Club Bytes 

Brought to you by the Lake Gaston Computer Club

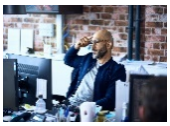
 Word of the Month

Bloatware: **BLOATWARE DOESN'T SOUND** pleasant, but it's a fairly mild condition: It's those apps that come preinstalled on your smartphone that you definitely didn't ask for and probably don't want. They're often used by manufacturers to push their own apps and services on top of (or instead of) what the smartphone offers by default. For more detail for the curious, see the following link: https://www.wired.com/story/remove-bloatware-phone/

Apple TidBits

Since the Repair Shop is only open with limited hours and the "Mac Guru" is not on board, this web link might help you if support is needed. Scroll down to the "Tell us How we can Help", Click, and the specific devices will be listed.

https://support.apple.com/

 **Repair Shop** will be **CLOSED Sept. 7, Monday for Holiday.**

KEEP YOUR COMPUTER CLEAN

It is important to keep your computer clean and running smoothly. For routine maintenance, it is suggested that you run the following 4 programs weekly. If you have trouble running these programs, the repair shop will help you.

1. **AdwCleaner** removes adware and potentially unwanted programs PUPS.

If you don't have it on your desktop do a Google search for AdwCleaner and download the free version from Toolslib.net or Malwarebytes.com. Go to the downloads folder and move AdwCleaner to the desktop. Open AdwCleaner > Scan > Ignore the preinstalled software found (do not check those boxes) > Quarantine > Clean and Restart Computer > close program.

2. **Malwarebytes** removes malware.
If you don't have it on your desktop do a Google search for Malwarebytes and download the free version from Malwarebytes.com. The free version includes a 14-day trial of premium (real-time protection). After the 14-day trial, either pay for the premium version or decline the upgrade and stay in the free version. Open Malwarebytes > Check for Updates by clicking on "Current" > Scan Now > Fix Issues > close program.

3. **Glary Utilities** cleans the registry, removes temporary files, manages startup programs and checks for software updates.
If you don't have it on your desktop do a Google search for Glary Utilities and download the free version from Glarysoft.com. Open Glary > click Overview tab > Check for Updates > click 1-Click Maintenance tab > check all boxes except disk errors and tracks eraser > Scan for Issues > Repair Problems > close program.

4. **SuperAntiSpyware** removes spyware, adware, and advertisers' cookies.
If you don't have it on your desktop do a Google search for SuperAntiSpyware and download the free version from SuperAntiSpyware.com. Open SuperAntiSpyware > update program if available then click on "Click here to check for updates" > OK > Scan This Computer > Quick Scan > Continue > Continue to remove threats > Continue > close program.

Who Is Being Hacked?

Software companies are being hacked/hijacked.

In July 2020, an exceptionally large Non-Profit Organization was contacted by a third-party service provider, **Blackbaud**, one of the world's largest providers of fundraising and donor engagement software for not-for-profit organizations. Blackbaud informed them that they had been the victim of a cyberattack and that a criminal was able to remove certain data from Blackbaud's clients. This included a subset of **donor data**.

Based on the information provided by Blackbaud the file removed may have contained contact information, date of birth, demographic information, giving capacity, and a history of donation dates and amounts.

Presently, we have no indications that your information has been misused. It is our understanding that Blackbaud investigated and ultimately paid the criminal's demand with the intent that the criminal would delete the data. **There was no mention as to the amount that was paid.** Although we have no way to confirm the data was deleted, Blackbaud has stated that it was deleted. Nevertheless**, we recommend you remain vigilant** and promptly report any suspicious activity or suspected identity theft to local law enforcement. For more information about this incident, please visit Blackbaud's webpage dedicated to this incident at **https://www.blackbaud.com/securityincident**.

Large Insurance Companies and Hospitals are being hacked/hijacked

Anthem BlueCross/Blue Shield of California, Bon Secours in Norfolk, and other Medical Insurance Companies have been hacked in the last several years. Medical fraud offers a considerable bounty for thieves because unlike a single credit card, health records can contain multiple personal identifiers. That's why stolen medical records tend to fetch higher prices. Whereas a credit card number on the black market may cost just 8 bucks, a medical record can be sold for $100. The following scenarios can help you catch medical fraud:

If you have ever gotten a bill for a procedure you didn't have or from a doctor you don't know, this may be medical fraud (lucky you caught it—lots of people don't!) Thieves may start by using stolen medical insurance for a small procedure with a physician you have never heard of—just to see if you notice.

Medical fraud can seriously disrupt your access to healthcare. If your medical data is stolen, thieves can create a fake ID and charge your insurance company until the limit's reached. If that happens, you may have to pay out of pocket for necessary procedures. Check those monthly reports from Medicare and your secondary insurance. All a thief needs are a few pieces of your healthcare information to charge prescriptions in your name—and then turn around and sell the medications. Make sure you black out those prescription bottles before you recycle them.

You can be hacked

Remember that NONE of the large computer companies call you. Do not fall prey to the phone hackers that tell you they are from Apple, Microsoft, Google, Amazon, McAfee, Norton, or any other software company that you may do business with. Hang Up! Be wary of any emails that you receive from these companies with suspicious deals that are too good to be true. They probably are. Delete the message, Don't open it. You can always do your research and put the catch phrase in the search bar of your browser. If it is a hack or other illegitimate deal the search will bring it up. You go to their web page and sign in, do not use the link on the email. Do not let anyone sign into your computer. There are exceptions. If you have called Support staff of a reputable company and asked for help with a problem, they will ask you if it is ok if they use a program to dial into your computer. You must give permission and you can see everything they are doing to fix your computer. They will give you a printout of the conversation, contact number and tracking number.

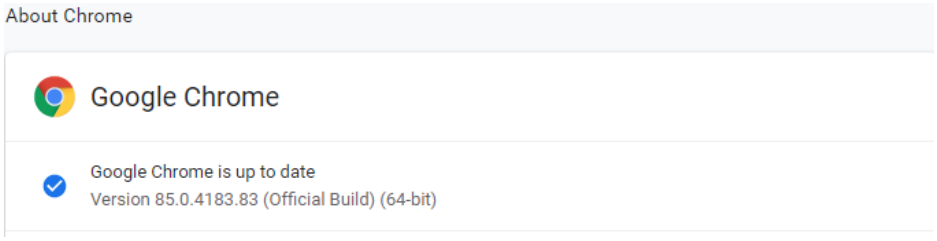
Email Hacked? Email account theft is rampant. If it happens to you, there are several steps you need to take -- not only to recover your account, but to prevent it from being easily hacked again.

Click on this link for the text article https://askleo.com/email_hacked_7_things_you_need_to_do_now/
For the video link click here or paste it in the browser address bar https://youtu.be/bDZcCNCYtxM

Attachments area
[Preview YouTube video Email Hacked? 7 Things You Need to do NOW]

Chrome 85 Now Available

Open your Chrome browser and move your cursor to the top righthand corner to the 3 dots that are vertically aligned. Click on them. Look at the bottom of the popup window for "Help" then "About Chrome" and select that. The Update Chrome should star automatically. If not click on Update. If it has already updated to Version 85 you will see that displayed.



How Much Can I Trust Information on the Internet?

This question opens a particularly important can of worms, because we get so much of our information from internet sources.

But we run into difficulty at the start. It's no longer "the internet" we should be wary of – it's the specific sources to which we choose to pay attention. In this context, the internet is nothing more than an information delivery mechanism. Almost every source of information we might previously have found offline is now present online, along with thousands of others.

Therein lies the fundamental problem: the internet has made it so easy to publish information, it seems everyone is doing so, whether they're a trustworthy surface of information.

So, the first and best recommendation: take everything, absolutely everything, with a grain of salt.

Don't trust any single source on its own – at least not until you've developed your own sense for just how accurate, reputable, or authoritative it happens to be. Even after that, it's smart to remain skeptical.

The truth is out there

So, in the digital era, where news travels quickly through multiple channels, how do you check for facts? Here are six of the best fact-checking websites, like Snopes and PolitiFact, so you can find the truth.

Snopes (www.snopes.com)

PolitiFact (www.politifact.com)

FactCheck.org (www.factcheck.org)

Lead Stories (www.leadstories.com)

Hoax Slayer (www.hoax-slayer.net)

Media BIAS/Fact Check (www.mediabiasfactcheck.com)