Club Bytes 

Brought to you by the Lake Gaston Computer Club

Word of the Month

What Does "JSYK" Mean, and How Do You Use It? It is one of many internet initialisms that we have become exposed to. There are many more such as FYI, TBH, BRB, TIL, and YEET.

JSYK: Just So You Know
FYI: For Your Information
TBH: To Be Honest
BRB: Bath Room Break
TIL: Today I Learned
YEET: Forceful Word

It is quite interesting, if you have spare time, to see how they came to be.

https://www.howtogeek.com/714759/what-does-jsyk-mean-and-how-do-you-use-it/
https://www.howtogeek.com/447760/what-does-tbh-mean-and-how-do-you-use-it/
https://www.howtogeek.com/436783/what-does-yeet-mean-and-how-do-you-use-it/

How to Add Private Labels in Google Maps

Google Maps offers various recommendations for travelers, including important landmarks to nearby businesses. If you want to save your own recommendations to Google Maps to quickly find in the future, you can do so by adding private labels. Here's how. Read More »

How to Enable Do Not Disturb During Workouts on Apple Watch

If you're in the middle of a hard run or chill yoga session, you probably don't want your phone to ring (unless it's really important). By automatically enabling Do Not Disturb on your Apple Watch when you start a workout, you can make sure you don't get interrupted. Here's how. https://www.howtogeek.com/711255/how-to-enable-do-not-disturb-during-workouts-on-apple-watch/

How to Stop Annoying Website Notification Pop-Ups in Edge

Microsoft Edge is a great web browser when it comes to speed and features. But website notification pop-ups can spoil your browsing experience and clutter your notifications. Microsoft Edge for Desktop (Windows 10 and Mac) and Android both have a built-in notification system for websites (It's not available on iPhone and iPad.). Here's how to stop annoying website notification pop-ups in Microsoft Edge.https://www.howtogeek.com/714111/how-to-stop-annoying-website-notification-pop-ups-in-edge/

How to Turn off "OK Google" on Your Android Phone or Tablet

The "OK Google" and "Hey Google" commands can be handy for hands-free tasks, but you might not want to use them. If you'd like to stop your Android device from listening for these Google Assistant hot words, it's easy to do. Read More » https://www.howtogeek.com/718100/how-to-turn-off-ok-google-on-your-android-device-2/

 How to Remove a Year from a Date in Microsoft Excel

There are a couple of ways you can remove the year from a date shown in Microsoft Excel. You can use custom cell formatting to hide it or use various functions like CONCATENATE to remove it completely. Here's how. Read More » https://www.howtogeek.com/714809/how-to-remove-a-year-from-a-date-in-microsoft-excel/

 What Is the Chrome "Reading List," and How Do You Use It?

There's so much great content being written on the internet that it's hard to find the time to read it all. Google Chrome's "Reading List" feature can help you save things for later, so you never miss something good. Read More » https://www.howtogeek.com/719357/what-is-the-chrome-reading-list-and-how-to-use-it/

 How to Turn off Save Password Pop-ups in Microsoft Edge  KHAMOSH PATHA

Microsoft Edge has a built-in password manager that offers to save all your passwords. When you log in to a new website, Edge will prompt you to save the login details. But this can get quite annoying. Here's how to disable the pop-ups in Microsoft Edge. https://www.howtogeek.com/715508/how-turn-off-save-password-pop-ups-in-microsoft-edge/

How to Turn Off Annoying "Save Password" Pop-Ups in Chrome KHAMOSH PATHAK

Google Chrome comes with a built-in password manager that helps you save and sync all your website logins. But if you use a dedicated password manager, the insistent "Save Password" prompts in Chrome can be annoying. Here's how to disable them.

https://www.howtogeek.com/715496/how-to-turn-off-annoying-save-password-pop-ups-in-chrome/

How to Read Kindle Books on Your Computer or a Website

Left your Kindle reader behind? Not a problem—you can still read your e-books on a nice big screen, without losing out on features like notes, bookmarks, and highlights. Here's how to read Kindle books on any Windows 10 PC, Mac, or desktop web browser.
https://www.howtogeek.com/715760/how-to-read-kindle-books-on-your-computer-or-a-website/

How to Clear Your Queue on Spotify BEN STOCKTON

If you fancy creating a one-time-only playlist of some of your favorite songs on Spotify, you can add them to your playing queue. If you don't like your choices, however, you can clear your queue in seconds. Here's how. https://www.howtogeek.com/714084/how-to-clear-your-queue-on-spotify/

How to Create a Geographical Map Chart in Microsoft Excel SANDY WRITTENHOUSE

Charts are helpful for visual displays of your data. They can make viewing and analyzing data easier, especially for your audience. So,

for geographical data, why not use the map chart type in Microsoft Excel?
https://www.howtogeek.com/713632/how-to-create-a-geographical-map-chart-in-microsoft-excel/

Avoid Online Tax Scams Gus Best

Tis the season, income tax time.

Both Virginia and North Carolina have extended their State & Federal tax filing dates this year to May 17th.

That is good for the people that need the extra time, and it is good for the scam artists. The enormous amounts of valuable personal and financial information shared online during this time of year make it a haven for thieves – and they will do everything they can to take full advantage of the opportunity this extended tax season brings them.

Here are four ways cybercriminals try to take advantage of taxpayers during tax season:

1. **IRS impersonation scams:** Callers claiming to be IRS employees might call and insist that you owe money and that it must be paid as soon as possible via gift card or wire service. If the call isn't picked up, they leave an emergency callback message. *The IRS will never call you to demand immediate payment or call asking for personal or bank account information.*
2. **Marked increase in phishing, email, malware, and phone schemes:** Watch for unsolicited emails, texts, social media posts, fake websites or phone calls that may prompt you to click a link or share personal and financial information.
3. **Fraudulent tax returns:** File your tax return as soon as possible. The IRS only accepts one tax return per Social Security number. If you file early, it becomes impossible for a fraudster to submit another return with your personal information.

4. **Tax preparer fraud:** The overwhelming majority of tax preparers provide honest services, but some unsavory individuals might target unsuspecting taxpayers, and the result can be refund fraud and/or identity theft. The IRS reminds anyone filing a tax return that their preparer must sign it with their IRS preparer identification number.

How Often Should I Reboot My Computer?

To view the AskLeo video, copy and paste this link into your browser: **https://youtu.be/VjM7SUQSYVI**

by Leo A. Notenboom "Ask Leo"

There's no hard-and-fast rule; it really depends on how you use your computer.

If you spend your entire day running only one program, there may not be a need to reboot it periodically at all. For example, if all you do is run your web browser to visit websites — including, perhaps, your email — then, while you might want to close and reopen the browser every so often (usually because it seems to be acting up), there's just no need to reboot the computer.

On the other hand, if you're running lots of different programs, opening, and closing them often, or just using the machine heavily, the answer might be different.

On the third hand, you may be running a single program that's not well behaved, and as a result, a reboot might be advised.

The rule that's the exception to the rule.

Reboot when asked.

Windows Update is a great example. Many times, the files to be updated are in use, and the only way to update them is during a reboot. The net result is that about once a month, you'll probably be informed that you should reboot your computer for updates to be applied. Or you'll find that Windows has simply rebooted for you.

It's also not uncommon for updates of other software to require a reboot to complete.

In either case, these reboot-forcing updates make the point moot. Update when they ask you to.

When I reboot

My computer is on all day, every day. I run *many* different things on it throughout the day.

It's a beefy machine, so performance isn't really an issue, so I also leave a lot of things running. As I type this, the Command Prompt "tasklist" command shows 413 processes running.[1]

Since I run so much, it's not uncommon for me to have to reboot for an update every so often.

If I don't, though, I find that about every other day or so it starts behaving … oddly. Something might be slow, the mouse might not be as responsive, or something just "ain't quite right".

I reboot, and all's well again.

Rebooting rule of thumb

Reboot when you need to.

That means either rebooting because an update needs it, or because you're experiencing a problem you think might be addressed by a reboot.

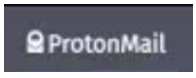
And of course, when you turn your computer off (without using Hibernate, or Sleep), you're also rebooting.

But in general, I wouldn't bother rebooting unless one of those situations comes up.

What Is Secure Email, and Should You Switch?

There has been a lot of discussion about secure mail since "ProtonMail" and "Tutanota" have become available. So, I thought I should have some articles about the issue. I can't imagine that anyone in our club would be concerned about a national security risk with their email but there are people who do in large businesses, Newspapers, and in government. I always felt if it were in an email anyone could have access to it so, be careful what you say. Read this article and see if you think you need secure email.

https://www.howtogeek.com/710380/what-is-secure-email-and-should-you-switch/



What Is ProtonMail, and Why Is It More Private Than Gmail?

TIM BROOKES

ProtonMail is a secure email service designed to protect your inbox and identity. So how exactly is ProtonMail different from a "regular" email provider like Gmail? And, more importantly: Is it time to make the switch?

While all major email services claim to respect your privacy, ProtonMail goes further than most in a bid to protect you. That's what makes it different from the big email providers like Google's Gmail and Microsoft's Outlook.com.

ProtonMail is one of a handful of so-called secure email providers that shun the traditional webmail route of plentiful free storage and integrated services in favor of heightened privacy and

security features. Unlike with Gmail, you'll have to pay to unlock many of these additional bells and whistles. Google profits off its free Gmail service by showing you ads, while ProtonMail doesn't have any ads.

Google and Microsoft use standard good security practices like two-factor authentication and securing the connection between your browser and their servers. ProtonMail goes further still by not logging identifying information, storing data on the server in a manner that's useless to third parties, and better facilitating private conversations between users.

While ProtonMail sounds like an upgrade over Gmail, it does come with some caveats. The free plan is limited—for example, it only offers 500 MB of storage. Many of the features that make Gmail so useful aren't possible in ProtonMail due to the emphasis on privacy and security. For example, it won't automatically crawl through your email and add events to your calendar.

Deciding between a traditional provider like Google and a secure provider like ProtonMail is a case of weighing up convenience and privacy. If you want an email service with all the conveniences of Gmail, ProtonMail isn't it.

ProtonMail Prioritizes Data Protection and Secure Messaging

ProtonMail encrypts all data on the server so that it is rendered useless to anyone without the key to decrypt it. In the case of a security breach, data swiped from ProtonMail's servers wouldn't be of any use. Not even ProtonMail can read your email.

This isn't the case with standard webmail providers like Gmail, which only encrypts data between your browser and its servers. Google will use AI to "read" your email for services like the Google Assistant to make useful suggestions at opportune moments. Gmail can tell what you're doing and when you're doing it based on the contents of your inbox, and that's become a feature that many users rely upon.

In addition to providing encryption on the server, ProtonMail also makes it easy to send encrypted messages between users. All communications between ProtonMail users are automatically end-to-end encrypted so that not even ProtonMail's employees can read them. ProtonMail also facilitates the use of Pretty Good Privacy,

or PGP, which allows you to "lock" email contents so that only recipients with the key can open them.

ProtonMail even allows you to send password-protected, self-destructing messages to users of any webmail platform. In essence, this is a bit of a trick, since the recipient must click on a link to open the message, but it works well enough, and it's not something that Gmail or Outlook provides. Using PGP inside of Gmail is possible but difficult, with browser extensions like Mailvelope and FlowCrypt making it easier to manage. Unlike with ProtonMail, which explicitly supports the feature, working with PGP inside of Gmail is much less streamlined and borderline unusable on mobile.

ProtonMail's Servers Are Located in Switzerland

In addition to not being able to read the email stored on their servers, ProtonMail is based in Switzerland, where privacy laws are notoriously strict. This means that ProtonMail can't be forced to hand over data to authorities in the U.S. Switzerland is not part of the Five Eyes intelligence-sharing agreement that exists between the U.S., Canada, Australia, the United Kingdom, and New Zealand.

By comparison, Google is located in the U.S. and may be forced by law to turn over information on its users. (And in the U.S., emails are considered "abandoned" after 180 days, so the government can request them without a warrant.) This includes inbox contents, metadata, IP addresses, and more. This information can then be shared with other members of the Five Eyes allegiance.

Because Google stores data in an unencrypted format on their servers, you don't need decryption keys to make use of it. The entire contents of your inbox could be handed over to authorities and used against you. If Google experiences a data breach and user data is leaked, there's no safety net in place to prevent that data from being used.

In the case of Gmail, identifying information like your IP address, real name, cell phone number, and locations from which you have logged in are all stored alongside the contents of your inbox.

ProtonMail Knows Very Little About You

ProtonMail doesn't require that you provide any identifying information to create an account. You only need to supply a

username (the email address you will be using) and a password. You can link a recovery email if you want, but you don't have to. On top of this, ProtonMail logs extraordinarily little about its users. No IP addresses are stored, and tracking is not used to follow users from one site to the next. Metadata is discarded so that it's harder to link an email to a point of origin. ProtonMail attempts to make you as anonymous as possible, though you should never assume complete anonymity online

Google is the web's largest advertising company. It's responsible for a huge amount of the tracking that takes place across the web. Tools like Google Analytics help website owners monitor traffic, while Google's advertising arm monitors your web usage to provide "relevant" advertising that you're more likely to click on.

Google also runs many other popular services. Tracking users removes the need to keep logging in when moving from Google Maps to YouTube or from Gmail to Google Drive.

ProtonMail is open source, too. You can hop on GitHub and download the code for the ProtonMail webmail application. You can deploy it on your own server if you know how—or simply comb through the codebase looking for bugs or potential security flaws. ProtonMail also uses well-established open-source cryptography techniques including AES, RSA, and OpenPGP.

Having an open-source codebase has two main benefits. The first is that the code can be audited by anyone. ProtonMail states that they do not include backdoor access for law enforcement or security agencies to use. Don't believe it? Download the source code and have a look for yourself.

The other upside to open-source code is that anyone can try and break ProtonMail's security. This "crowdsourced" approach to security exposes any potential weaknesses in a way that closed-source applications do not. Google also uses open-source technologies, but the Gmail codebase is ultimately closed.
This is a link that compares ProtonMail and Tutanota.

https://www.howtogeek.com/718159/protonmail-vs.-tutanota-which-is-the-best-secure-email-provider/

IP PINs for Everyone: How This IRS Security Tool Could Help Protect You From Identity Theft

Written by a Norton LifeLock employee Feb. 13, 2021.

Ever try to file a tax return online with the IRS only to find your efforts blocked, with the IRS saying that someone with your same Social Security number and name already filed? You might be the victim of tax-related identity theft.

In this type of identity theft, someone uses your stolen personal information, including your Social Security number, to file a tax return in your name. The goal of these criminals? To claim your tax refund.

The IRS has now given taxpayers a new tool to help prevent tax-related identity theft: an Identity Protection Personal Identification Number, better known as an IP PIN. And the best news? This tool is now available to all taxpayers, not just people who have previously been victims of identity theft.

What is an IP PIN?

Starting in 2021, the IRS is making IP PINs available for all taxpayers. In the past, only taxpayers who had been victims of identity theft were eligible for this tool.

IP PINs are designed to make it more difficult for thieves to file false tax returns in the names of other taxpayers. These PINs are unique six-digit numbers. When you file your return with an IP PIN, it provides the IRS with additional information to verify your identity.

Identity thieves, then, would need to know not just your Social Security number, but your IP PIN, too.

IP PINs are only temporary. Each taxpayer's IP PIN lasts for a year. The following year, taxpayers will have to sign up for a new IP PIN that they will use when filing that year's income tax returns.

How to get your IP PIN

Getting an IP PIN is an easy process, but you won't be able to start the process until the middle of January. That's because the online portal offered by the IRS to get one of these numbers was down for maintenance at the start of 2021. The IRS says the tool will be online again starting in the middle of January.

Starting then, you can log onto the Get an IPN tool offered by the IRS. You will have to verify your identity. This means that you'll have to register an online account with IRS.gov, a process that the IRS says takes about 15 minutes.

To register, you'll need to provide your email address, Social Security Number or Individual Tax Identification Number, tax filing status, mailing address, and one financial account number linked to your name.

This can be the last eight digits of your credit card, as long as it's not an American Express, debit, or corporate card; the account number listed on your student loan statement; the account number on your mortgage or home equity loan; account number of your Home Equity Line of Credit; or the account number of your auto loan.

You will also need to provide a mobile phone number linked to your name so that the IRS can send you an activation code. If you can't provide this, the IRS will send your activation code to you by mail.

If you are a confirmed victim of identity theft, the IRS will mail you a CP01A Notice with a new IP PIN each year. This process will be automatic.

Your IP PIN will be valid for one calendar year, so you'll need to obtain a new one each year if you want to remain in the program. The IRS says that its Get an IP PIN online tool is usually unavailable from the middle of November through the middle of January each year.

How to request an IP PIN offline

If you can't register for an IP PIN online, you can ask for one through the mail, though there are limits. If your income is $72,000 or less, you

can file IRS Form 15227 , Application for an Identity Protection Personal Identification Number.
To do this, you'll need a Social Security number or Individual Taxpayer Identification Number, an adjusted gross income of $72,000 or less and access to a telephone.

You can also make an appointment for an in-person meeting at your nearest Taxpayer Assistance Center. You'll need one picture identification document and another identification document to prove your identity.

The IRS will, after verifying your identity, send you your IP PIN through the mail within three weeks.

What to do if you are a victim of tax-related identity theft

As the IRS says, tax-related identity theft occurs when an individual uses your personal information — including your Social Security number — to file a tax return in your name. The fraudsters behind this scam hope to snag whatever refund you had coming.

If you suspect that you have been the victim of tax-related identity theft, you should continue to pay your taxes and file your tax return. You might have to file a paper return even if you'd prefer to file electronically.

But how do you know if you've been victimized by this form of identity theft? First, you won't be able to file your tax returns electronically. That's because someone else has already filed a return in your name using your information. When you try to file, you'll get a message from the IRS that your name and Social Security number have already been used to file a return.

Other signs you have been a victim of tax-related identity theft.

There are other signs, though. You might get a letter from the IRS asking about a suspicious tax return that you did not file, or you might receive a tax transcript in the mail that you did not request.

You might also receive a notice from the IRS saying that an online account has been created in your name or that your existing online account with the agency has been accessed or disabled.

If you get any of these notices, respond to them immediately. Call the number provided on the notice. Ignoring these notices won't make the problem go away. Calling the IRS quickly, though, could mitigate any damage from the identity theft.

If you try to e-file your tax return and it is rejected because of a duplicate filing, complete IRS Form 14039, Identity Theft Affidavit. Fill out the form at IRS.gov, print it, attach the form to your paper tax return and mail that and your return to the IRS according to the instructions on the form.

You can also request a copy of your fraudulent tax return from the IRS. For more information about this, visit the IRS' page on dealing with fraudulent returns. You should also visit IdentityTheft.gov to learn more about the steps you should take to protect yourself and your finances from identity thieves.

zoom How to Look Better on Zoom (and Other Video-Calling Apps)

More professional and personal interactions are happening via Zoom and other video-calling apps, and it doesn't look like that'll be changing anytime soon. The same as an in-person meeting or date, it's important to look your best on video calls. Here's how to work it for your webcam.

Find Better Lighting

Raise Your Camera

Look at the Camera (and Dim Your Screen)

Test Your Internet Connection

Use Your Best Camera

To read the full article, copy and paste this link into your browser: **https://www.howtogeek.com/673264/how-to-look-better-on-zoom-and-other-video-calling-apps/**

FIDO

What is the FIDO Alliance and what does FIDO stand for?

The FIDO (fast identity online) Alliance is an industry association that aims to reduce reliance on passwords for security, complementing or replacing them with strong authentication based on public-key cryptography. To achieve that goal, the FIDO Alliance has developed a series of technical specifications that websites and other service providers can use to move away from password-based security. In particular, the FIDO specs allow service providers to take advantage of biometric and other hardware-based security measures, either from specialized hardware security gadgets or the biometric features built into most new smartphones and some PCs.

Public key cryptography is already the basis for most secured internet communication. The SSL/TLS standard is based on it and has been built into most web browsers for decades, and the larger set of technologies and specifications known as the public key infrastructure, or PKI, helps not only encrypt data but also ensure that communicating parties online are who they say they are. In almost every case today when you enter a password into a web browser, that password is being transmitted across the network in an encrypted form, thanks to PKI.

How to Fill Excel Cells Automatically with Flash Fill and Auto Fill **BRYAN CLARK**

I didn't know about flash fill but now I do it will save me a whole bunch of time. I hope it does the same for you. Thank you, Microsoft!

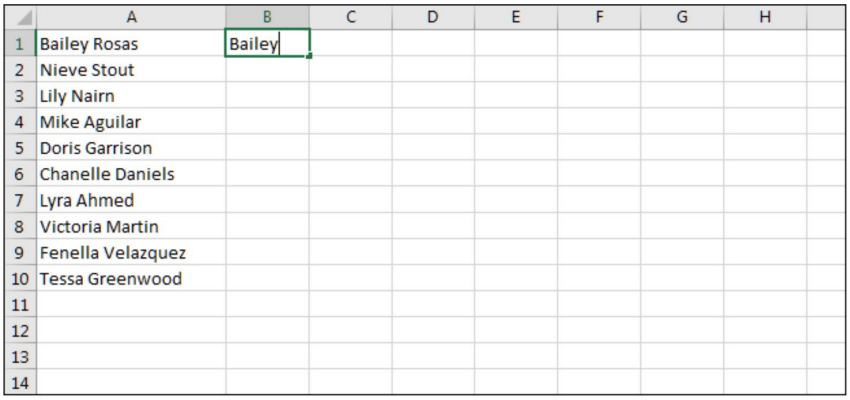
A lot of the tasks you'll complete in Microsoft Excel are tedious. Luckily, Excel has several features that make this kind of spreadsheet work bearable. We'll look at two of them: Flash Fill and Auto Fill.

How to Use Flash Fill in Excel

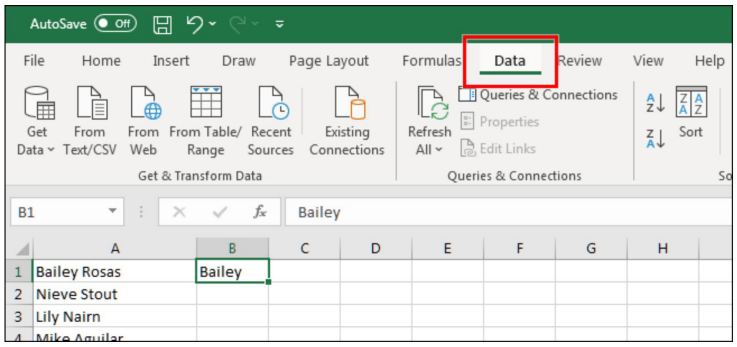
Flash Fill can automatically detect patterns in data and help you quickly fill cells.

For example, if we start with a list of full names (first and last), but then decide that we should have split them into separate columns, Flash Fill can automate a lot of the work.

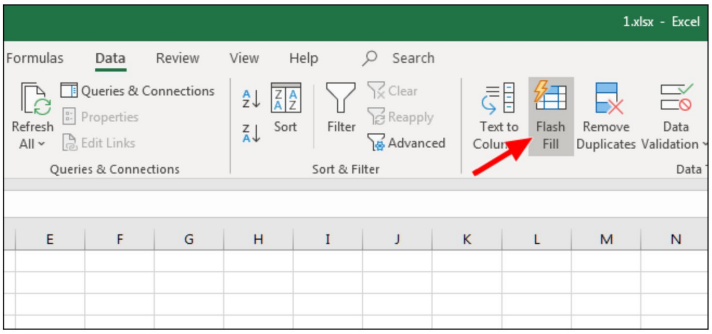
To start, let's assume that we have a list of names. In the column where you want the first names to go, type just the first name from the first cell.



Click the "Data" tab on the ribbon at the top of the Excel window.



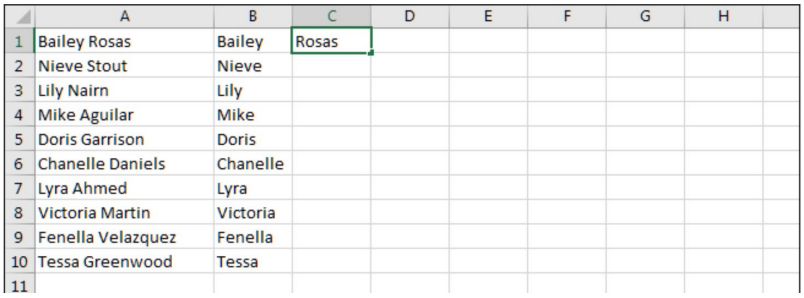
Then, click the “Flash Fill” button in the Data Tools section.



As you can see, Excel detected the pattern, and Flash Fill filled the rest of our cells in this column with only the first name.

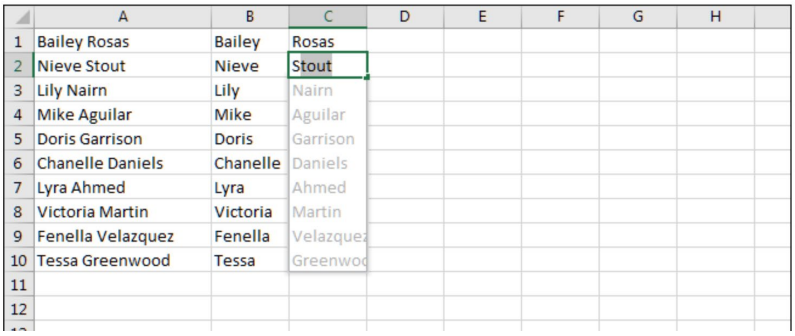
	A	B	C	D	E	F	G	H
1	Bailey Rosas	Bailey						
2	Nieve Stout	Nieve						
3	Lily Nairn	Lily						
4	Mike Aguilar	Mike						
5	Doris Garrison	Doris						
6	Chanelle Daniels	Chanelle						
7	Lyra Ahmed	Lyra						
8	Victoria Martin	Victoria						
9	Fenella Velazquez	Fenella						
10	Tessa Greenwood	Tessa						
11								

From here, now that Excel knows our pattern, it should show you a preview as you type. Try this: In the next cell over from where you typed in the first name, type in the corresponding last name.



	A	B	C	D	E	F	G	H
1	Bailey Rosas	Bailey	Rosas					
2	Nieve Stout	Nieve						
3	Lily Nairn	Lily						
4	Mike Aguilar	Mike						
5	Doris Garrison	Doris						
6	Chanelle Daniels	Chanelle						
7	Lyra Ahmed	Lyra						
8	Victoria Martin	Victoria						
9	Fenella Velazquez	Fenella						
10	Tessa Greenwood	Tessa						
11								

If we click "Enter" on the keyboard, which moves us to the cell below, Excel now shows all of the last names in their proper places.



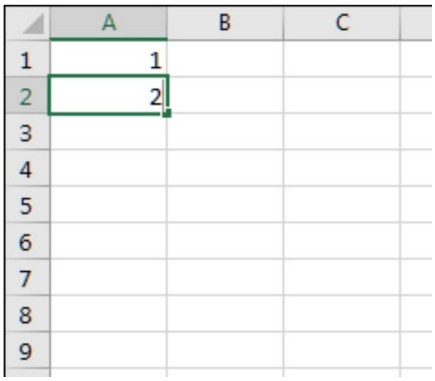
	A	B	C	D	E	F	G	H
1	Bailey Rosas	Bailey	Rosas					
2	Nieve Stout	Nieve	Stout					
3	Lily Nairn	Lily	Nairn					
4	Mike Aguilar	Mike	Aguilar					
5	Doris Garrison	Doris	Garrison					
6	Chanelle Daniels	Chanelle	Daniels					
7	Lyra Ahmed	Lyra	Ahmed					
8	Victoria Martin	Victoria	Martin					
9	Fenella Velazquez	Fenella	Velazquez					
10	Tessa Greenwood	Tessa	Greenwood					
11								
12								

Click "Enter" to accept, and Flash Fill will automatically complete the rest of the cells in this column.

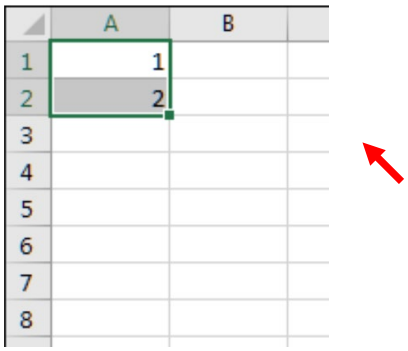
	A	B	C	D	E	F	G	H
1	Bailey Rosas	Bailey	Rosas					
2	Nieve Stout	Nieve	Stout					
3	Lily Nairn	Lily	Nairn					
4	Mike Aguilar	Mike	Aguilar					
5	Doris Garrison	Doris	Garrison					
6	Chanelle Daniels	Chanelle	Daniels					
7	Lyra Ahmed	Lyra	Ahmed					
8	Victoria Martin	Victoria	Martin					
9	Fenella Velazquez	Fenella	Velazquez					
10	Tessa Greenwood	Tessa	Greenwood					
11								
12								

How to Use Auto Fill in Excel

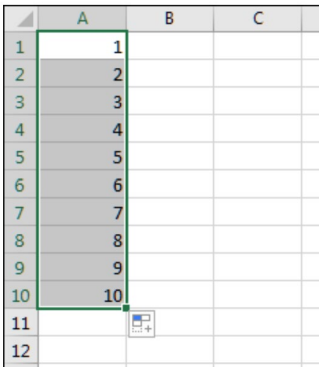
Auto Fill works a little like Flash Fill, although it's better suited for tasks that involve a lot of cells. It's also better for cells that have an even more obvious pattern, such as numbers, for example. To see how it works, let's type in a few numbers.



Type 1, Enter. Type 2, Enter



Find the square in the bottom right of the cell and drag it down. You can drag it as far as you'd like.



Excel recognized the pattern and filled all of the cells below that you told it to.

Just like in the previous example, if we click the box at the bottom right and drag it down, Excel will fill all of the cells below using the Auto Fill feature.

	A	B	C	D	E	F	G	H	I	J
1	1	January								
2	2	February								
3	3	March								
4	4	April								
5	5	May								
6	6	June								
7	7	July								
8	8	August								
9	9	September								
10	10	October								
11										
12										
13										
14										

Using Flash Fill and Auto Fill are two easy ways to automate your work in Excel, so long as it's an obvious pattern.

Although Excel sometimes surprises us with its ability to detect more complex patterns, it's not something that you can count on. Stick to easy stuff for the best, most consistent results.

Just a Few Giggles

"No, it's not a computer monitor. It's a doggy door. Not everything is technology related."

"I see you sitting at your computer. Now you are opening up your email. You see a strange email with an attachment. Don't open it! Oh no, what have you done?"

"This job requires the skill to work under extreme conditions. To test you, you'll be using a 20 year old computer. Not many pass this test."

"That news you're reading is 24 hours old. I can get it 23 hours and 57 minutes sooner online."

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

"You don't need to attach a magnifying glass above your smart watch. Just use the zoom."