 by Elon Musk with the goal of reducing space transportation costs to enable the colonization of Mars. SpaceX manufactures the Falcon 9 and Falcon Heavy launch vehicles, several rocket engines, Dragon cargo, crew spacecraft and Starlink communications satellites.
https://www.spacex.com/

Starlink currently is a project in Beta production by an American private company named SpaceX. It is a collection of satellites that organize in a proper formation which may be called mega Constellation.  They will eventually include 30,000 satellites orbiting the earth at 328 miles. Look up in the sky at night and you can see them flying like a train over Lake Gaston.  Sometimes you can see the satellite launch streak up from Cape Canaveral as the rocket heads this way.
https://www.spacex.com/
https://www.youtube.com/watch?v=GambrByc01A
https://findstarlink.com/

## Tips from the Repair Shop

Did you know that Windows Defender has ransomware protection features?  If you answered no, you're not alone.  Unfortunately, the setting to protect your personal files is "turned off" by default.  Malwarebytes Premium (not the free version) and antivirus software packages like Norton 360 provide ransomware protection

so no change to the Defender default setting is needed with secondary software. If Windows Defender is your active antivirus protection, then you should consider enabling "Controlled folder access" within Defender. Once enabled, Defender prevents ransomware from encrypting your data and protects files from malicious apps trying to make unwanted changes. Click on the YouTube link below for instructions on how to make this setting change.
Ctrl + Click to follow the link.
https://www.youtube.com/watch?v=HbcqLUPEeqE

**VS**

## Microsoft Office vs. Microsoft 365: Which One Should You Buy?

To read the full How-to-Geek article, copy and paste this link into your browser: https://www.reviewgeek.com/72454/microsoft-office-vs-microsoft-365-which-one-should-you-buy/

Microsoft Word, Excel, and PowerPoint are the standard productivity applications for most businesses and classrooms. But how do you choose between the traditional Office suite and the Microsoft 365 subscription service? What's the difference between Office and Microsoft 365, and which is more cost-effective?

Table of Contents of the full article:

- What's the Difference?
- Microsoft Office: Pros and Cons
  - Buy It Once, Own It Forever
  - Microsoft Office vs. Office Online
- Microsoft 365: Pros and Cons
  - Work From Anywhere
  - Collaboration to the Max

    - The Latest Features and Support
    - Membership Bonuses
- Okay, So Which One Costs More?

## What's the Difference?

Everyone's familiar with the old Microsoft Office ritual. You buy a disc full of Word, PowerPoint, and other Microsoft-branded software, stick it in your computer, and get to work. A few years go by, and your job or classroom requires a newer version of the Office suite, so you go out and blow your savings on another disc. Rinse and repeat.

But the traditional Office bundle is a lot less common than it used to be. Today, many people access Excel, Word, and other software through a Microsoft 365 subscription or the free, browser-based Office Online suite (which is a stripped-down version of Office).

Unlike an Office bundle, which requires a one-time payment of $150 and only works on one computer, Microsoft 365 costs $7 a month, works on all of your computers and mobile devices, and includes collaborative features and perks that don't come with a standard Office bundle. Microsoft launched its 365 service in 2011 to help modernize the Office suite, which hadn't experienced a major overhaul in nearly a decade. The subscription model allows Microsoft to offer constant updates and support for its productivity software, along the with the cloud storage and deep collaborative features made famous by Google's browser-based productivity tools (Google Docs, Drive, Sheets, etc.).

Microsoft still sells its traditional Office suite for people who don't want to pay a monthly fee or use the free, stripped-down Office Online tools. But is the Office bundle really that cost-effective? And even if you can save some money by avoiding Microsoft 365, is it worth missing out on the subscription services' exclusive features?

## Dell computers found to have “severe” system flaws that compromise security.

Dell has repaired the vulnerabilities, but **customers need to install the patch.**

Security researchers have discovered that Dell has been pushing a firmware update for the last 12 years that contains “five high severity flaws.” Experts at Sentinel LABS say those flaws impact hundreds of millions of Dell desktops, laptops, notebooks, and tablets.

Although the vulnerabilities could allow hackers to exploit Dell computers and do further damage, Sentinel LABS says it has not discovered evidence of any “in-the-wild abuse.”

As for owners of non-Dell computers, there’s good news: this specific vulnerability affects only Dell-specific systems.

### Dell steps up to fix the issue

Even though Sentinel LABS hasn’t uncovered any widespread abuse, Dell isn’t taking any chances. Just to make sure nothing goes wrong, the company has sent a security update to its customers to address the exposure. It recommends that every Dell computer owner apply the patch as soon as possible.  Dell warns owners that a hacker could use phishing techniques to gain access to their computer if it is left unpatched. “To help protect yourself from malicious actors, never agree to give remote control to your computer to any unsolicited contact (such as from an email or phone call) to fix an issue,” the company advises.

Sentinel Labs also says customers should not waste time installing the patch. “It is inevitable that attackers will seek out those that do not take the appropriate action. Our reason for publishing this research is to not only help our customers but also the community to understand the risk and to take action” said Sentinel LABS’ Kasif Dekel.

## How to Get Wi-Fi on the Road

JOHN BOGNA @JBOGNA

Staying connected when traveling can be tricky if you're not in a hotel, but it's possible. Whether you're on a cross-country road trip or going camping, or even if you just need some Wi-Fi on a long drive, there are ways to stay connected while you're on the road.

### Use Your Smartphone's Hotspot Function

Probably the most straightforward solution, your smartphone's hotspot mode can be a lifesaver when it comes to staying connected on the road.

Android and iPhone both make this easy to do, creating a secure local network complete with a password. This method lets you connect other devices (like a laptop, for example) to the network if you have to send a few emails—or if you just want to stream shows on a bigger screen.

Make sure that you're familiar with the limits of your wireless contract before going this route. If you have an unlimited data plan, you'll likely avoid any charges from increased data usage. If you don't, know how long your data will last and plan accordingly. To save power and megabytes, download entertainment to your phone or hard drive before you leave.

Also, check to see whether hotspot data is transmitted at the same speed as your phone. Even if you have a 5G device, your carrier might restrict hotspot (also called "tethered") data to something slower, like 3G.

If you're going this route, you'll definitely need a car charger and/or a power pack to keep your phone's battery life up. Hotspot mode burns through power pretty quickly on most phones.

### Bring a Mobile Hotspot

You can create a similar network to a cellular hotspot with a dedicated mobile hotspot device. It's basically just a router, so you can't browse on one, but it still works if you're using something like a lightweight laptop as your main device and don't have a hotspot-capable phone.

The price for one of these devices can be anywhere from $100 to over $200, and some of them require a monthly service fee. They usually plug into a USB port and can come with an internal battery, making the network that they create more portable.

You'll want to look for something that fits your budget and provides:

- fast data speeds
- a flexible plan
- multiple Wi-Fi options
- good battery life
- a portable form factor.

Portable hotspots can also be great when you're traveling internationally, as they help you avoid massive data roaming charges and might provide faster speeds than the local internet can. Your wireless service provider will likely have one that you can buy but be sure to shop around to find the best deal.

**Use an OBD-II Device**

These devices are different from a typical mobile hotspot in that they don't connect via USB. Instead, they plug into your car's OBD-II port—the same one that mechanics use to connect a diagnostic tool.

That means that you won't be able to get far from your car when you're using this device's network. But if you're only planning to use it in route to the campsite or hotel, it shouldn't be an issue.

Since it plugs into the diagnostic port on your car, an OBD-II device can actually broadcast diagnostic information to an app on your smartphone. In addition to a local wireless network, you also get metrics like vehicle-tracking data.

One of these will run you anywhere from $50 to $200, depending on how advanced the device is and what kind of contract you get with it. AT&T, T-Mobile, and Verizon all offer these devices with data plans. Contracts are around $20 and up, usually paid per month.

**Find a Public Wi-Fi Connection**

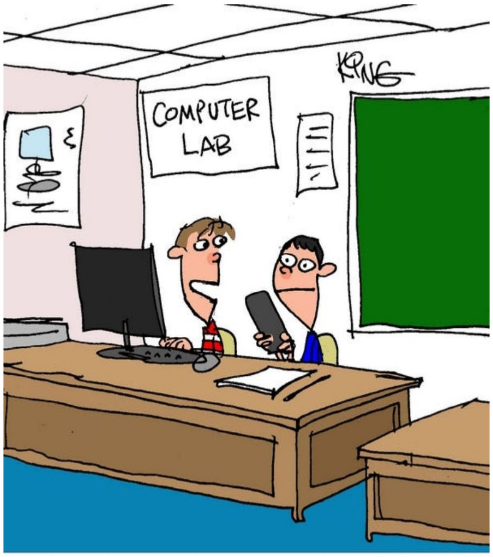
If none of these is an option or you don't have service, there's always the old standby of public Wi-Fi hotspots. McDonald's, Starbucks, and even big box stores like Target all usually have public

Wi-Fi that you can use in a pinch—often while sitting in the parking lot.

If you're unsure of where to find free Wi-Fi near you, apps like NetSpot and Wi-Fi Map offer databases of public hotspots. Even Facebook's app can help you find the closest free network.

If you have to use a public connection, be as safe as possible with your data. Use a VPN if you have one and avoid entering sensitive information or payment details on any websites that you visit.

*"My fitness app just sent me a message. It says it just added another 40 hours of treadmill time this week to offset this one meal."*



*"The jocks bullied me in gym class, so I erased all the data on their computers. They should know to never mess with a computer geek."*

## Apple Tidbits' Paul Bernard

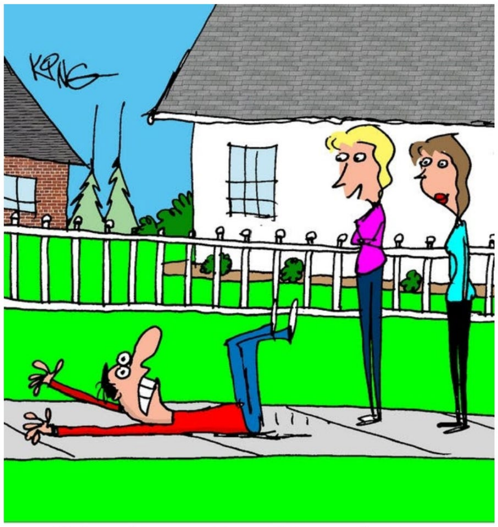
Apple has started making devices with their own chips again. The 8 core M1 chip uses memory which is designed to serve both large chunks of data and do it very quickly. This removes the need to have two different types of memory and all the copying of data between them making it faster. It also does this with incredibly low power consumption. The new iPad Pro, the new 24" iMac, the Mac

Mini, the MacBook Air, and the MacBook Pro are all available with the M1 chip.

The new 24-inch iMac is a great new addition to Apple's line of products. It come in various colors with matching accessories, and it starts at only $1299. That may look like a lot, but it is much lower than the 27 inch. The MacBook Air is Apples thinner and lightest notebook, completely transformed by the M1 chip. CPU speed up to 3.5x faster and GPU speeds up to 5x faster and has great battery life. The MacBook Air starts at $999. The new MacMini, also uses the M1 chip, is even smaller in size with much improved speeds and capability. It starts at $699. The 4K Apple TV is also out.

The WWDC, World Wide Developers Conference, starts June 7th at which we should learn more about what Apple will be coming out with this fall. It's always interesting to see what new developments in computer technology is coming our way.

***The Apple SIG is starting back up this coming Thursday the 3rd at the classroom at 9am in the shop at the Littleton Towne Center. If you are interested in learning more about your Apple devices, we will try to help you with any of its products from iPhone, iPad to Mac.***



*"I love his smart watch's new feature. It drags him to the gym."*

*"Then it is true. There is a little demon who steals phones, my mouse and my AirPods."*

## 5 awesome apps are hiding on your iPhone right now, and you had no idea **Yoni Heisler** Mon, May 31, 2021

Lurking behind the scenes on the iPhone are a handful of hidden apps that you probably had no idea existed. And while you might be inclined to believe that any app Apple doesn't make conspicuous probably lacks any meaningful utility, that couldn't be further from the truth. Ctrl + Click to follow the link.
https://www.yahoo.com/entertainment/5-awesome-apps-hiding-iphone-130049996.html
iPhone Updates
https://www.techradar.com/news/ios-147-release-date-and-all-the-iphone-features-we-know-about-so-far
M1chip: what it does for the systems
https://www.techradar.com/news/apple-event-april-2021-live-blog

## What Is End-to-End Encryption, and Why Does It Matter? **CHRIS HOFFMAN** @CHRISBHOFFMAN

I included this article to help explain how individuals can pass messages through electronic messaging systems. We use these systems to protect ourselves in our everyday transactional life. Some individuals use them to plan others to violently disrupt everyday life throughout the world on the internet and the dark web. Legal authorities have difficulties tracking them and you may understand why after reading this article.
Nancy Nicholson

**End-to-end encryption** (E2EE) ensures that your data is encrypted (kept secret) until it reaches an intended recipient. Whether you're talking about end-to-end encrypted messaging, email, file storage, or anything else, this ensures that no one in the middle can see your private data.

In other words: If a chat app offers end-to-end encryption, for example, only you and the person you're chatting with will be able to read the contents of your messages. In this scenario, not even the company operating the chat app can see what you're saying.

## Encryption Basics

First, let's start with the basics of encryption. Encryption is a way of scrambling (encrypting) data so that it can't be read by everyone. Only the people who can unscramble (decrypt) the information can see its contents. If someone doesn't have the decryption key, they won't be able to unscramble the data and view the information. (This is how it's supposed to work, of course. Some encryption systems have security flaws and other weaknesses.) Your devices are using various forms of encryption all the time. For example, when you access your online banking website—or any website using HTTPS, which is most websites these days—the communications between you and that website are encrypted so that your network operator, internet service provider, and anyone else snooping on your traffic can't see your banking password and financial details.

Wi-Fi uses encryption, too. That's why your neighbors can't see everything you're doing on your Wi-Fi network—assuming that you use a modern Wi-Fi security standard that hasn't been cracked, anyway. Encryption is also used to secure your data. Modern devices like iPhones, Android phones, iPads, Macs, Chromebooks, and Linux systems (but not all Windows PCs) store their data on your local devices in encrypted form. It's decrypted after you sign in with your PIN or password.

### Encryption "in Transit" and "at Rest": Who Holds the Keys?

So, encryption is everywhere, and that's great. But when you're talking about communicating privately or storing data securely, the question is: Who holds the keys? For example, let's think about your Google account. Is your Google data—your Gmail emails, Google Calendar events, Google Drive files, search history, and other data—secured with encryption? Well, yes. In some ways.

Google uses encryption to secure data "in transit." When you access your Gmail account, for example, Google connects via secure HTTPS. This ensures that no one else can snoop on the communication going on between your device and Google's servers. Your internet service provider, network operator, people within range of your Wi-Fi network, and any other devices between you and Google's servers can't see the contents of your emails or intercept your Google account password.

Google also uses encryption to secure data "at rest." Before the data is saved to disk on Google's servers, it is encrypted. Even if someone pulls off a heist, sneaking into Google's data center and stealing some hard drives, they wouldn't be able to read the data on those drives. Both encryption in transit and at rest are important, of course. They're good for security and privacy. It's much better than sending and storing the data unencrypted! But here's the question: Who holds the key that can decrypt this data? The answer is Google. Google holds the keys.

**Why It Matters Who Holds the Keys**

Since Google holds the keys, this means that Google is capable of seeing your data—emails, documents, files, calendar events, and everything else. If a rogue Google employee wanted to snoop on your data—and yes, it's happened—encryption wouldn't stop them. If a hacker somehow compromised Google's systems and private keys (admittedly a tall order), they would be able to read everyone's data. If Google were required to turn over data to a government, Google would be able to access your data and hand it over.

Other systems may protect your data, of course. Google says that it has implemented better protections against rogue engineers accessing data. Google is clearly serious about keeping its systems secure from hackers. Google has even been pushing back on data requests in Hong Kong, for example. So yes, those systems may protect your data. But that's not *encryption* protecting your data from Google. It's just Google's policies protecting your data. Don't get the impression that this is all about Google. It's not—not at all. Even Apple, so beloved for its privacy stances, does not end-to-end encrypt iCloud backups. In other words: Apple keeps keys that it can use to decrypt everything you upload in an iCloud backup.

### How End-to-End Encryption Works

Now, let’s talk chat apps. For example: Facebook Messenger. When you contact someone on Facebook Messenger, the messages are encrypted in transit between you and Facebook, and between Facebook and the other person. The stored message log is encrypted at rest by Facebook before it’s stored on Facebook’s servers.  But Facebook has a key. Facebook itself can see the contents of your messages.

The solution is end-to-end encryption. With end-to-end encryption, the provider in the middle—whoever you replace Google or Facebook with, in these examples—will not be able to see the contents of your messages. They do not hold a key that unlocks your private data. Only you and the person you’re communicating with hold the key to access that data. Your messages are truly private, and only you and the people you’re talking to can see them—not the company in the middle.

### Why It Matters

End-to-end encryption offers much more privacy. For example, when you have a conversation over an end-to-end encrypted chat service like Signal, you know that only you and the person you’re talking to can view the contents of your communications.  However, when you have a conversation over a messaging app that isn’t end-to-end encrypted—like Facebook Messenger—you know that the company sitting in the middle of the conversation can see the contents of your communications.  It’s not just about chat apps. For example, email can be end-to-end encrypted, but it requires configuring PGP encryption or using a service with that built in, like ProtonMail. Very few people use end-to-end encrypted email. End-to-end encryption gives you confidence when communicating about and storing sensitive information, whether it’s financial details, medical conditions, business documents, legal proceedings, or just intimate personal conversations you don’t want anyone else having access to.

### End-to-End Encryption Isn’t Just About Communications

End-to-end encryption was traditionally a term used to describe secure communications between different people. However, the term is also commonly applied to other services where only you hold the key that can decrypt your data.

For example, password managers like 1Password, BitWarden, LastPass, and Dashlane are end-to-end encrypted. The company can't rummage through your password vault—your passwords are secured with a secret only you know. In a sense, this is arguably "end-to-end" encryption—except that you're on both ends. No one else—not even the company that makes the password manager—holds a key that lets them decrypt your private data. You can use the password manager without giving the password manager company's employees access to all your online banking passwords.

Another good example: If a file storage service is end-to-end encrypted, that means that the file storage provider can't see the contents of your files. If you want to store or sync sensitive files with a cloud service—for example, tax returns that have your social security number and other sensitive details—encrypted file storage services are a more secure way to do that than just dumping them in a traditional cloud storage service like Dropbox, Google Drive, or Microsoft OneDrive.

**One Downside: Don't Forget Your Password!**

There's one big downside with end-to-end encryption for the average person: If you lose your decryption key, you lose access to your data. Some services may offer recovery keys that you can store, but if you forget your password and lose those recovery keys, you can no longer decrypt your data.  That's one big reason that companies like Apple, for example, might not want to end-to-end encrypt iCloud backups. Since Apple holds the encryption key, it can let you reset your password and give you access to your data again. This is a consequence of the fact that Apple holds the encryption key and can, from a technical perspective, do whatever it likes with your data. If Apple didn't hold the encryption key for you, you wouldn't be able to recover your data.

Imagine if, every time someone forgets a password to one of their accounts, their data in that account would be wiped out and become inaccessible. Forget your Gmail password? Google would have to erase all your Gmails to give you your account back. That's what would happen if end-to-end encryption were used everywhere.

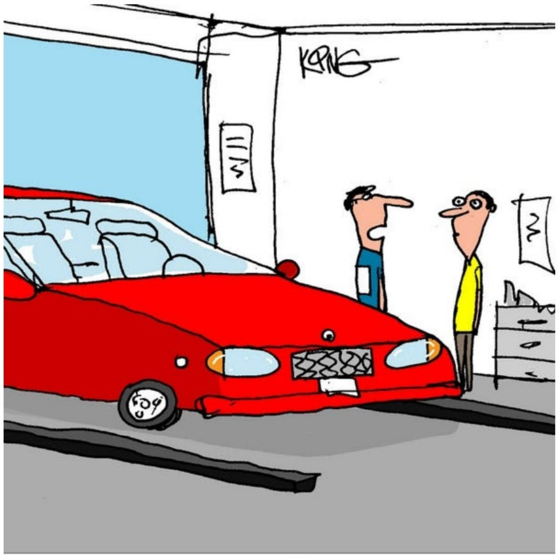
**Examples of Services That Are End-to-End Encrypted**

Here are some basic communication services that offer end-to-end encryption. This isn't an exhaustive list—it's just a short introduction. For chat apps, Signal offers end-to-end encryption for everyone by default. Apple iMessage offers end-to-end encryption, but Apple gets a copy of your messages with the default iCloud backup settings. WhatsApp says that every conversation is end-to-end encrypted, but it does share a lot of data with Facebook. Some other apps offer end-to-end encryption as an optional feature that you have to enable manually, including Telegram and Facebook Messenger.

For end-to-end encrypted email, you can use PGP—however, it's complicated to set up. Thunderbird now has integrated PGP support. There are encrypted email services like ProtonMail and Tutanota that store your emails on their servers with encryption and make it possible to send encrypted emails more easily. For example, if one ProtonMail user emails another ProtonMail user, the message is automatically sent encrypted so that no one else can see its contents. However, if a ProtonMail user emails someone using a different service, they'll need to set up PGP to use encryption. (Note that encrypted email doesn't encrypt everything: While the message body is encrypted, for example, subject lines aren't.)

*"I'm sorry, sir, but we can't help you stop butt dialing people. You may try locking your phone when not using it."*

*"I set your ringtone to the sound of snoring. I want you to experience what I go through each night."*



*"I found the problem. The reason your car wouldn't move is because someone hit the pause button on it."*

KING
Landfill

*"I'm sorry I accidentally threw the USB flash drive away. If we go through the trash, we can find it. It should only take a few years."*

*"My computer's sucking me back to my seat. Unplug it!"*

*"I built a ball out of all of our old computer cords for the dog to play with. We had a lot."*