Club Bytes

Brought to you by the Lake Gaston Computer Club

Word of the Month

VTuber   What Is a VTuber?

VTuber is a word blending the sounds and combining the meanings of two others. They are transforming online content creation by changing the way people look, sound, and act. Here's who VTubers are, and why they're so different from an average internet influencer such as an avatar.

https://www.howtogeek.com/720841/what-is-a-vtuber/

Notice:

Next LGCC Zoom Club Meeting:
May 11,2021, Tuesday at 1:00 pm

Subject: Sherry Herzing LKG 911 Community Task Force Update. Deployment of What3Words technology.

All members will receive an email on Monday, May 10, with instructions and a link to the meeting. Please join us.

We do record all our Zoom meetings. They are posted on the Club website under the Education Tab – Virtual Zoom Meetings.

The 5 Best Bluetooth Trackers

JOE FEDEWA

We all have had a problem keeping track of various items, people, pets, glasses, and even our cell phones. These blue tooth trackers can help with those problems. They are very handy but there are several models and each one has its fit. Take a look and see it any can solve a problem you may have.

https://www.howtogeek.com/724315/best-bluetooth-trackers/
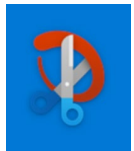
How to Annotate Screenshots with Windows 10's Snip & Sketch SAMIR MAKWANA

IF YOU HAVEN'T FOUND THIS EXCELLENT TOOL FOR SCEEN SHOTS YET, TAKE A LOOK AT THIS INFORMATION. YOU WILL BE GLAD YOU DID.

https://www.howtogeek.com/722790/how-to-annotate-screenshots-with-windows-10s-snip-sketch/

Having a Weird iPhone Problem? Reboot It! BENJ EDWARDS

We have all had those problems that make us wonder why we ever became involved with electronic devices that rule our world. Stranger Things happen on them and not just on the movie screen. Well you do still have "The Power". In previous days we called it "DeBoot". Now it's "ReBoot"! Read on my frustrated friends.

https://www.howtogeek.com/723487/having-a-weird-iphone-problem-reboot-it/

Can your home network be hacked? Christine McKenzie

The short answer? Yes, it's absolutely possible for your home network to get hacked. There are a couple of ways hackers can gain access to your network.

One common method is to guess the password. It sounds simple, but routers often come with a preset default password that the manufacturer uses for all devices. A hacker could easily look up the default password associated with a given type of router and use it to access countless devices.

Hackers can also exploit security flaws in the router's firmware. Since firmware is updated so infrequently, hackers have ample time to discover and exploit security flaws before they're patched. Infrequent firmware updates leave 83% of home Wi-Fi routers vulnerable to attack, according to a [study by The American Consumer Institute (ACI)](#).

Your home network is naturally vulnerable, which means the responsibility falls on you, the end user, to keep an eye out for signs of suspicious activity and figure out what to do if your network is hacked.

How do you know if your home network has been hacked?

The signs of a hacked home network can be subtle, but there are certain clues you should keep an eye out for. Here's how to detect hackers on your network:

Your network has an unusual spike in activity

When a hacker gets into your home network, they're free to piggyback off your bandwidth. This can lead to your internet connection becoming unusually slow.

Your firewalls have been mysteriously uninstalled

Your firewall is your network's first line of defense against would-be intruders. Certain types of malware can uninstall or disable your firewall, which make it easier for intruders to access your network in the future.

Your computer starts operating on its own

Seeing your cursor move around on its own can be spooky, but that doesn't mean there's a ghost in the machine. Instead, it means an intruder has gained remote access to your computer, and that's a lot scarier than a ghost!

Once a hacker has access to your computer, they also have access to all of your data, including sensitive documents, emails and images. They can also install new software on your computer and uninstall security measures like your antivirus and firewall.

Your web browser's default home page changes

If your default browser changes suddenly or redirects you to an unfamiliar page, then your home network has probably been hacked. Usually, this type of activity is caused by a browser redirect virus. Be especially careful with browser redirects, since attackers may send you to a spoof website where they will try to harvest personal or financial information.

You're asked to give access to a program

It's normal for legitimate programs to request access to our network from time to time, but if you notice an unknown program making that request, that's cause for alarm.

How to detect hackers on your network

Hackers like to use stealth to operate undetected for as long as possible. Fortunately, there are ways you can check to see if someone is hijacking your network.

The first thing you can do is check out what devices are connected to your network. You can do this right from your computer. All you have to do is type your router's IP address into your browser's URL bar. If you're unsure of the router's IP address, that's OK; it's usually printed right on the router.

Once you're logged in, you can take a look at what devices are associated with your network. Usually, this is located in a section called Device List or Attached Devices. Identifying devices is easy when they're named, like "Christine's Laptop," but keep in mind that some devices will only appear as their IP addresses. This will take a little more detective work to match up your device's IP addresses with the ones listed. If any of the IP addresses don't match up, that means they're being used by an intruder.

What to do if your network is hacked

If your network has been hacked, don't panic — there are steps you can take to mitigate the damage and shut out the hackers. Take a look at these steps for how to stop hackers in your home network.

Reset your router

When the VPNFilter malware gained infamy in 2018, the FBI recommended a router reboot as the best way to get rid of the virus. Every wireless router comes with a reset button that restores the router to its default settings. When you hit the reset button, it will disrupt anyone lurking in your network.

Keep in mind that resetting your router is not the same as power flushing it. When your router boots up after resetting it, be prepared to reconfigure your network settings.

Change your wireless network password

Your network should be protected by a strong, unique password. If your network isn't password-protected, you should add one immediately as an extra layer of protection. If your network was

password-protected prior to being hacked, you should reset the password to make it more difficult for intruders to re-establish access to your network.

Deactivate remote administration

Remote administration is a setting on your router that permits someone to access your system from a far-away location. While the setting can be useful in some legitimate scenarios, it can also be abused by hackers. There are red flags that a hacker has gained remote access to your computer, such as when your cursor moves on its own or programs seem to install themselves all on their own. Deactivating remote administration will no longer allow hackers to abuse that feature to access your network.

Run a virus scan on your devices

There are multiple ways to hack a home network, and one of them is via malware. Certain viruses, like a keylogger, record everything you type on your keyboard, including your usernames and passwords. Running a virus scan should detect and remove any malicious software lingering around on your computer.

Update your router's firmware

Routers are built with network security in mind, but that doesn't mean exploits and vulnerabilities are impossible. If a hacker exploited a vulnerability in the router's firmware to gain access to your network, then a software update could patch up the hole and secure your device.

Keep in mind that most routers don't automatically update firmware, so you'll have to do it manually when a security update becomes available. When it comes down to how to stop hackers, regularly updating your router's firmware is one of the best things you can do.

How to stop hackers from infiltrating your home network

Once an attacker gains access to your home network, they can do a lot of damage. That's why it's critical to prevent attackers from getting into your system in the first place. Here are some tips for home network protection.

Don't open any unusual links or attachments

Malware is often transmitted via infected files or links. When you click on the link or attachment, the virus will download and install itself on your device. Once installed, it can make changes to your network, like removing firewalls, enabling remote access and spying on your activities.

Run a reliable antivirus program

Keep in mind that antivirus software is not foolproof. It can only detect malware that it's programmed to recognize, so cutting-edge new viruses will most likely slip past its defenses undetected. You'll also need to keep up with updates as soon as they come out. This ensures your antivirus's library of known malware is as up-to-date as possible.

Update your software regularly

Updating your software goes beyond just antivirus. Router firmware updates are a critical part of securing the device. If the router manufacturer discovers the device is susceptible to attackers, then a security update will patch up the vulnerability and prevent future attackers from invading your network.

Keep your home network safe and secure

Thanks to ever-improving communication technology, more and more people are able to work from the comfort of their own homes. Unfortunately, hackers are taking advantage of home networks, which are typically less secure than corporate networks, to steal information and money. If you work from home, it benefits you to know how to detect hackers on your network and what to do if your network is hacked.

How to Take a Screenshot by Tapping the Back of Your iPhone BENJ EDWARDS

If you own an iPhone 8 or later running iOS 14 or later, you can now take a screenshot just by tapping its back thanks to a new accessibility feature called Back Tap, which you'll have to configure for the task. Here's how to set it up.

https://www.howtogeek.com/681816/how-to-launch-actions-by-tapping-on-the-back-of-your-iphone/

Here Are the 2021 Spring and Summer Meteor Showers (and Other Events) SUZANNE HUMPHRIES

Sometimes we just need fun things to do and get any from the techno geeky stuff. This article will take you to the star gazing fun of summertime. Get your gear if needed, spread a blanket, and just enjoy the time outside in the fresh air.

https://www.reviewgeek.com/75025/here-are-the-2021-spring-and-summer-meteor-showers-and-other-events/#htg=2085569

"I accidentally hit 3 keys and then hit enter. CTRL + Z didn't get rid of it. Can we keep it as a pet?"

What Is a No-Log VPN, and Why Is That Important for Privacy? FERGUS O'SULLIVAN

At our March Zoom Club Meeting, we briefly discussed VPN's and Incognito mode. I ran across this article for the geeks in the club who may want to know a bit more concerning these subjects and how they work or don't to keep your information secure/private.

One of the biggest promises VPN services make is that they don't keep logs. It's plastered across their websites and features prominently in their marketing material. But what are logs, exactly, and what makes for a "no-log" or "zero-log" VPN?
https://www.howtogeek.com/717096/what-is-a-no-log-vpn-and-why-is-that-important-for-privacy/

How to Subscribe to Podcasts on Spotify

How many of you have heard of Spotify? How many of you want something different to listen to rather than music? Want something stimulating? You can understand the words? The words stimulate thought? Humm. How do I get a podcast on Spotify?

https://www.howtogeek.com/717860/how-to-subscribe-to-podcasts-on-spotify/

"Our laptop is defective and heats up, so the kids are using it as their campfire."

How to Securely Shop Online: 8 Tips to Protect Yourself

Cybercrime is an epidemic. In the U.S. alone, nearly half a million complaints are filed about it each year, according to the FBI—and that's just what's reported. Here's how you can stay safe and avoid becoming a statistic.

- **Only Shop on Sites Using HTTPS**
- **Be Careful Who You Shop with**
- **Shop Online with Credit Cards If Possible**
- **Use Strong Passwords**
- **Use a VPN If Shopping in Public**
- **Watch out for "Too Good to Be True" Deals**
- **Know Your Rights and the Return Policies of the Site**
- **I've Been Hit by Cybercrime, Now What?**

For more information, Ctrl + Click to read more about what you should do. https://www.howtogeek.com/702286/how-to-securely-shop-online-8-tips-to-protect-yourself/

"We're cyber criminals, Barnes, NOT common criminals. Go get cleaned up and look like you're tech-savvy."
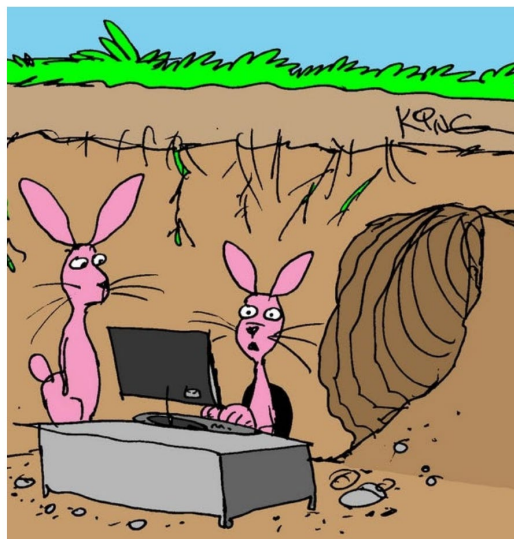
"We shouldn't have had so many kids. Now they all want computers and phones."
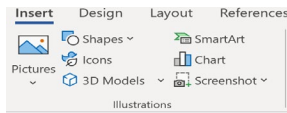
How to Insert an Image Inside of Text in Microsoft Word

You can fill text with a color, but the feature for filling text with an image was removed in Microsoft Word 2013. However, with a little workaround, you can still do this in Word for Microsoft 365. Here's how.

If you want to fill your text with an image in Word, you can't simply type the text and fill it like you could in Word 2010, or even in the latest version of PowerPoint. But you can fill the text of a SmartArt graphic with an image.

First, open the Word application. In the "Illustrations" group of the "Insert" tab, click "SmartArt."
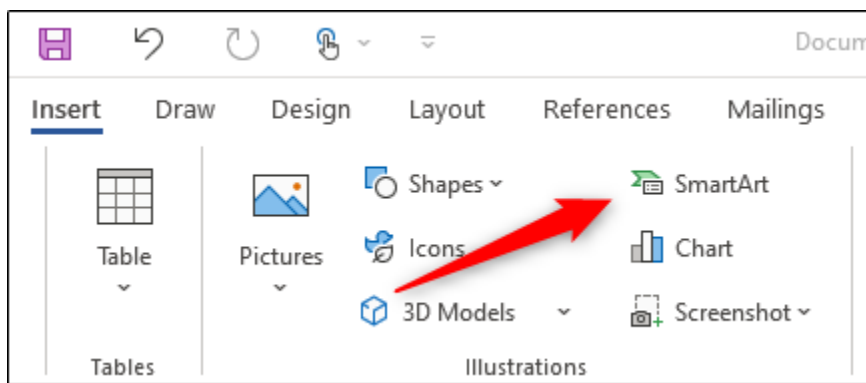
The "Choose a SmartArt Graphic" window will appear. In the left-hand pane, choose an option that provides a type of SmartArt graphic that you can type text within. We'll use "List" in this example.
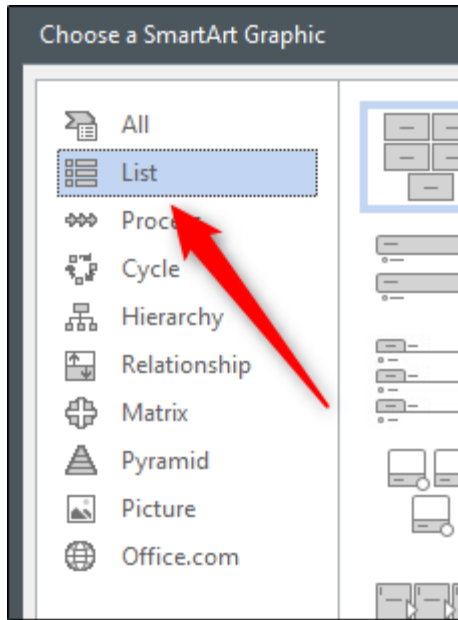
Next, choose the SmartArt graphic that you'd like to use from the available options within the selected tab. We'll use the "Basic Block List" SmartArt graphic. Once it's been selected, click "OK."
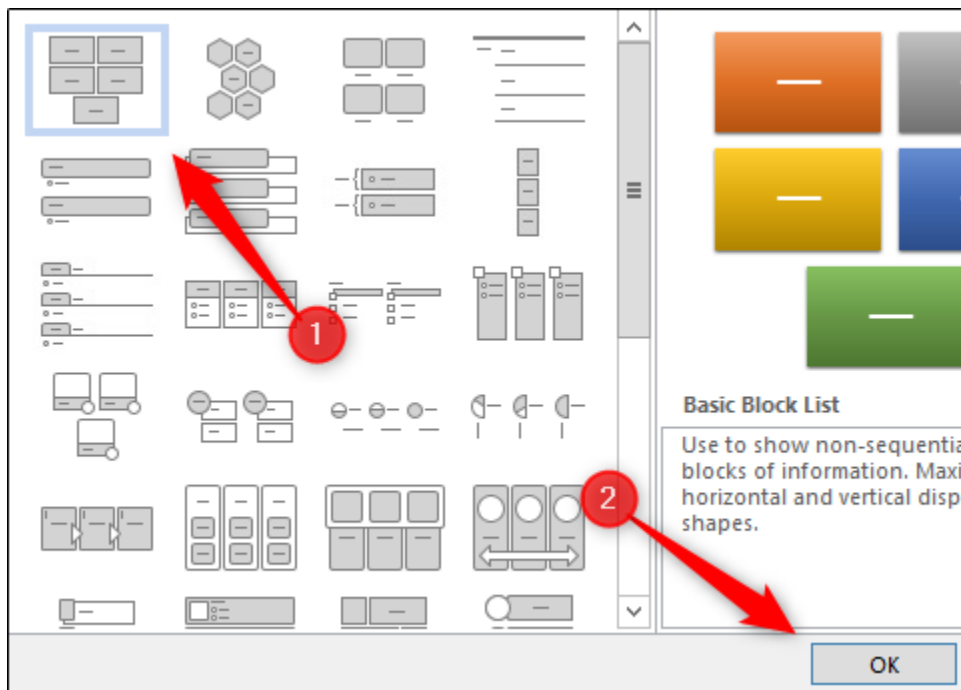
The SmartArt graphic will now appear in the Microsoft Word document. Now, delete all but one of the items within the graphic by clicking each item and pressing the Delete key.

Next, type the desired text in the remaining graphic.

To better see the image inserted in the text, format your text to be larger. You can do so in the "Font" group of the "Home" tab.

Here are the font specs we'll use:

- **Font type:** Cooper Black
- **Size:** 82 pt.
- **Format**: Bold

This is what our text looks like now.

Next, highlight the text by clicking and dragging your cursor over the text.
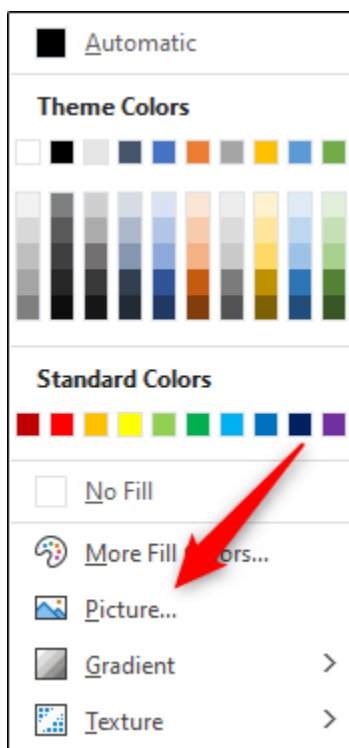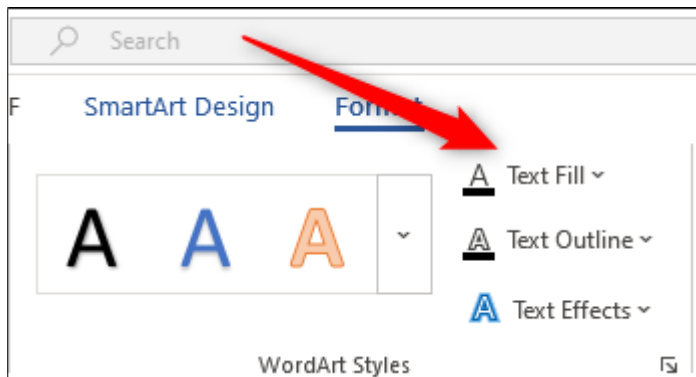

The "Insert Pictures" window will now appear. Here, choose where you'd like to locate an image:

- **From a File:** Choose an image from your computer.

- **Stock Images:** Choose an image from a stock image library.

- **Online Pictures:** Search for an online image.

- **From Icons:** Choose an icon from Word's icon library.

We'll use a stock image.
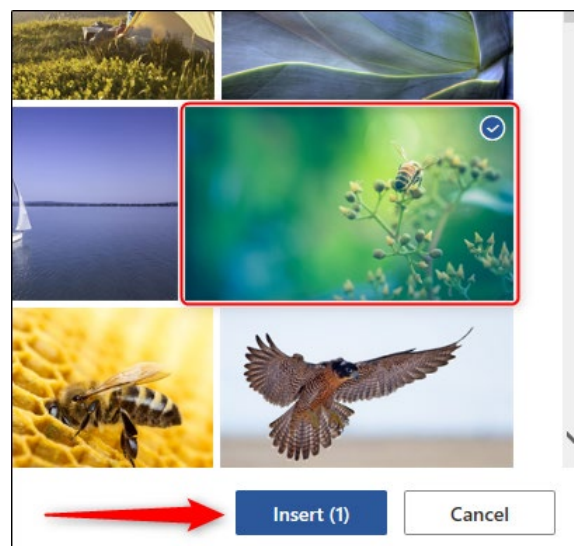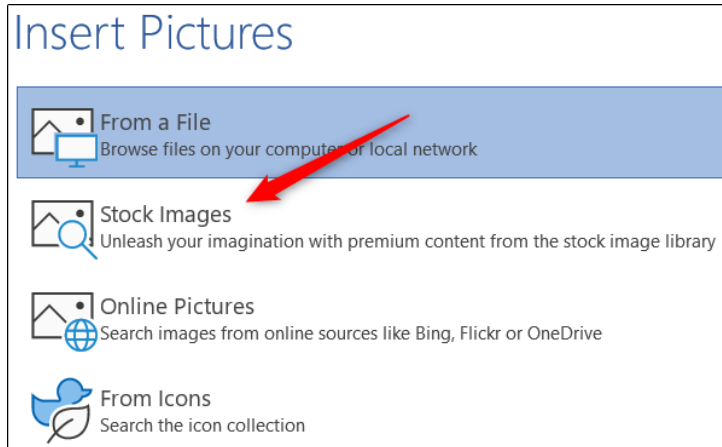
Next, you'll need to remove the background of the SmartArt graphic. Select the box and then, in the "Shape Styles" group of the "Format" tab, click "Shape Fill."
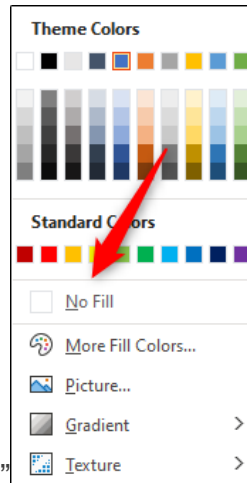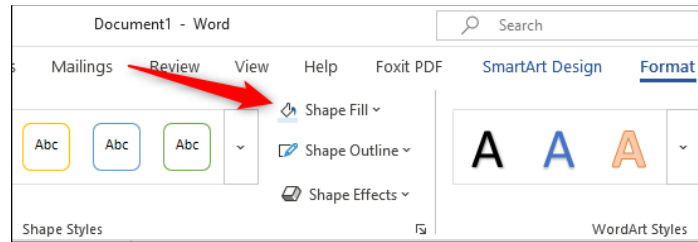
In the drop-down menu that appears, click "No Fill

The SmartArt background will now be removed, leaving only the text behind.

Though not as convenient as it used to be, with this little trick, you can still insert an image inside your text.