

Club Bytes



Brought to you by the Lake Gaston Computer Club



Word of the Month - Arping

It's a command that you use to probe or discover systems in your local network. I think most of you have heard of the "ping" command when you externally test your router in a speed test. The "Ar-ping" is appended to the word when you query what is happening internally in your computer. For a little more geekie explanation you can listen to this YouTube video.

https://www.youtube.com/watch?v=g_slrZZNYdM&feature=youtu.be



THE TWELTH DAY OF CHRISTMAS 2021

Happy New Year to all our members. Does everyone know what the Twelfth Day after Christmas is?

To a religious person it is known as the Epiphany, to others it might bring the thought of 12 drummers drumming and a partridge in the pear tree.

Did you know that the 12 drummers drumming dates to the 1909 when as an old English children's song it was put into a printed version and the music, we know today was put to it? Or do you remember when in 1949, Bing Crosby and the Andrews Sisters made it a number one hit at that years' Christmas.

If you are one of our members who have looked diligently at our website and bothered to read our history you will know that January 6, 1996 was the first meeting of the Lake Gaston Computer Club. Yes! we will be twenty-five (25) years old on Wednesday the 6th of January 2021. If you have not read it, I suggest you do so it is worth the read.

Yes! there are few around that remember the early days meeting in the Littleton Community Center and we were trying to put their memories to good use and had planned to put on a program during the first meeting in January. But along came something called the Coronavirus in 2020 and put a glitch in all our thinking.

We are still planning some type of event, but it looks like we will be a while before we meet in 2021 because people refuse to heed all the data and follow the three “Ws” and the virus is spreading again. Our best hope is that we can get the new vaccines administered in a way that we all have the good sense to get vaccinated and we can meet again.

Keep an eye on your email from the LGCC and we will let you know when that will happen. Meanwhile look through your old photos or have something to share contact me at vicepresident@lakegastoncc.org and we will put it to use. Meanwhile stay healthy follow the rules and we are there if you need us.



Can a USB Thumb Drive “Wear Out?”

Do USB drives actually wear out? Yes.

Depending on what you have saved on a USB device, if it's important, make sure it is backed up.

Inexpensive flash memory, the type used in USB thumb drives, memory sticks and other devices, is very, very cool. But there is a dark side that people don't talk about much.

Flash memory “wears out”

Any mechanical device that has a moving part will someday quit moving or stop working as it was designed to do. Some sooner than others.

A lot of electronic devices today use a technology known as “flash”. Flash memory chips are called “flash” because in order to write to it, the memory is loaded, and then a signal is sent to the memory circuitry that says, “remember this”.

Once the memory has been “flushed”, power can be completely removed, and the memory will retain whatever was written to it.

Example: You copy a file to a USB, that is a “flash” procedure. You make changes to a document on a USB, that is a “flash” procedure.

The problem is that memory can be flashed only so many times. The estimated number for that is between 10,000 and 100,000 times depending on quality and design of a particular USB drive.

When that limit is approached, some portion of the memory may not properly remember what was written to it, resulting in corruption. It may only take a simple bit of information to be wrong, or to “wear out”, for the entire contents of a flash memory chip to be lost.

The best use of USB thumb drives and other flash memory-based devices is simply copy-to and copy-from. Copy the information to the thumb drive to store

it, copy it from the thumb drive to a local hard drive to use it, and then copy it back to the thumb drive to store it.

Knowing that inexpensive flash memory-based devices will wear out eventually, there's one other thing you need to make sure to do, and that's to *back up*. If you keep your only copy of important data on a flash drive you are asking for trouble. I will wear out eventually and your data will become completely unrecoverable.

Remember the golden rule of backing up.

If there's only one copy: it's not backed up.

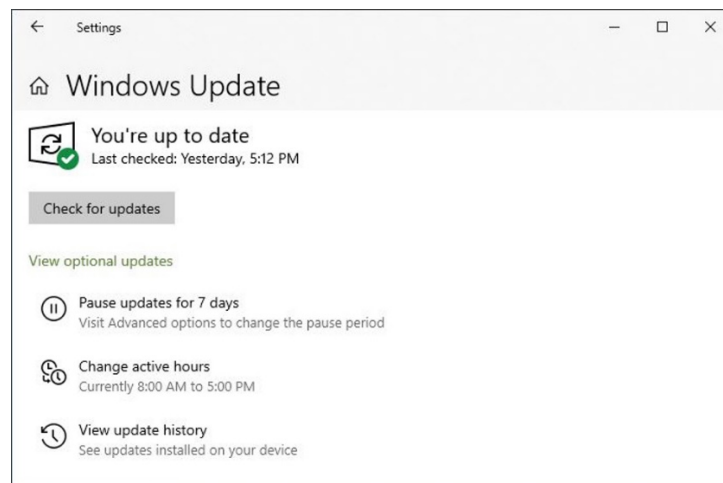
If there's only one copy on a flash driver, its days are numbered.



Windows 10's new optional updates explained

Recent versions of Windows 10 have introduced optional updates to Windows Update. What are they and how should you handle them?

Windows 10 users who have upgraded to version 2004 or 20H2 might have noticed something new when they go to *Settings > Update & Security > Windows Update*. Beneath the always-present “Check for updates” button, Windows update sometimes presents an optional updates item, as shown in Figure 1.



IDG

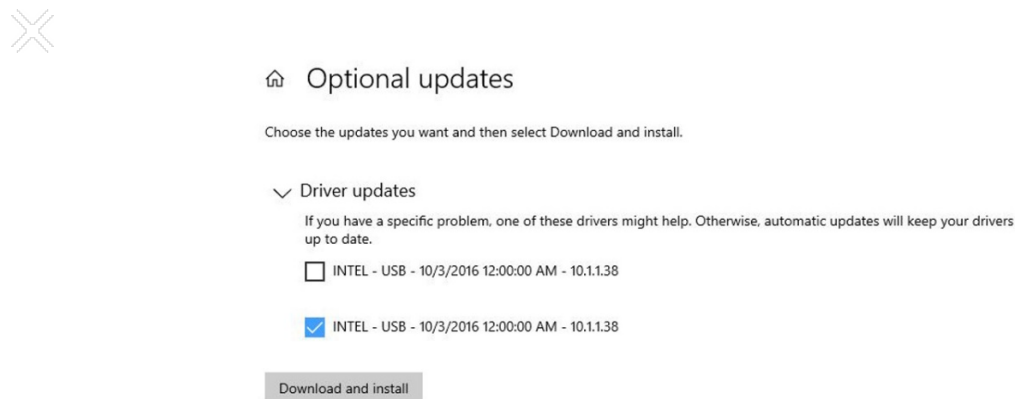
Figure 1: Occasionally, Windows Update shows a link that reads “View optional updates.” (Click image to enlarge it.)

This, by the way, is a return to functionality offered in Windows 7, when optional updates were tucked away in a separate window. When Windows 10 rolled out, Microsoft began putting all updates in one stream, but now the company is

returning to clearly labeling and separating optional updates from the usual monthly cumulative updates packaged up on “Patch Tuesday” (the 2nd Tuesday of each month). What are these optional updates, and what should users and administrators do with them?

Optional update type 1: driver updates

First and foremost, optional updates give Microsoft a way to let users know that device drivers other than the ones a PC is currently using are available for the target PC. In fact, most of the time when you click the *View optional updates* link, you'll see a display that reads “Driver updates.” As shown in Figure 2, if you expand that item (click the > sign, and it turns into the downward caret that appears in the screencap), you'll see a list of optional drivers available for the target PC.



IDG

Figure 2: You must select at least one checkbox to make the “Download and install” button active. (Click image to enlarge it.)

To install any of the driver updates, check its box and click *Download and install*. If you don't want to install any, simply ignore them.

Notice Microsoft's caveat ahead of the device driver list: “If you have a specific problem, one of these drivers might help. Otherwise, automatic updates will keep your drivers up to date.” Basically, this means that not even Microsoft itself recommends that users or admins routinely install these drivers. As with most device drivers, the conventional wisdom is “Don't install a new one unless A) the old one has issues as described here, or B) the new one has new features or functions the old one lacks.”

For the record, case A is far more common and typical than case B, except perhaps for GPU drivers, which routinely add support for new games and gaming engines to just about every new release. I've learned to avoid driver updates when they appear as optional updates in Windows Update. In most

cases, if you do the research work, you'll find that the optional item is a generic version that's been deliberately backdated (as with the USB driver shown twice in Figure 2, dated 10/3/2016). Microsoft does this on purpose to make sure that if a non-generic driver is available — most likely with more recent component files — the generic one won't overwrite the newer one unless the user forces it to.

Where to get driver updates, if not via Windows Update's optional updates?

Good question! As the prior caveat claims, WU will provide automatic updates when Microsoft decides that driver updates are required (rather than simply "available," as with optional ones). That said, most Windows 10 power users and admins don't much care to rely on Microsoft to handle driver selection and installation. Best practice is to watch the OEM website for specific PC models and get drivers from those sources, or to gPersonally, I follow that best practice, but I also watch for mention of new drivers in the [Drivers and Hardware forum](#) at TenForums.com. The regulars there are very conscientious about mentioning new versions of noteworthy drivers, especially for chipsets, networking devices, audio devices, and GPUs. The French website [Station-Drivers](#) is also an excellent site for finding current device drivers, often newer versions than those available through other means. Over the past decade and more, I've had excellent luck with this sometimes surprising but always reliable resource.

Optional update type 2: quality updates

Another type of optional update you might see is called a *quality update*. These are packages that roll up several fixes to address non-security bugs and stability issues. When they appear as sub-items beneath Optional Update in Windows Update, they're often previews of the upcoming month's non-optional Patch Tuesday release. (Note: Optional quality updates don't include security patches, which are pushed out immediately when ready, and may appear in Windows Update at any time if judged to be of sufficient severity and import.)

Figure 3 shows an optional quality update ready to be installed.

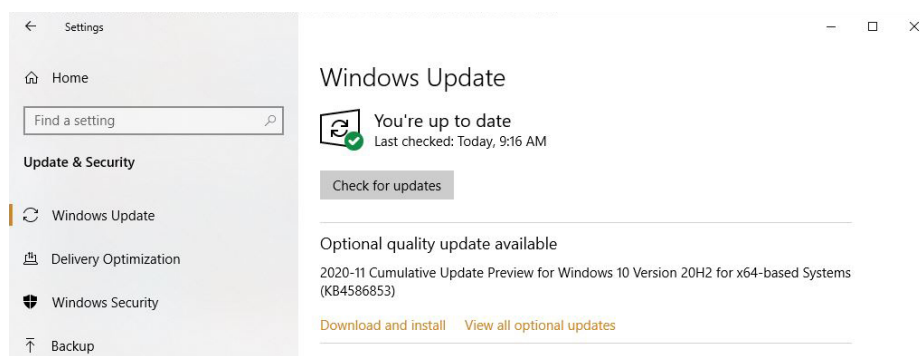


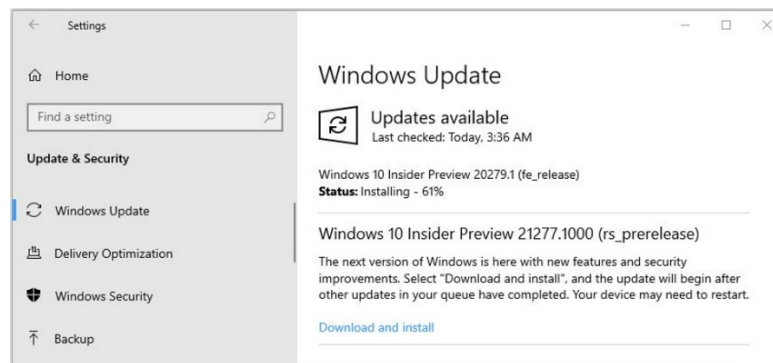
Figure 3: Here Windows Update offers the chance to download and install an optional quality update or to see a list of all available optional updates. (Click image to enlarge it.)

Except for testing purposes on non-production machines, I don't recommend installing optional quality updates. (I'll talk about this in more detail later in the story.)

Optional update type 3: feature upgrades and Insider previews

These days — by which I mean in Windows 10 versions 2004 and higher — when a new version or *feature upgrade* appears, it shows up as a kind of optional update, too. Same goes for new Insider previews for people who have opted into the [Windows Insider program](#), primarily for those signed up for Dev Channel releases for early testing of features Microsoft developers are working on.

Figure 4 shows what WU presents when it decides to offer an Insider preview update to a PC. A normal feature upgrade looks the same, except its title reads “Feature update to Windows 10, version YYHN” — for example, version 20H2 appears in the most recent such offer. For all such updates, one must click the *Download and install* link to fire off the upgrade/update process.



IDG

Figure 4: Notice the *Download and install* link. Only if users/admins click that item will the upgrade download and install process begin. (Click image to enlarge it.) Strictly speaking, this is a kind of optional update in the sense that Microsoft doesn't force it onto PCs without user knowledge and consent. This is a welcome change from the early days of Windows 10 when Microsoft could — and often did — force-upgrade PCs to a new (or newer) Windows 10 version automatically, including all the reboots typical once the Windows installer takes over a machine.

Nowadays, Microsoft only force-installs newer Windows versions over older ones as those older ones begin to approach end-of-support status. This happened recently (October 2020) with version 1903. [It was replaced with 1909](#) rather than

a more recent version, though, so trailing-edge installations did not suddenly find themselves forced into running a leading-edge version at Microsoft's whim.

Managing the update process

For most business operations (except perhaps in the smallest of businesses), IT manages the update process. Most production Windows PCs don't get updates when Microsoft issues them. Rather, designated update pros only permit such updates to apply to test machines. Those test machines are carefully examined and run through a battery of checks to make sure an update has no unwanted or untoward effect on the applications and data that production PCs handle routinely.

Only those updates that work properly without adverse effects are candidates for inclusion in the next upcoming, scheduled maintenance window — often scheduled over holiday breaks because workers are off, not using their PCs, and the on-duty maintenance team has a big chunk of time in which to perform maintenance. The big chunk of time is helpful because despite testing in the lab, problems do occasionally occur during patches and updates inside the maintenance window. If that happens, extra time means that the maintenance team can roll systems back to their original states before someone logs on at the start of the next workday, expecting access to a working PC (and working back-end systems to interact with).

Microsoft's new approach to optional updates and "optionalizing" feature and quality updates makes things easier for businesses and their maintenance teams. It flags non-essential items clearly and unambiguously as non-essential. This means that the maintenance pros in many businesses, and people like me, will mostly ignore them. One exception occurs when device drivers are showing problems or other software difficulties are present that optional updates are explicitly known — and have been successfully tested — to address.

If you're managing your own computer(s), take a cue from IT departments and don't install optional quality or feature updates until they've been thoroughly tested. With optional quality updates, that means waiting until they're pushed onto your machine by Windows Update.

With feature updates, it's best to wait at least 6 months after the update becomes available and then check for reports of problems before downloading and installing it. Unless you're actively seeking excitement and potential trouble, let other users — like your humble author — do the pioneering work, and install the updates only after most of the wrinkles have been worked out.



How to reset Google Chrome By [Paul Wagenseil](#) May 20, 2020

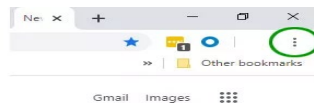
Web browsers now include 'reset' buttons to swiftly get rid of browser-hijacking adware. Here's how to reset Google Chrome.

If your Google Chrome Web browser suddenly has an unwanted toolbar, or its home page has changed without your permission, or your search results appear in a search engine you never chose, then it may be time to hit the browser-reset button.

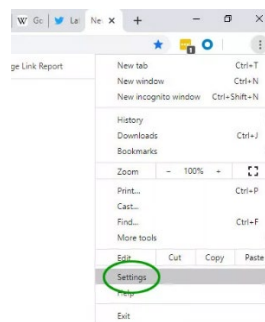
Many legitimate pieces of software, especially freeware, that you download from the internet slap on third-party, browser-hijacking extensions when you install them. The practice is highly annoying, but it's unfortunately legal. Fortunately, there's a fix for this in the form of a full browser reset, and Google Chrome makes it easy to perform.

The steps below are identical for the Windows, Mac, and Linux versions of Chrome.

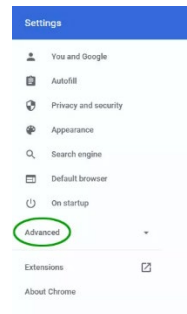
1. Click the icon that looks like three vertical dots at the top right of the browser window.



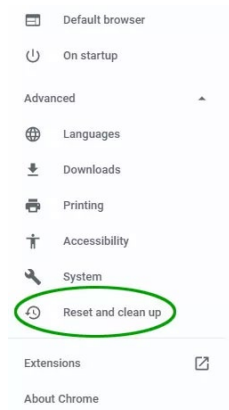
2. Select 'Settings' in the drop-down menu.



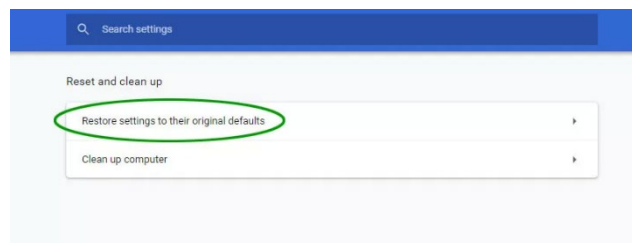
3. Click Advanced in the left-hand navigation bar in the resulting Settings page.



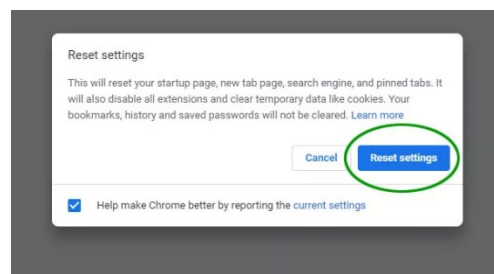
4. Select 'Reset and clean up' at the bottom of the expanded menu.



5. Select 'Restore settings to their original defaults'.



6. Select 'Reset settings' in the confirmation pop-up window.



If you've done the browser reset but your search engine and home page are still set to something you didn't want, or they revert to unwanted settings after a short period of time, then you may have a potentially unwanted program (PUP) lurking in your system that is making the changes.

Like a browser-hijacking extension, PUPs are legal in most cases, which makes them no less irritating. But you'll want to track down each PUP and kill it.

Start by running one of the [best antivirus](#) programs to try to get rid of the PUP, but be aware that some AV programs will not remove PUPs because makers of legal but unwanted programs may sue when that happens.

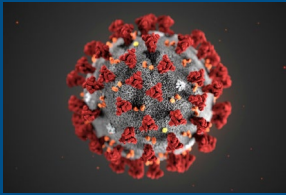
Then install and run [Malwarebytes Free](#) for Windows or Mac to zap anything the antivirus program missed. Malwarebytes Free isn't antivirus software and won't stop you from being infected by malware, but it's a great way to clean out unwanted files.



Best productivity tools of 2020: free and paid

Tech Radar has an article on all the new productivity apps. Look but hold on to your hats. I have never seen so many new software apps for every conceivable situation. The problem is how do they integrate between applications. Have fun investigating the time management part.

<https://www.techradar.com/best/best-productivity-apps>



Watch out for COVID-19 vaccine scams

As the country begins to distribute COVID-19 vaccines, there's no doubt scammers are already scheming.

Medicare covers the COVID-19 vaccine, so there will be no cost to you. If anyone asks you to share your Medicare Number or pay for access to the vaccine, you can bet it's a scam.

Here's what to know:

- You can't pay to put your name on a list to get the vaccine.
- You can't pay to get early access to a vaccine.
- Don't share your personal or financial information if someone calls, texts, or emails you promising access to the vaccine for a fee.

If you come across a COVID-19 vaccine scam, **report it to the Federal Trade Commission** or call **1-800-MEDICARE**. And check out **CDC.gov** for trustworthy information on the COVID-19 vaccine.



Searching for files and folders in Windows 10...

Knowing that everyone has one time or another lost track of a file and or a folder.

This can be very frustrating because you know where you put it... or did you. Microsoft has designated certain folders that files and sub-folders can be stored in. These are generally

referred to as “Libraries”, they are Documents, Pictures, Music and Videos. You create a file in a word program, and you would generally save that file to Documents or a sub folder within Documents.

Time goes by and you would like to retrieve that file, but you can't remember where you put it. Well, Windows 10 has ways and means of finding that file.

If you remember the name you gave the file, this becomes quite easy. The traditional way to locate a file in Windows is the **Search** item on the **Start** menu. Windows 10 makes this simple. Click on the **Start** button and just start typing the name of the file, or some portion thereof. The same thing can be accomplished by just clicking on the **Windows key** on the keyboard and that will open the Search box.

Another means of finding a file or folder is to open File Explorer (located on the Task Bar). This App will show all the folders and files located on your computer. You can initiate a search within File Explorer by selecting a folder you want to search and in the upper right corner insert the name of the file it will show everything saved in that folder that corresponds to the name of the file. You can open a document directly from the search results by double-clicking on it; open the folder containing the file, by right-clicking on it and clicking on **Open file location**; or copy or move the file as you like.

It's not a last resort but you can always check the Recycle Bin, it's amazing how some files inadvertently get in the Bin, but it does happen, so check it.



Apple and Amazon Won't Call You About Fraud Purchases

If there's one basic rule of safety you should be aware of, it's that large companies generally won't call out of the blue about your computer,

fraud on your account, or any other support related issue. Unfortunately, it's a scam that continues unabated, and now it seems the scammers have moved on from [pretending to be Microsoft](#) to [claiming to be Apple and Amazon](#).

The Federal Trade Commission (FTC) [issued a warning](#) about the scam calls on its website, and it even included two sample calls. In each case, rather than hear from an actual human, you get a text-to-speech robot voice. That's another increasingly common tactic and is likely a way to avoid arousing suspicions from an accent or less-than-adequate grasp of English.

The scammers are also using the common tactic of employing fear, uncertainty, and doubt (FUD). They'll claim that someone tried to do something terrible, like purchase an iPhone using your account and credit card, and they're here to help.

No one made a purchase, not yet anyway. But the call includes a way to contact the scammers, either through a call-back number or a dialing system (press one to stop fraud!). And that's the trick: rather than contact Amazon or Apple, you'll end up talking with the scammers.

Naturally, the next step is to "confirm your identity" by providing details like your name, address, and credit card info. And in the process, you hand over everything the scammer needs to go on a spending spree.

As the FTC states, the best thing you can do is hang up on these kinds of calls. Do not call any provided number and don't press one for help. Instead, if you're worried about your account, head to Amazon or Apple's site (or Microsoft or whoever contacted you) and directly contact the company.

Don't follow a web link provided in an email or phone call either, as that could be a redirect to a scam site. Use Google to find the website you need (or go straight to Apple.com or Amazon.com), then locate the "contact us" page.

Scams like these aren't going away, so it's best to be aware and tell your friends. Companies won't contact you to [solve your virus problems](#), [offer you a job over hangouts](#), [validate your account](#) over phone call or text, or even try to prevent a fraudulent sale. If the

company had reason to suspect a fraud purchase, it wouldn't have let the sale go through in the first place.

When in doubt, assume it's a scam. And if you think someone has compromised your credit card call your bank.



Should I Give an App or Website Location Information? Why You Should and When You Shouldn't.

Granting location permission gives apps and web sites a more accurate idea of exactly where you are. The question is: do they need it, or will they abuse it?

To view the AskLeo video, Ctrl+Click to follow this link or copy this link into your browser:

<https://askleo.com/grant-location-permission/#foobox-1/0/WD8rHEakrgl>

To read the full AskLeo article, Ctrl+Click to follow this link or copy this link into your browser:

<https://askleo.com/grant-location-permission/>











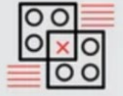

Fact or Fiction? By Nancy

Many years ago, I taught a class for the computer club on Google Search. One of the areas I touched on was fact searching. It dealt with those pesky emails we got spreading all sorts of false information. In this day and time, we are overloaded with so many pieces of information from the TV news media, internet sources, Facebook, Tweets, and blogs it

becomes difficult to discern fact from fiction. There are quite a few very disturbing groups doing excellent jobs bending and distorting the truth to challenge your mind to question even the most believable events. QAnon is one of the most well know conspiracy groups and there are more referred to as echo chambers on the internet.

When providing information to our fellow members we need to make sure it is reliable. You know the adage, "If it's too good to be true, or in these times, bad, then it isn't." So, think about these "fact-checks" before you pass emails, or share FaceBook, news, etc. along.

- **Identify and spot the different types of misinformation and why someone shared them.**

 <p>FALSE CONNECTION When headlines, visuals or captions don't support the content</p>	 <p>FALSE CONTEXT When genuine content is shared with false contextual information</p>
 <p>MANIPULATED CONTENT When genuine information or imagery is manipulated to deceive</p>	 <p>SATIRE OR PARODY No intention to cause harm but has potential to fool</p>
 <p>MISLEADING CONTENT Misleading use of information to frame an issue or individual</p>	 <p>IMPOSTER CONTENT When genuine sources are impersonated</p>
 <p>FABRICATED CONTENT Content that is 100% false, designed to deceive and do harm</p>	 <p>PROPAGANDA When content is used to manage attitudes, values and knowledge</p>
 <p>SPONSORED CONTENT Advertising or PR disguised as editorial content</p>	 <p>ERROR When established news organisations make mistakes while reporting</p>

- **Fact-check social media posts using tools and techniques of professional fact-checkers and share what you find to each social media platform.**



CONSIDER THE SOURCE

Click away from the story to investigate the site, its mission and its contact info.



READ BEYOND

Headlines can be outrageous in an effort to get clicks. What's the whole story?



CHECK THE AUTHOR

Do a quick search on the author. Are they credible? Are they real?



SUPPORTING SOURCES?

Click on those links. Determine if the info given actually supports the story.



CHECK THE DATE

Reposting old news stories doesn't mean they're relevant to current events.



IS IT A JOKE?

If it is too outlandish, it might be satire. Research the site and author to be sure.



CHECK YOUR BIASES

Consider if your own beliefs could affect your judgement.



ASK THE EXPERTS

Ask a librarian, or consult a fact-checking site.

- **Verify the images and videos you encounter on the internet in less than five minutes using techniques such as lateral reading.**

<https://www.commonsense.org/education/videos/how-to-use-google-reverse-image-search-to-fact-check-images>

- **Operate as a good digital citizen by not sharing misinformation on your social media account.**

DON'T GET TRICKED BY ONLINE MISINFORMATION

Remember these checks when browsing social media

Source

Look at what lies beneath. Check the about page of a website or account, look at any account info and search for names or usernames.

History

Does this source have an agenda? Find out what subjects it regularly covers or if it promotes only one perspective.

Evidence

Explore the details of a claim or meme and find out if it is backed up by reliable evidence from elsewhere.

Emotion

Does the source rely on emotion to make a point? Check for sensational, inflammatory and divisive language.

Pictures

Pictures paint a thousand words. Identify what message an image is portraying and whether the source is using images to get attention.

Think **SHEEP** before you share

FIRSTDRAFT

- Explain to family members and friends the pitfalls of sharing misinformation and teach loved ones how to fact-check on their own.

Misinformation spreads faster on social media and if the correct information then follows to correct it – that goes slower and is sometimes ignored or unread. A study results suggest that online trust, self-disclosure, fear of missing out (FoMO), and social media fatigue are positively associated with the sharing fake news (intentionally). In contrast, social comparison has a negative association. The study findings also indicate that online trust has negative association with authenticating news before sharing. The study

concludes with some implications for policy makers and marketers that could be useful in protecting society and brands from the perils of the misuse of social media and fake news.



The best news of all is the Lake Gaston Computer Club Website has been revamped and is available for all our members. Look at the new Education Tab for Virtual on-line classes. We all hope you enjoy.



lakegastoncc.org