



THE WYSIWYG



November 2021

Volume 33 Issue 9

STERLING HEIGHTS COMPUTER CLUB

PO Box 385

Sterling Heights, Michigan 48311-0385

**MAIN MEETING:
TUESDAY NOVEMBER 2
7:00 PM**

Meeting room is open from 7PM to 9PM only. Be on time!!!

**Faith Baptist Church
34950 Little Mack Ave,
Clinton Township, MI 48035**

Located on the south-east corner
of 15 Mile Rd and Little Mack Ave.

➔ This is the SAME room location where we met
when Baker College owned the building.



IN THIS ISSUE:

About SHCC	2
President's Pen // Helpful Memory Bytes	3
Tricky Spam Emails // Club Officer Election	4
Need a PC Tuneup? Free PC Maintenance Tools	5
I Was A Fool, So You Don't Have To Be // Ads in Videos	7
It's Called "Clickbait", And You Need To Learn To Avoid It	9
Cautionary Tale About Free VPNs	10
Beware Of The "Auto-Renewal" Option In Your Security Software	12
Pay Close Attention When You Are Offered A Cookie Selection	13
Web Page Reviews	14

This Month's Main Meeting Topic:

Cyber Security

will be presented by the

Macomb County Sheriff's Office

Note the meeting location specifics above.
The meeting room is only open to our group from
7pm to 9pm.

Building door opens at 7pm — *please be prompt
and settle in quickly.*

Face masks are optional.

Guests and visitors are welcome. People can attend any SHCC meetings during two consecutive months before deciding whether or not to become a member. July and August do not count since there is no main meeting in those months. Membership includes admission to all SHCC functions and the newsletter. Membership is open to anyone. It is not limited to the residents of the city of Sterling Heights.

DUES: \$30/YEAR

CLUB ADDRESS: PO Box 385, Sterling Heights, MI 48311-0385
CLUB E-MAIL ADDRESS: Info@SterlingHeightsComputerClub.org
CLUB WEB PAGE: <http://www.SterlingHeightsComputerClub.org>

2021 SHCC Officers – Thanks for all your hard work!!!

President	Don VanSyckel	President@SterlingHeightsComputerClub.org
Vice President	Mike Bader	VP@SterlingHeightsComputerClub.org
Secretary	Paul Baecker	Secretary@SterlingHeightsComputerClub.org
Treasurer	Bernie DeFazio	Treasurer@SterlingHeightsComputerClub.org

Resource People

Firefox	Don VanSyckel
General Computer Questions	Jack Vander-Schrier
Hardware	(open)
MS Publisher	Paul Baecker
MS Word	Rick Schummer
Spreadsheets	Rick Schummer

SHCC Coordinators

Associate Editor	Rick Schummer
Door prizes	Don VanSyckel
Greeter for visitors	Jim Waldrop
Newsletter Publisher/Editor	Paul Baecker
Program Coordinator	Mike Bader
Publicity	Patrick Little
Publicity	Phil Reynaud
Welcome & check-in desk	Jim Waldrop
Web Site Admin	Don VanSyckel
Web Watch column	Paul Baecker

Contact Information

(Use the appropriate e-address for your questions/comments.)

Mike Bader	586-447-6683	programs@sterlingheightscomputerclub.org
Paul Baecker		newsletter@sterlingheightscomputerclub.org webwatch@sterlingheightscomputerclub.org
Patrick Little	586-264-1497	publicity@sterlingheightscomputerclub.org
Phil Reynaud	586-212-2848	publicity@sterlingheightscomputerclub.org
Rick Schummer		assoc-ed@sterlingheightscomputerclub.org
Don VanSyckel	586-731-9232	doorprizes@sterlingheightscomputerclub.org webmaster@sterlingheightscomputerclub.org
James Waldrop	586-731-6481	greeter@sterlingheightscomputerclub.org check-in@sterlingheightscomputerclub.org

Club Dues Amounts

The club dues were increased to \$30 per year at the November 2018 meeting.

This includes a digital version of the newsletter sent monthly, except for July and August, when the club does not meet.

A paper version of the newsletter is available in place of the digital newsletter, for an additional \$31 per year (increased at the March 2019 meeting).

Associate memberships, for a second member of a household, remain at an additional \$15 per year.

Two-Month Meeting Schedule

November 2021	December 2021
2 - SHCC Main Meeting	7 - SHCC Main Meeting
14 - SEMCO meeting	12 - SEMCO meeting

Newsletter submissions are due 20 days before the club meeting, but the earlier the better. They should be sent to : newsletter@SterlingHeightsComputerClub.org

© Unless stated otherwise, all materials contained in this newsletter are copyrighted by the Sterling Heights Computer Club. License is hereby granted to other clubs (non-profit) to reprint with credit.

The President's Pen

by Don VanSyckel



We've been back live for two months and all's going well with the meetings. The only real issue on the horizon is budget. With the current room cost, the current number of members, and the current dues level, we're good for about two more years. To address this we continue to seek out a meeting place at a lower cost. We have a couple of alternate locations under consideration and we are waiting for details from a third. No decisions are likely to be made until at least December. The one thing we need to survey members about is the possibility of changing the meeting time from evening to morning or afternoon.

For many November club meetings in the recent past we've invited Mr. Tapaninen from Micro Center to bring his "What's Hot For the Holidays" presentation to us. Unfortunately, Micro Center management has eliminated the training position which included these presentation opportunities, so there will not be any more presentations from Micro Center, at least in the foreseeable future. The good news for Mr. Tapaninen is that he transferred to the service department, so you might still see him around the store.

This month we will open nominations for Officers again and then elect our club Officers for 2022. If you're interested in serving as an Officer, nominate yourself or it can be arranged to have someone nominate you. The Officer duties are available in the member-only section of the web site. If you have misplaced the web site address recently emailed to you, request it again from an Officer.

We're looking forward to this month's presentation on **Cyber Security** by the *Macomb County Sheriff's Department*. There are many facets to cyber security and it'll be great to get a briefing by professionals in the field. The sheriff's department works with other branches of law enforcement which gives them an even broader view of this subject.

Remember, please be on time, 7:00 PM. We don't have access to the building until 7:00 PM and we want to get started as quickly after 7:00 PM as we can to maximize our time.

Last Month:

We had a presentation in October by SHCC member Paul Baecker. Paul presented "PC Tools for Windows". He covered many useful tips for you to use. Very useful info.

(Editor's note: Since we had an issue with accessing the network to present some Internet tools and services, a follow-up session is being considered for the near future.)



Helpful Memory Bytes

By Jim Cerny, Forums Coordinator / Instructor
Sarasota Technology Users Group (FL)
www.thestug.org vp1@thestug.org

Let's review and explore what we need to know about basic computer storage (bits and bytes) and how it helps us get an idea of the data space needed to save and backup our stuff.



Flash drive



External Hard drive



Internal Hard drive

Suppose you landed on a planet, and the aliens there only had one hand and one finger on it (not ten fingers like we do). All they could do was flash a single digit or none at all (hence, a zero or one). How high could they count? Could they do basic math?

All computers use the binary system (a single digit of 1 or 0) – that is, they store and work with data saved in memory as zeros and ones. But there is NO LIMIT to how high you can count – you keep adding on more zeros and ones. For example, the digits we know in our numbering system such as 1, 2, 3, 4, 5, 6, 7, 8, 15, 16, 31, 32, 33, etc. would be the following in binary = 1, 10, 11, 100, 101, 110, 111, 1000, 1111, 10000, 11111, 100000, 100001, etc. So, adding a new digit to the left doubles the size of the memory (or number). Believe it or not, math gets a lot simpler with only two digits.

A single binary digit is called a BIT. Eight bits together form a BYTE of data. Eight bits allow for 256 different combinations, enough to cover not only our 26-character alphabet, but special characters and more. Every keystroke on your keyboard enters one byte into memory!

I love the old science fiction movies – where the spacecraft command center was filled with gauges and dials! To read a value on a dial, you had to look closely to see where the arrow was. It showed measurement on a scale of lines, and it was up to you and your eyesight to see the amount or "reading." But with binary digits, you don't care about "how much"; you only need to know if it is there or not there -- a one or a zero. To get more accuracy, you add more binary digits. So, you will need a lot of them, but they are cheap and much easier for use in electronics.

One KILO-byte of memory is 1024 bytes, but when we start dealing with large amounts of computer storage, we round it off and call it a thousand.

One MEGA-byte of data is one million bytes or one

(Continued on page 10.....Bytes)

Tricky Spam Emails

By Jim Cerny, Forums Coordinator / Instructor
Sarasota Technology Users Group (FL)
www.thestug.org vp1@thestug.org

You probably are all aware of those awful spam emails that come to you in your inbox. But recently, I had a very sneaky and tricky spam email that appeared to come from a friend, and I need to tell you about it so you can be very careful.

First, I received a brief email from a friend of mine who was also listed in my contact list, but I found out later that the source email address was not really his. It "looked" like his, even having his wife's first name in it, but it was NOT his email address; it was from a different email provider, which he never used. Yes, that was tricky all right, but later that week, I received one even worse. The email sent to me appeared to come from another friend and, being very careful, I "hovered" my mouse on the email address, and it did show his actual email address, exactly as it is entered in my contact list! But it was NOT from him. Fortunately, I called him, and he confirmed that someone had "stolen" his email address and was using it to try to get gift cards from people.

So, in addition to the usual email precautions, I would like to offer these to help you from being scammed –

+ Brief emails from a "friend" that say something like "Can you help me?" or "Can I ask a favor?" are clues that they are bogus. Call your friend to confirm if they really need your help. As they say, if it was really urgent, they would have called you, not sent an email.

+ If you do reply to such an email by mistake, you will get a follow-up email with a sad story and an urgent request for something like a "cash card" or donation. Don't do it!

+ Do not reply or provide ANY personal information in ANY email. Emails can be forwarded to anyone anywhere. Valid email addresses are traded like stolen credit card numbers.

+ Do NOT send money or credit card information in any email. Instead, use your online banking to pay bills.

+ THINK – did the email text really appear to be something your friend would write to you? If there is the least bit of oddness about it, call the person.

How do these scammers get started? Our neighborhood has a directory provided to all residents, which includes phone numbers and email addresses. Many people purposely do not provide their personal information in such a directory. Once you get an email address, I suppose it

(Continued in right column —>>>>>)

Club Officer Election Announcement and Officer Duties

Our SHCC Officer elections will be held at this month's November main meeting.

Generally at this time each year, the duties for each of the officers of the club and the nomination and election process is printed here in the newsletter. This year we'll do it a bit differently. You can review the individual officer duties and the election process on the SHCC web site, in the special members-only section.

The President sent an email to you in September, briefly outlining the processes, and including the members-only web page URL, where you can review the information at your leisure.

It should be mentioned here that every member should take a moment to consider volunteering for an office, to give back to the club for everything that you get from being a member. YOU can take the opportunity to help shape the club for the next calendar year. Even though any member can make suggestions and recommendations to the officers, the officers make most decisions about changes as needed and requested.

So, think about it. Nominate yourself for an office, or nominate a fellow member (with his/her consent first, of course). We all look forward to a healthy nominee selection for each office!

Officer nominations were opened at the September and October meetings, and will be opened again at the November meeting. Elections will occur in November (after nominations are closed) for a term in the next full calendar year.



is possible to tap into some emails sent by that address and thus obtain many more email addresses.

Finally, it appears a scammer can send an email that appears to come from someone else's address, and yet they still receive replies to the scammer's email inbox. How they do this, I have no idea, so be careful.

One final story – I was at the Walmart customer service desk when an older man was requesting a money transfer to his son, who needed money quickly. The Walmart people knew right away that it was a scam and refused to fulfill his request. The man was angry, but it was the right thing to do. He wanted to send "his son" several thousand dollars!

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.



Need a PC Tuneup? Free PC Maintenance Tools

By Bob Rankin

<https://askbobrankin.com/>

An astute AskBob reader asks: 'I know I need to clean up my hard drive every once in a while. But are there any other regular PC maintenance tasks you recommend doing on a regular basis?' Well, yes! Here are more than ten free programs you can use to clean up and tune up your Windows computer...

Keep Your Computer Running Fast and Reliably

Just like a car, your computer needs regular maintenance to continue performing at its best. Waiting until accumulated minor problems make your computer run intolerably slow is bad for it. A neglected PC works harder than it should and then hardware can start to fail. You may experience a sudden catastrophic crash similar to a car engine seizing up because you never changed the oil.

Fortunately, there are some free PC maintenance tools that make it a breeze to keep your system in top shape. Their functions generally include hard disk management; optimization of system settings; and deletion of unnecessary, duplicate or temporary files. Some free PC maintenance tools include scheduling of maintenance, diagnostic tests, backups, malware cleanup, and system-tweaking options for advanced users.

Free Computer Maintenance Tools

Smart users perform PC cleanup and tune-up operations at least once a month. Here's what I recommend, and some free computer maintenance tools to help you do the job. Unless otherwise mentioned, all of them work with Windows 7, Windows 8 and Windows 10 computers.



[CCleaner](#) by Piriform is a popular PC cleaner/optimizer/privacy tool that's developed a sterling reputation over many years. CCleaner zaps temp files, web browser history, cookies, and form inputs, to remove all traces of your online activities. It also mops up after Windows, cleaning out your Recycle Bin, removing unneeded log files, deleting memory dumps, and pruning obsolete registry entries. CCleaner does not include a defrag module, but Piriform also offers the free [Defraggler](#), which does the job quite well.

The [Glary Utilities](#) is another PC maintenance suite, downloaded over 40 million times. It, too, does registry, privacy, defrag and junk files cleanup. It includes an application uninstaller that is more sophisticated than Windows Add/Remove app; for example, you can tag multiple applications to be uninstalled in one operation. It also includes a startup programs manager, a memory manag-

er, and a nifty utility to remove unwanted context menu items. Cleanup can include a sweep for duplicate files, empty file folders, and broken shortcuts. It will also back-up and restore all your hardware device drivers. The latest version claims to be 800% faster at analyzing your PC for potential problems.

[PrivaZer](#) is a hard drive clean-up utility on steroids. It gets rid of junk files and wipes away traces of activity that could compromise your privacy. PrivaZer zaps duplicate files, temporary files, log files, unneeded Windows update files and old Windows installs left over from a system upgrade. In addition to cleaning files and filesystems, PrivaZer does a thorough scrubbing of your Windows registry, and will also remove web browsing history, saved passwords, and cookies.

A few notes about defragmenting your hard drive. Traditional magnetic hard drives installed in most computers do benefit from defragmenting, as it speeds up disk access. However, SSD (solid state) hard drives do not require defragmenting, and some people believe that you can shorten the life span of an SSD by defragging. I don't think that's true of newer SSD's, but it's still a best practice to defrag only magnetic drives. Treat hybrid (magnetic/SSD) drives the same as magnetic drives. Also note that Windows 7, 8 and 10 have automatic defrag built in, but you may still benefit by running a third-party defragger a few times per year.

My article [Free Hard Drive Tune-up Tools](#) has links to several programs that will help you identify large, duplicate or unwanted files that are clogging up your hard drive. You'll also find links to recommended software that will help you permanently erase a hard drive, recover accidentally deleted files, or fix damaged drives that won't boot up.

[Macrium Reflect](#) is my preferred software for making backups. The *Free Edition* offers backup, disk imaging and cloning solution for both commercial and personal use. It can schedule your backups to run automatically, which I consider a must.

The [NirSoft](#) website provides a collection of freeware, including Windows password-recovery tools, network monitoring tools, and some privacy-related utilities.

[Speccy](#) and [Belarc Advisor](#) are two diagnostic programs I rely on when a computer doesn't seem to be running optimally. See my article [What's Going On Inside My PC?](#) to learn how they can help you identify overheating and other potential problems.

The [Windows Memory Diagnostic Tool](#) is built into Windows 7 and higher. To run it, click the Start button and type memory in the search bar. Click Windows Memory Diagnostic in the search results. You can choose to restart and check for memory errors, or tell it to check for memory problems the next time you start your computer.

Don't Forget About Security

Finally, it should go without saying that you need to be vigilant about computer security. Here are the two most important pieces of advice I can give on that subject:

- Keep Your Software Updated - See my related article [Keep Your Software Updated \(or else...\)](#) to learn how to scan your computer for software vulnerabilities, and how to make sure you have the latest versions and security patches.
- Use Anti-Malware Protection - See my list of [Free Anti-Virus Programs](#) to learn how to get excellent security software for free.

Each of these free PC maintenance programs has additional bells and whistles for advanced users or troubleshooting. Some have premium versions that you can purchase, to get additional features. Read the product features lists carefully if you have a particular issue that you want to resolve. In my opinion, all of these freebies will do a good job of tuning up your computer for top performance. Try a few of them, and then uninstall the ones you don't want to continue using.

This article is republished, with permission, from the Ask Bob Rankin web site.

{Editor's note: When selecting software products to download from the Internet, sometimes a site will request personal info from you (your name, email address, etc.) during your request process. In most cases, you do not need to enter this info to acquire the free software offering. Be aware of this, and don't offer what you don't need to offer. Your request to download the free version of [Macrium Reflect](#) (excellent backup software), for example, asks you to 'register' by entering an email address, but it's not necessary....just move along with your download process. Also, during the installation of this product, you will again be prompted to register with an email address to continue the installation of the software. But you can ignore it and move along to complete the installation without giving up this personal info. It is totally legal to ask for your info — they want to know who is using their software, but Macrium has not made it absolutely a requirement yet. Also, when you update software, the product may again prompt you to enter private info. Resist whenever possible. You won't get anything in return for your personal info (which includes your email address!).}

Protect your identity (including your email address!) whenever and wherever you can. IF some place (whether on the web or local) REQUIRES an email address, have one available to use (your ISP offers you several free email addresses to use for whatever purpose you choose) to keep this stuff separate from your friends/family email, because you may receive follow-up messages or even spam (when your email address is shared or sold by/to spammers/hackers). GMX.com is one of many online email systems where you can create an email account using a fictitious name, a fake birth date, and does not require a phone number. I have created a separate anon-

ymous email account there for each of my PCs (remember, this is a hobby to me) in order to download promotional software that is limited to one per 'user' (meaning per 'email address') on more than one PC. Don't use your name in your email address, to further protect yourself from scammers and bulk emailers.

Free software often does not come with any technical support — that is reserved for users who pay for the product (which is why some free software also has an associated "PRO" version available, at cost and with technical support). Most popular software has lots of support on the web, in the form of blogs, forums, and videos, AND your club members, and therefore paid technical support is often not needed, unless you want/need the bells or whistles that come with "PRO" versions.

Belarc Advisor is a fine product, but when it scans this PC that I use for publishing the WYSIWYG, which was upgraded directly from Windows 7 to Windows 10 early in 2020, it keeps noting that the PC has Windows 8.1 installed (but it NEVER had Windows 8.1). Perhaps it is getting that detail from somewhere in the PC's registry? I don't know why Microsoft did not update the OS details within the PC, and Belarc Advisor only collects what it can find on the PC, so its resulting report might not be 100% accurate to your eyes. If you choose to keep the Belarc Advisor report (it opens in Internet Explorer by default on my PCs) as a permanent record, choose "Print" and save it as a PDF file. But note that that PDF file is an image in time — running Belarc Advisor a day or week later will generate a different report about the state of your PC.

The term "top performance" is only relative, of course. Your PC's top performance will be different from that on someone else's PC (partially due to the CPU and RAM installed, but also somewhat due to how files are organized and fragmented, and whether the drive is an HDD or SSD), but regular maintenance is mandatory to keep your PC in its best possible performance state — and to also keep it secure.

It goes without saying, but I'll repeat it: Be sure to have at least one Full System Backup available, in case a maintenance software product gets too aggressive with its 'cleaning', and corrupts or removes one or more critical files — perhaps even files that are SHARED among two or more software products on your PC. And make sure that periodic Restore Points are being created automatically.

Regarding defragmenting (or not) an SSD (Solid State Drive), the [Crucial](#) company (a major manufacturer of RAM memory chips and SSDs) states that "you don't have to defrag an SSD, because there is no performance advantage". Further they say "do not defrag a solid state drive. At best it won't do anything, at worst it does nothing for your performance and you will use up write cycles". That means that the SSD's life will be shorter. Good defrag software, like Defraggler, will recognize an existing SSD and will not allow you to defrag it.}



I Was A Fool, So You Don't Have To Be

By David Kretchmar, Hardware Technician
Sun City Summerlin Computer Club (NV)

<https://www.scsccl.com>
dkretch@gmail.com

I don't necessarily think of myself as a fool, but I did a foolish thing a few years ago. I bit on one of Motley Fools' ubiquitous teaser Internet ads promoting the best new emerging technology stocks that were about to "explode." I



paid (I think) \$29 to Motley Fool to get the names of the stocks. Motley Fool sent me the names of several mostly small and pink sheet stocks. Most pink sheet companies are highly speculative, have little or no earnings, and are low-priced penny stocks. For many pink sheet stocks, a price appreciation up to one penny would be wildly profitable, but well over 90% of these stocks appeared worthless.

I wonder if they are buying shares before they recommend them and running the shares up and then maybe even shorting them or just taking advantage of people willing to pay for their information. Their expertise seems to be selling themselves, not researching companies.

The Motley Fool's website is self-described as "A wide-ranging investment resource that intended to "educate, enrich, and amuse individual investors around the world." The site includes discussion boards, quotes, data, and of course, stock-picking advice. Many of the articles are voluntarily contributed by various individuals. Unfortunately, I suspect that many have taken a position in the stocks they are now pumping, not unlike the Motley Fools, with hopes of profitable dumping.

Upsells

If you are not satisfied with the advice provided according to your original subscription, the Motley Fools will offer you "better" subscriptions, such as:

<p>Everlasting: Cloud Disruptors 2020 Invest in The Motley Fool's "No. 1 Technology of the 2020s"</p> <p>\$1,999/year</p>

Or:

<p>One Full access to all Motley Fool stock services and exclusive access to Tom Gardner's Everlasting Portfolio</p> <p>\$13,999/year</p>

A Foolish Website

I am not new to the stock market; I focused on security analysis in college and have been doing my own research for over 50 years. Almost everything I have seen

(Continued on page 8.....**Fool**)

Ads in Videos

News and/or Opinion From the Editor

When you surf the web, looking for information or entertainment in a video format, you have certainly become aware that web sites (like Google's YouTube, for example) are increasingly forcing us to view ads, either before the video, or in the middle of the video, or at the end of the video. At one time in the recent past, Google considered charging a fee for all of us to view content on their YouTube web site, but the feedback in various articles attacking that idea was swift. Google needs to make a buck somehow, so an alternate method of doing so is to push ads in our digital faces when watching their videos, similar to ads on network television. Often, there is a button in the video window that allows us to skip the included ad after a few seconds. In other situations, we have to waste part of our life on the whole ad, before getting to view the valuable content we intended to watch.

Good stuff is often not totally free (although lots of truly free software is actually very good, but that's another discussion). As for web sites, someone has to pay for the salaries and the technical services and equipment that make the site, and the video, available to visitors. Ads are usually the method for recouping these costs, but many viewers (including myself) are not going to buy anything that's advertised anyway, so why be forced to view them?

There is a link in the WebPageReviews (on page 14) that discusses the various types of ads that YouTube uses as methods for generating revenue, both in videos and outside of videos, as well as what you *can* block and how to do so. Some ads you can avoid (using ad-blocker software installed into your web browser, such as [Ublock Origin](#)); some (like non-skippable types in videos) you can *not* block.

So, when watching a video wherever you are on the web, don't get upset that you have to wait for an ad to pass by to get to the meat of the presentation, or when the presenter takes a moment to push a product that is or isn't necessarily related to the content of the video. Stay calm and understand the reason for the ad. In a video, the ad is not tracking you (unlike some ads appearing on the web sites themselves), so you are not in any danger of giving up any personal information, as long as they are just playing in the video content.

Another type of advertising in videos is the kind that pop up in a box, usually near the bottom of the video window, covering part of the video's content. Usually, if you look closely, you will find a small "x" in one of the corners of this ad box. It may be in the typical upper right corner (just like closing the window of an application on your computer), but they can try to trick you by locating it in another corner. Click it (remember: "click" means using the LEFT mouse button) and it will usually close, and free up the whole video window for your further video enjoyment.

There is a link in the WebPageReviews (again, page 14) to a video that discusses why you should gracefully shut down your PC. The presenter has a long ad at the end of his presentation to cover his costs. This is an example of an ad that you *can* skip over, if you wish.



(Fool.....Continued from page 7)

from the Motley Fools is absolute garbage. I highly recommend not using their website for any information except maybe for the entertainment value of how foolish it is. Often there are contradicting opinions on the same stock on the same day!

There is way too much advertising on the Motley Fools subscription website. This site is without transparency and, therefore, of questionable value for investors. Suppose you want to be successful, and actually be one of the rare investors who make money relying on the advice of others. In that case, you need to

receive information from people whose own investing/trading results you can clearly see. There are several dozen articles every day, and I believe no one could construct a good trading strategy based on the hundreds of stocks they say are "ready to explode."

The Motley Fool's subscription website is a mess of marketing. Most of the articles provide virtually no actionable information, except pitches for more expensive Motley Fool newsletters. Occasionally there is a well-written article that contains decent information, but this is rare.

To be fair, I do agree with their philosophy that a buy and hold strategy, not trading, is the path to real wealth accumulation. They deride ALL short-term trading dogmatically but make tons of picks, some work, others totally fail. Also, they advise not to bother trying to time the market; just spend time in the market holding your winners and trimming losers. So there – in this paragraph, I've reflected virtually all of the sound advice you are likely to glean from the Motley Fool website – and it was FREE!

Can they do 5X better than the market?

It is inconceivable that The Motley Fool could beat the S&P 500 by over 500%, as they claim in their current advertising. Most professional money managers and advisors have difficulty equaling the performance of the market averages. Those who are considered investment geniuses, such as Peter Lynch and Warren Buffett, could beat the market by a few percentage points a year. Anyone able to beat the market averages by 500% would be able to amass great wealth investing and would not have to sell a tout service.

Even the free offers are less than worthless

Almost every day, I see Motley Fool teaser articles on sites such as Yahoo Finance, and often the headline is misleading. The article provides just a superficial discussion of a stock. Usually, the article ends stating the stock discussed is OK (or bad), but the Motley Fools knows ten stocks that are better, which they will provide to you if you just furnish your email address. I have done this several times (providing my "junk" email address) and have never received the information the Motley Fools promised. Instead, they bombard my mail account with worthless spam. I suspect they also sold my email address since I also started receiving spam from unknown companies.

The sports betting scam

When I worked as a Special Agent in a former life, I was involved in investigating an off-shore sports betting site.



The owners of this site quickly discovered they could make more money selling gambling advice, also known as tout services, than from the bets themselves. The

profit on sports bets was about 5 percent – (10% of losing bets), similar to on-shore bookies and casino sportsbooks.

Say Boston was playing New York, they would tell half their new subscribers (or potential subscribers) to bet on Boston, and the other half New York. After the game, half of their customers would feel their handicapping might be good, and the other half would probably quit. The subscribers who stayed would tell half of them to bet one side of a game and the other half to bet the other side. Again, half of their customers would think they were great, and the other half would have their doubts. After doing this once or twice again, they would have a smaller pool of customers who thought they were geniuses and would pay big bucks for their next tip.

Conclusion

The Motley Fool and many other stock picking services operate similarly to the sports tout scam. But, at least they are no fools; only people who buy their services are.

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.



It's Called "Clickbait", And You Need To Learn To Avoid It

By Kurt Jefferson, Editor
Central Kentucky Computer Society (KY)
<https://www.ckcs.org>
lxtown2@gmail.com

I was eating yogurt as I was reading stories about one growing danger on the Web: Clickbait. What I read made me pause and put down my spoon.

It turns out that plenty of us are clicking on email links or Facebook postings sent to us from unknown senders. Unfortunately, this can lead to malware and trojan horses infecting your computer.

The practice is called clickbait. Someone you don't know sends you an email or a Facebook posting. It contains a link. You click on it.

Catchy and provocative headlines are usually a dead giveaway that you're being targeted by clickbait.

Clickbait often contains these qualities:

- Headlines that appeal to your strong emotions, such as humor or outrage
- Headlines designed to grab your attention, leaving you wanting more information
- Headlines that tell you nothing about the content of the article
- The headline is too good to be true
- Content that encourages you to share the item with someone else on Facebook *{or other social network}*
- Funny images or video

Examples of clickbait headlines include:

- * *87-Year-Old Trainer Shares Secrets to Losing Weight*
- * *When You Read These Shocking Food Facts, You'll Never Want to Eat Again*
- * *Stop Eating Chicken Breasts Immediately*

The point is to teach people to recognize clickbait and to avoid it. It's not worth your time.

Free IQ tests and credit score checks often ask you to fill in personal information. Unfortunately, you don't know that the website collects your personal details to build a profile on you. Once you submit this information, you'll be subjected to scams and even more links to dangerous websites.

Clickbait links open the door to more spam and potential malware, adware, spyware, viruses, worms, trojan horses, and the real possibility that someone could take

over control of your computer. Just say "no" by refusing to click on links you aren't sure about.

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.

{Editor's note: Clickbait is just one method for gathering your web-surfing habits and info, which IS part of your personal identity, connected with your IP address. One of the most common methods of collecting info about you is via services that deliver your credit report to you. Places like CreditKarma, and so many others, do supply your credit report for free, but in doing so, you are giving them your permission to take a copy for their own possession and use, before they pass it on to you. Imagine the vast amount of your personal information and identity in those reports, and what they might do with it, or to whom they might sell it! The only secure method of getting your three free credit reports each year (one from each of the three credit reporting companies) is by visiting the <https://www.annualcreditreport.com> web site.}

(Free VPNs.....Continued from page 10)

VPN service. One of the interesting things that this data leak revealed was that there were several differently-named free VPN services that all appear to be run by the same company. These were all supported by mobile apps that were gathering inappropriate data, combined with the attempt to disguise the company's true identity, suggest that this was a deliberate attempt to engage in unethical behavior.

Caveat Utilitor

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.

{Editor's Note: Are you getting bored yet with hearing about VPNs? If you don't already use a VPN service when surfing the web, you will relatively soon consider one as your next level of safety and security in the dangerous world known as the Internet.}

Door Prize Winners!

October 2021

Mary Ann Warner — Triangular safety light
Ralph Osinski — Screwdriver
Sharon Patrick — Sharpie set
Ron Linsley — Inspection beam flashlight
Paul Baecker — DVD set

Cautionary Tale About Free VPNs

By Joel Ewing, President
Bella Vista Computer Club (AR)
www.bvcomputerclub.org
president@bvcomputerclub.org

One of the caveats in the VPN article in the March 2021 Bits & Bytes (the Bella Vista Computer Club, Arkansas, newsletter), also mentioned at the March General Meeting, was that free VPN services were not recommended. As if on cue, see the following article recently published by Malwarebytes Labs on "[21 million free VPN users' data exposed](#)."

A hack of several free VPN services revealed that not only were some services collecting user activity logs in contradiction of their advertised policy, but some were also collecting email addresses, passwords that were not encrypted, IP addresses, mobile device models, and IDs.

The whole point of using a VPN with mobile devices is to avoid exposing non-encrypted data when using a public Wi-Fi network; but if that data would have been non-encrypted on a public Wi-Fi without VPN, then with a VPN service, it is still exposed non-encrypted within the server of your remote VPN service. In addition, if the service also requires a special app to be installed on the mobile device, then that app will also see any non-encrypted data before it is sent to the VPN service and potentially have access to other data on the mobile device. Thus, a free VPN service is much more likely to be tempted to exploit their access to non-encrypted data if that is their only way to profit from the free service.

One of the reasons for distrusting the security of a public Wi-Fi network is that you can never know whether or not it is supported by secure hardware or whether that hardware is configured correctly to at least make it as secure as possible. Because of the limited number of users on one Wi-Fi network, the motivation to expend much effort to hack that one network is not high. But, if it shares an exposure common to many other Wi-Fi networks using similar hardware, it could be at risk. Furthermore, the users have no way of knowing the details of a particular public Wi-Fi node, so it is wise to err on the side of caution. A VPN service, on the other hand, may have hundreds of thousands of users.

The possibility that a free VPN service may be engaging in questionable behavior and be holding sensitive user data on its servers makes it an extremely attractive target for hackers and data thieves, who can justify spending much time and effort to break in. That makes any collection of sensitive information by a VPN service a more serious concern. One of the suggestions made is that you should look for reviews of a VPN service by known and trusted organizations before deciding on a

(Continued on page 9.....Free VPNs)

(Bytes.....Continued from page 3)

thousand kilobytes. Those old 3.5-inch computer disks (remember them?) held about one and a half megabytes or about 220 pages of text. A CD-ROM (computer disk) could hold about 700 megabytes, that's over 400 of those old floppy disks and approximately 90,000 pages of text. It is good to remember that photos, depending upon the number of pixels in them, can be from 10 or 20 kilobytes up to 2, 12, 24, or more megabytes each! So, is a picture worth a thousand words? You bet, and more!

One GIGA-byte is one trillion bytes or one-thousand megabytes. Now we are talking serious (and very inexpensive) memory! You can buy a small portable USB drive (called a "thumb" drive or "flash" drive) in various gigabyte sizes – I tend to like the 32 or 64-gigabyte size because it can easily hold all my photos and documents as my backup. Just one gigabyte can hold almost 700,000 pages of text. That's a den full of books. One HD (high-definition) movie can take 2 to 5 gigabytes of memory. Movies and videos are moving pictures, of course, several pictures (or "frames") per second. Fortunately, the data used to store photos and movies are "compressed" or coded to take up much less space than you would expect.

One TERA-byte is one thousand gigabytes. For us ordinary people, this is a HUGE amount of memory! You can get a one-terabyte drive for about \$50. It can hold 300,000 photos or about 500 hours of movies. And, unlike my memory, it will never forget anything.

The next memory size up is the PETA-byte -- yup, one-thousand terabytes! And, no, they are not going to run out of prefixes. All just to store ones and zeros.

I use a nice little thumb drive to back up my memory, but I seem to forget where I put it!

This article has been obtained from APCUG with the author's permission for publication by APCUG member groups.



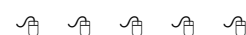
Just Forwarding The News...

News and/or Opinion from the Editor

In a local publication of news, it was reported earlier this Summer that, at a residence near Lakeside Mall in Sterling Heights, a resident claimed to authorities that personal possessions were stolen from his room.

The items missing were reported to be headphones and a KFC chicken meal, the latter of which had been in his refrigerator. However, moments later, the caller told police that the issue had been resolved.

Over and out.



Erasing Your Hard Drive — The Nuclear Option

By Bob Rankin

<https://askbobrankin.com>

My earlier article "[Erasing a Hard Drive? Not So Fast...](#)" delved into the difficulties of doing the job right. But now securely wiping a hard drive, or even a stubbornly data-persistent Solid State Drive (SSD), is easier than ever.

Did you know that the "delete" command doesn't really delete the target data? It only deletes the location of that data from the hard drive's index of files. Think of it as removing an entry from a library card catalog. The book is still there, but the "pointer" to its location on the shelf is gone, making it harder to find.

After a "deletion," the hard drive will re-use that file's space as if it was empty. But until data has been overwritten many times, it can still be recovered by a determined person. Military-grade standards call for overwriting each disk sector at least nine times before data stored in it can be considered truly "unrecoverable." That can take a long time, even on a relatively small 500 GB hard drive!

Securely erase your hard drive

There is a solution, and you probably already have it. The firmware of nearly every hard drive built since 2001 contains a "Secure Erase" command so effective that NIST (the U.S. National Institute of Standards and Technology) rates it as good as degaussing a hard drive - that is, using a powerful magnet to completely scramble the bits stored on a drive. So why haven't we been using "Secure Erase" for all these years?

Most BIOS developers disable the "Secure Erase" feature because they think consumers won't use it wisely. Indeed, "SE," as it's called, is a "nuclear option." It wipes data, and no amount of panicked, tearful phone calls to tech support or data recovery specialists will get it back. It even wipes data stored in bad disk blocks, something other disk-wiping utilities can't do. When Secure Erase finishes its job, your hard drive will be, as they say in Latin, "tabula rasa." In English, that means clean slate, squeaky clean, empty of all data, and ready to be used again.

Unlock the Power

A freeware utility called HDDEraser 4.0 unlocks the power of the Secure Erase feature in nearly every standard magnetic hard drive built since 2001. You can download it from the UC-San Diego's [Center for Memory and Recording Research](#), but note that no tech support is available and you use it at your own risk. Because it runs from a bootable disk, HDDEraser can erase any operating system, using the drive's own built-in sanitizer. Tim Fisher's [April 2021 review of HDDEraser](#) provides a little more insight into this powerful command-line utility.

The documentation for the program does not mention SSDs at all. But I've read in various places that HDDEraser will work on SSDs (solid state drives) in addition to traditional spinning magnetic hard drives.

There is one important caveat, though, according to SSD manufacturer Kingston Technology. HDDEraser can only be run on

hard drives that are directly attached to a SATA or IDE port, and not through a USB bridge or enclosure. Put more simply, HDDEraser will ONLY work on internal drive, and WILL NOT work on external hard drives.

Other Disk Wipe Options

I've mentioned [Darik's Boot and Nuke](#) (DBAN) in the past as one way to erase a hard drive. DBAN does a good job of erasing all accessible data on a drive, but it cannot access data that is no longer accessible through software, such as bad blocks, and it cannot detect or erase SSDs.

Another method of rendering a drive forever unreadable is known as "Encrypt, Reformat, Encrypt Again." Unlike other options, this WILL work on SSDs or an external drive. First, encrypt your entire hard drive; users running Windows 7 Ultimate, Windows 8.1 Pro, or Windows 10 Pro can use the built-in BitLocker utility, if their PCs include a Trusted Platform Module (TPM) chip. Another alternative for encryption is the [free VeraCrypt software](#), which works on Windows, Mac OS X and Linux computers.

Encrypting a working drive that contains lots of data may take many hours, but you'll be able to work on other things while encryption proceeds in background. Once your drive is encrypted, do a FULL reformat of it. A "quick" format only wipes the index of files mentioned above, leading the drive to treat the whole disk as empty space. A full format overwrites all data.

Next, encrypt the reformatted drive AGAIN before adding any data to it. This won't take long, because there is very little data to be encrypted. Now what do we have?

The re-encrypted, re-formatted drive has a security key that is required to decrypt data stored on the drive; the key is stored on the drive itself for BitLocker to access on the fly. The security key of the first encryption has been overwritten during reformatting and encrypted by the second encryption. Even if a hacker recovers the second encryption key, he can't recover the first one that might give him access to your old data. Now your drive is truly wiped and unrecoverable!

One more thing to consider is that some office photo copiers have a hard drive inside, which stores copies of the documents that pass through the machine. Consider what private or confidential information might be stored there, when disposing of a copier, or returning a leased machine.

Shake and Bake? Or the Total Annihilation Method

One person told me that placing a hard drive in the oven at 400 degrees for an hour would melt the coating on the disk platters, making the data unreadable. I would not advise that, or using any type of torch, as toxic fumes would likely be released.

It's good clean fun to use a drill press or sledge hammer on an unwanted hard drive (with the appropriate safety equipment). But if you lack those tools, a commercial hard drive shredding service will do the job. [Ameri-Shred](#) is one company that offers the service (see their shredding tool video [here](#)).

This article is republished, with permission, from the Ask Bob Rankin web site.



Beware Of The “Auto-Renewal” Option In Your Security Software

News and/or Opinion from the Editor

If your ISP is Comcast — that is, if you subscribe to Comcast as your *Internet Service Provider* — then you might recall that Comcast stopped supplying you with a free subscription to the excellent Norton Security software product for your computer at the end of 2020. Then you were left to fend for yourself by having to choose your own security path forward. Some of you might have accepted the economical \$15 one-year option arranged by Comcast with NortonLifeLock (the company that publishes Norton products since it changed its name in 2019 from Symantec). That was a rather good choice — an excellent security product at a good price. Anyway, when you purchased that one-year software coverage, you also agreed to an auto-renewal price for a second year of coverage at \$105. That is an outrageous price for a year of security software, no matter how good it is or isn't. So, before the company charges the card they have on file in your account, you need to deactivate the auto-renewal option. This is relatively easy to accomplish in your Norton account (go to my.norton.com and log into your Norton account and find the option to deactivate the auto-renewal option).

The following applies to most any security software that you might purchase for your computer these days, whether because you are a Comcast subscriber or not, and whether you use a Norton product or something else.

These days, retail security software purchases typically come with an auto-renewal agreement. You buy the product and the software publisher will auto-renew their software on your PC when the 1-year license is about to expire, for another year. The price for the second (renewal) year will most assuredly be much higher than what you paid for the first year, and also higher than it will cost for the same software if purchased new a year later (not as an auto-renewal). Read the small print in the account that you created with the software publisher to find out for sure. You would be wise to cancel (deactivate) any auto-renewal agreement at least a couple of months before it would go into effect. They will hope that you will have forgotten that you gave them your authority to rob you blind almost a year later.

I've bored you with this before, but personal computer security software is highly competitive, and so are the prices for the various brands and models of the many offerings.

So what do you do when the renewal time comes?

When your present license year expires, just purchase a new license for whatever product you want to use for the next year (either of the same product or switch to a dif-

ferent one), and the day after the current one expires, install and activate the newly purchased security product. If you choose a good security product, you will have another year of protection, but you will have saved oodles of bucks in the process. The best places to purchase security software on sale are at Newegg.com (my fave) and Amazon.com, and occasionally at local computer stores and office-supply stores during holiday sales. Typically, a 1-year 3-PC license for a quality security software product might cost around \$20-\$25 on sale, and a 1-year 5-PC license might cost around \$30-\$35 on sale. Paying much more than that is akin to highway robbery, so avoid it. When you see a good price, take it and store the product until you are ready to install it and use its license. Share (or sell) the extra licenses with friends/relatives, if you purchase a multi-PC pack.

When you shop for PC security software, do not settle for so-called “anti-virus” products. Select instead a more robust so-called “Internet Security” product, which (depending on the brand) may include additional features such as ransomware/phishing/spyware protection, parental controls (for the little tykes that might come visiting), enhanced firewall and financial security, VPN service, and who knows what else (check the product's web page for its details). And for only a pittance more.

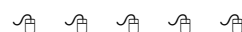
Whether you purchase your security software on the web or in a local store, you will probably be required to create an account with the publisher of the software. In most cases they will require a credit card to be included, for the auto-renewal process to be enabled. Check the small print on the package or on their web site for details on how the particular publisher handles this. Perhaps search the web for **xxxx auto renewal**, replacing the **xxxx** with the name of your chosen security software.

The whole purpose of this discussion is to get you to pay attention to the current agreement that you probably ‘signed’ when you purchased your security software, and to make sure that you don't let the publishing company take advantage of your wallet.

You can avoid all of this nonsense if you choose to use free security software or choose to use Windows Defender (also free). In my opinion, you get what you pay for. Read reviews of the free offering that you are considering, and decide whether it is enough coverage for your purposes. But sufficient security is the most important aspect of computing, especially when connecting to the dangerous entity known as the “Internet”. Let caution — and your safety/security/privacy — be your guide. But for now.....

Check the auto-renewal option in your security software agreement, and account, TODAY!!!

Questions?
Just ask.



Pay Close Attention When You Are Offered A Cookie Selection

News and/or Opinion from the Editor

As I was preparing an article for this WYSIWYG issue, I visited a few web sites of software publishers, and noticed a web site feature (actually, more like a “condition”) that is becoming more prevalent recently.

It concerns cookies. Lately, you may see a statement when you arrive at a web site, informing you that they use cookies to ‘improve the user experience’ on the site. Well, maybe so, but that’s just part of the purpose. Sometimes you can ignore this privacy invasion attempt (if it allows you to), but it is totally legal. You get to choose if the web site is important enough to you to accept their cookie(s), or surf elsewhere.

But more recently, I see web sites which offer you some sort of selection of cookie types, and the ability to opt-out of *some* of them. This column is about the series of pop-up cookie announcement windows that one web site offered to me when I arrived at their site. I’ve hidden the web site’s name, simply because so many other web sites are acting similarly.

First, the quick push to just accept that I was doomed to take what they were forcing onto my PC.

We value your privacy

By clicking “OK” you allow cookies that improve your experience on our site, help us analyze site performance and usage, and enable us to show relevant marketing content. You can manage cookie settings below. See [Cookies Policy](#)

OK

Manage...

Sure, “we value your privacy”, so they’re at least *telling me* that they’re going to track me with cookies. Click **OK** if you trust them, or if you just don’t care (notice that it is colored to attract your initial attention). Click **Manage** if you are curious. Be curious!!! I was curious.

Privacy preference center

By clicking “Accept all” you allow cookies that improve your experience on our site, help us analyze site performance and usage, and enable us to show relevant marketing content. You can manage cookie settings below. By clicking “Confirm selection” you agree with the current settings. See [Cookies policy](#)

Manage consent settings

Necessary cookies

Always Active ▾

Necessary cookies help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies.

Their series of *Privacy Preference Center* selections opens, to explain the many types of cookies that will be placed on your computer (into your web browser), if you allow them. But at least they are giving you *SOME* choices.

“*Necessary cookies*” — “always active”, they tell us, because the web site can not function properly without them. Well, maybe. Moving along down their cookie list....

Preference cookies



Preference cookies enable a website to remember information that changes the way the website behaves or looks, such as your preferred language or the region that you are in. De-selecting these cookies may result in improper functionality and setting of the website.

Performance cookies



Performance cookies help us improve our website by analyzing how visitors use it and interact with it. De-selecting these cookies may result in poorly-designed content and slow site performance.

Marketing cookies



Marketing cookies are used to track visitors across websites. The intention is to display ads that are relevant and engaging for the individual user and thereby more valuable for publishers and third party advertisers. De-selecting these cookies may result in seeing advertising that is not as relevant to you.

Targeting cookies

These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information, but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

“*Preference cookies*” — “your preferred language or the region you are in”.

“*Performance cookies*” — “analyzing how visitors (you!) use the web site and interact with it”.

“*Marketing cookies*” — “used to track visitors and display ads that are relevant and engaging to the individual user (you!), and therefore more valuable for publishers and third-party advertisers”. Third-party advertisers are companies, organizations, or individuals who pay web sites to be able to piggy-back their cookies onto your PC through the host’s web site. Your cookie cleaning software will show you web sites that are tracking you, but where you have never visited.

So here is where YOUR control comes into play. The small dots in the sliding bars allow you to enable or disable those selections by clicking on the dots. The dots will toggle on or off (right or left, colored or ‘greyed-out’) as in this example:

Preference cookies



Preference cookies enable a website to remember information that changes the way the website behaves or looks, such as your preferred language or the region that you are in. De-selecting these cookies may result in improper functionality and setting of the website.

The obvious action would be to opt-out of every cookie that you can (disable it/them) in this manner. At the bottom of this opt-out window, you then click the button to confirm your selections.

Confirm selection

In summary, take control of YOUR privacy (on or off the web) and opt out of any tracking that you see happening when you can.

By the way — after opting out of ALL of these optional cookies, the web site still worked just fine for me.



Web Page Reviews

Collected by Paul Baecker — webwatch@sterlingheightscomputerclub.org



This column attempts to locate sites containing valuable, amusing, and free content, with no overbearing pressure to purchase anything. **Our club members only** are encouraged to submit favorite sites (a description is optional) to the e-address noted above, for inclusion in a future WYSIWYG issue. Also check the SHCC web site (“Web Page Reviews”) for previous gems.

38 popular text shortcuts and Internet **slang terms** to know. <https://www.maketecheasier.com/internet-slang-meaning/>

What happens if you don't **shut down** your computer properly? (6-min. video, but ignore the long ad at the end) <https://www.youtube.com/watch?v=3TovcF1j3bE>

Find organized and advertised book sales in your vicinity. <https://booksalefinder.com/>

Tutorial shows you how to install Ubuntu Desktop on a **Raspberry Pi 4** device. <https://itsfoss.com/install-ubuntu-desktop-raspberry-pi/>

Difference between **apt** and **apt-get** commands of Linux. Also lists some of the most commonly used apt commands that replace the older apt-get commands. <https://itsfoss.com/apt-vs-apt-get-difference/>

Dark Web Price Index 2021 — understand what your personal information is worth and why you should protect it. <https://www.privacyaffairs.com/dark-web-price-index-2021/>

It's important to understand how to **manage directories** in your OS. If you're new to Linux, this article shows how to delete a directory. <https://www.maketecheasier.com/delete-directory-linux/>

Why “**long-pressing**” the power button could damage your system <https://www.howtogeek.com/747587/why-long-pressing-the-power-button-could-damage-your-system/>

Have you seen the TV ads for the “**Robokiller**” phone app? Here is a luke-warm review of this robo-call killing service. <https://www.komando.com/smartphones-gadgets/robokiller-heres-what-we-liked-and-didnt-like/545200/>

When does **cable-length** matter? (6-min. video -- ignore the long ad at the end) <https://www.youtube.com/watch?v=p9nqQuu4lmQ>

How much is your hacked info worth on the **Dark Web**? <https://www.maketecheasier.com/hacked-info-on-the-dark-web/>

Running a train in the Linux terminal to amuse your friends/family. <https://itsfoss.com/ubuntu-terminal-train/>

Why does YouTube have ads? 5 ways to block them! <https://newsandshit.com/why-does-youtube-have-ads/>

In 2018, **Spotify** filed a patent that would essentially allow it to make music suggestions to you *based on your emotional state, gender, age, social setting, or even accent*. It was approved in January 2021. What does this mean for you? What info does Spotify collect about you? <https://www.makeuseof.com/spotify-data-collection/>

How does **CAPTCHA** really work? Also learn how Google's version measures how you use your mouse! (7-min. video, but ignore the long ad at the end) <https://www.youtube.com/watch?v=MWu2UjLLJI8>

NOTE: Many of the links in the digital newsletter connect to the Internet if clicked. For those that do not, copy and paste the link into your Internet browser.



Web Watch Column on the Club Web Site

Check out the **WebPageReviews** section on the club's web site. There you can see past web sites reviewed in this column. They are arranged into various **keyword** categories to help locate a specific topic or site.