



THE WYSIWYG



September 2021

Volume 33 Issue 7

STERLING HEIGHTS COMPUTER CLUB

PO Box 385

Sterling Heights, Michigan 48311-0385

**MAIN MEETING:
TUESDAY SEPTEMBER 7
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	3
Is Your Email Address Vulnerable To Spammers? // Bald-faced Hornets	4
Suspicious Activity on Your Account? // How Healthy Is Your PC Battery?	5
The Biggest Myths About Techies and Tech Enthusiasts	6
Your Cost for PC Security	7
How Latency Can Make Even A Fast Internet Connection Feel Slow	8
What is Network Congestion, and How Can You Work Around It?	9
How to Archive Facebook Posts (without Deleting Them)	12
Web Page Reviews	13 & 14

This Month's Main Meeting Topic:

We are very pleased to be able to meet in-person again, following a long year of Zoom-based meetings.

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.*

Of course you may wear a face mask in the meeting, but the Church does not require them (as of this newsletter print date).

This month's presentation has not yet been determined as of newsletter press time.

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 March 2019 meeting).

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

Two-Month Meeting Schedule

September 2021	October 2021
7 - SHCC Main Meeting	5 - SHCC Main Meeting
12 - SEMCO meeting	10 - SEMCO meeting

Newsletter submissions are due 10 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

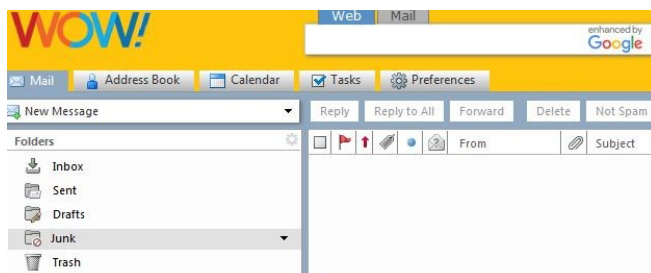


Do you have WOW as your ISP and use email in your WOW web-based account? I do and my wife does also. Even if you use a different ISP the ideas below could apply.

My wife and I each run Thunderbird (a free "email client", similar to MS Outlook) which I configured to download (to Thunderbird) and delete the email in our WOW email inboxes. For this reason I never log into the WOW web site from home, only on travel. Back a week or so ago it became apparent to me that I was not receiving all my emails in the Thunderbird program. My wife had already commented about missing emails and I initially assumed she was doing something strange. But after a while I thought I'd check my email account on WOW. To my surprise there was a lot of email in the "Junk" folder. I, on purpose, have never set up any spam rules at WOW because I manage unwanted emails with Thunderbird's "Message Filters". This is easier for me because I'm in my email (using Thunderbird) most days and the "Message Filters" are a click away versus logging into WOW. The other advantage to doing these rules in Thunderbird is if I choose to change my ISP provider my Thunderbird email client will move with me and WOW rules would be lost.

I looked all over and finally concluded that WOW (big brother) was "helping" all their customers and running spam filters before emails were presented to the customer accounts. There is no way for a customer to turn off WOW's interference with their email. I complained to WOW about this and as of now have not received a reply to my complaint.

When I clicked on the "Junk" folder to view the emails in it, most or all of the emails were definitely not junk or spam. I selected all the emails and moved them to the "Inbox". I then logged into my wife's email and did the same thing. Unfortunately, I did not specifically note the earliest date of emails trapped in "Junk", but it was about the beginning of July. I did this again later that day and sure enough there were more emails in "Junk". While I had the "Junk" folder selected and there were emails in it, I noticed a button "Not Spam". With no emails in "Junk", this button is grayed out as shown below.

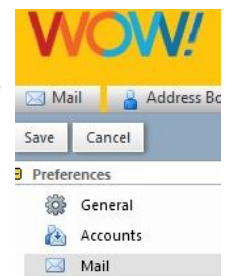


Selecting all the emails in "Junk" and clicking the "Not Spam" button moved all the emails to the "Inbox" which was a little easier and quicker than my original method.

Not believing that there was no permanent solution to our email issues, I hunted a couple more times for relief to big brother's heavy-handed actions. I finally found a solution though, in my opinion, it's a little indirect. When in WOW email you see a "Preferences" tab.



Click "Preferences" and then on the left, click "Mail".



Use the drag bar on the right to move down to the "Access from Other Mail Clients" section. Here click the "Incoming Junk Messages" check box.



What this does is when your email client (Thunderbird) checks your WOW inbox, the WOW email server software also provides your email client with the emails, if any, that are in the "Junk" folder.

Initially I ignored the section "Access from Other Mail Clients" because I was not using another email client; I was only using WOW email. This approach works, but my "Junk" folder is not another email client; it is a part of my WOW email.

It would make more sense to me to include something in the "Receiving Messages" section of "Preferences". What would make things even clearer is put a "Turn off WOW email filters" check box in the "Spam Mail Options" section.



Is Your Email Address Vulnerable To Spammers?

By Bob Rankin
<https://askbobrankin.com>

Spammers, scammers, and other cyber-miscreants appear to have supernatural powers that enable them to guess email addresses accurately and quickly. But in reality, the bad guys harvest email addresses by pretty mundane means. YOU may even be contributing to the problem without realizing it. Let's dig in to this problem to see what can be done to limit the flow of digital canned lunch meat.

Using web-crawling "spider" programs (similar to the ones search engines use to

index Web pages) some spammers hunt down email addresses by looking for the telltale "@" symbol. Working swiftly and ceaselessly, spiders can harvest millions of email addresses automatically. To avoid being "bitten" by an email harvesting spider, don't put your email address on public spaces on the Web. That means not posting it to online forums or personal web pages. If it's included in online directories (school, work, clubs, etc.) ask to have it removed.

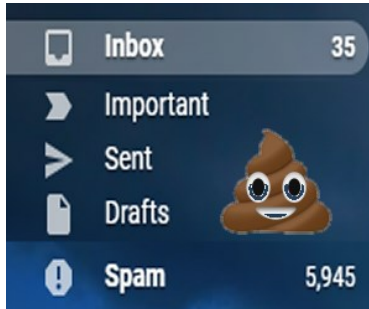
Do a Google search to see where your email address is available, and work towards becoming invisible. (Tip: enter your email address in the Google search box enclosed in double quotes.) If you must make your email address visible in public, you can obscure your address by avoiding the "@" symbol, i.e., use "joe at schmoe dot com" instead, or create an image with the address instead.

How Do Spammers Get My Email Address?

"Dictionary attacks" are another way to collect email addresses. This method, which combines common words with popular domain names, relies on the fact that you don't need a valid email address to generate an outgoing email. Spammers generate emails to computer-generated addresses, accepting millions of bounce-backs in exchange for a handful of replies from valid addresses. That's why the first rule of dealing with spam is "don't reply to it." Doing so just tells the spammer that you are a "live one" and worth hitting with more spam. Delete that unwanted message, or banish it to the Trash folder.

You can make it harder for a dictionary attacker to guess your address by NOT choosing any combination of dic-

(Continued on page 5.....Spammers)



Club Officer Election Announcement and Officer Duties

Our SHCC officer elections are held at the 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 will be sending an email to you, 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 will be open at the September, October, and November meetings. Elections occur in November (after nominations are closed) for a term in the next full calendar year.



Bald-faced Hornets

News and/or Opinion from the Editor

A few years ago the siding on my house was invaded by buzzing insects, which later were identified as bald-faced hornets. My feeble attempts to eradicate them with hornet-wasp spray cans failed. Later I learned that the only critters affected were those on which I hit a direct bull's eye with my can pointing. There was no lingering chemical to infect the rest, or the nest.

Eventually the traffic got pretty heavy, so I employed a popular pest service, which had to visit twice to complete the job. During the 3 weeks between visits, half a dozen of the little beasts found their way into the house (one took up residence in a shoe that I was about to use).

See the skin-crawling activity in a hornet's nest in a couple of videos in the WebPageReviews on page 14.



(Spammers.....Continued from page 4)

tionary words, common first or last names, and a string of numbers. If your email address is smith123@aol.com or susie90210@gmail.com I can guarantee that you'll get loads of spam, no matter how careful you are. Those addresses are just easy targets, because they're so easy to guess.

Margaritaville? Huh?

With apologies to Jimmy Buffett, some people claim that there's a hacker to blame, but you know, it's your own damn fault sometimes. Many people simply hand over their email addresses, no questions asked, just to get access to a game, contest, some free program, a ringtone, or other supposed "valuable prize." It's a good idea to have a "throwaway" email address that you can enter into Web forms, rather than using your everyday address. See my related article [Fight Spam With a Disposable Email Address](#) for more tips on how to protect your inbox.

And if you have an email password that's easily guessable, spammers may hack into the email account and steal all of the contacts stored there. If your computer is not adequately protected from viruses, spyware and phishing attacks, all of the people in your email address book are vulnerable to spam attacks as well. See my article [Here's the END of Weak Passwords](#) for help picking a secure password.

I'm pretty sure that email "forwards" play into the hands of spammers, because they accumulate a large number of addresses as the message spreads from one person to another. For a while, I wasn't sure how this worked, because I didn't see an easy mechanism for those bloated messages to wind up in the hands of the the spammer. But then I realized that if even one of those recipients had their email hacked (or computer compromised by malware), the entire trove or addresses would be vulnerable.

This may or may not be a major source of email address harvesting, but at the very least, you must agree that blindly forwarding every silly story doesn't contribute anything positive to the Internet. Cambodian midgets fighting lions? Nigerian prince wants your help transferring millions? Really?? If you're tempted to forward something that seems dubious, check it out on [Snopes](#) before hitting the Send button. If you don't trust Snopes, use another myth-busting or fact-checking site such as [TruthOrFiction](#).

Along those lines, I cringe whenever I get an email that includes my address, along with dozens of others, in the TO: or CC: line. It's especially irksome when they come

(Continued on page 10.....Spammers)

Suspicious Activity on Your Account?

News and/or Opinion from the Editor

Do you get those annoying "suspicious activity on your account" phone calls? They are very common. They are often claiming that your Amazon account has been charged an exorbitant amount for some sort of order that you really never made. I recall that these calls to my phone number started at \$299, but today's call hit \$1,499. They are really trying hard to get my attention and to get me to pick up the phone and cooperate with their 'investigation'. What's going to happen if I do converse with these fools? They will ask me for my financial credentials — maybe a credit card, or maybe an account I have with Amazon (after all, anyone who buys on Amazon has an Amazon account). What can they get in my Amazon account? Perhaps a credit card number and expiration date and PIN, if I have not deleted that info from the Amazon site.

Some folks still fall for this scam, so this caution bears repeating. If you have any concerns about calls of this sort, call the bank that controls your credit card account, and inquire about anything that looks suspicious. Each time I've chosen to inquire (which isn't often anymore), the folks there have been very courteous and helpful.

Just DO NOT converse with the scammers, whether on the phone or in email or even in 'pop-ups' that might display on your computer/tablet/phone screen. Don't answer their phone calls. NEVER give out any personal or financial details to anyone whom YOU have not contacted *first!*



How Healthy Is Your PC Battery?

News and/or Opinion from the Editor

Over time, the battery in your laptop loses its charging capability. I recently checked the laptop of an acquaintance, and discovered that it only operated at 47% of when it was new just 5 years ago (meaning that it only charged to less than half of its original capacity).

Several web sites and battery sales representatives suggest 'exercising' the battery of any device that allows it, including computers. How to accomplish this? Simple. Unplug the device from A/C power (usually the wall power socket in the home or business), and use the device until the battery meter informs you that the battery is down to around 15-20% of its charge. Often, the device will warn the user on-screen when the battery's power capability gets that low. Then just plug the device back into the A/C power source until it is at least 80% charged. Many 'experts' suggest not running any device all the time on A/C, resulting in the battery always being 100% charged and affecting the battery's 'memory'.

See the two web sites in WebPageReviews (on page 13) to learn how to monitor your battery in Windows and in Linux. Apple discusses battery health on several of their pages.

But nevertheless, these batteries should be exercised *at least* every three months to get the maximum life and support possible. Exercise yours today!



The Biggest Myths About Techies and Tech Enthusiasts

By Johnathan Jaehnig

<https://www.makeuseof.com>

There's a certain depiction of tech enthusiasts out there that doesn't always track to real life. When you write for tech publications, you meet a lot of tech enthusiasts and learn pretty quickly that not everything we're lead to believe about techies is necessarily true.

So, let's tackle a few of the big myths about technophiles.

1. All Techies Like All Technology

One of the most common misconceptions is that people who spend a lot of time working with technology like technology for the sake of technology.

Sure, there are people out there who live to find technically complex solutions to technically simple problems. However, a lot of people really get behind a technology because it enables something else that they're passionate about, not because they like the technology itself.

In fact, many people who spend a lot of time working with technology are close enough to it to understand when it becomes obstructive or even dangerous. Perhaps nothing speaks better to this than the number of popular media representations we have of a future in which technology has led us astray.

2. All Techies Understand All Tech

Another common misconception about technophiles is that all of them know how to do everything tech-related. For example, in television and films, it's common for a techie to be the master of all things automated, but this is seldom the case in real life.

Expecting someone who likes one area of technology to be fluent in all technology is like expecting someone who watches films to like all films. Like some film fans might like romantic comedies and detest horror, some tech fans really enjoy virtual reality but don't care about blockchain.

This has to do with our first misconception. Someone who is really familiar with a technology is usually using that technology to do something else. They won't care about technologies that don't allow them to do that thing.

There are universal "technologists" who are interested in any and all technologies, but many tech users have their niche interest just like anyone else.

3. All Techies are Socially Awkward

The "techie" character in a television show is often depicted in two ways: as a loner or as a member of a clique with other tech enthusiasts. Unfortunately, this is also predicated on the usually incorrect assumption that technology is the only interest that the tech user has.

This also may simply be an anachronistic depiction that we as a culture have chosen to hold onto. This is the way that techno-centric characters were commonly depicted in television in the '90s. Think characters like Urkel and Screech. Of course, this was at a time before all of us had computers in our homes, let alone in our pockets.

Still, this trope has carried on into modern and contemporary programs like "The Big Bang Theory". Why? Because it's always been done that way.

A closely related myth is that tech enthusiasts are unpopular. This misconception may have a complicated origin.

The two big threads in the geek/nerd narrative (lacking social skills and liking science, technology, engineering, and mathematics) are both common to autism. Books and resources on autism commonly point this out, as does this poorly-aged article from WIRED, which, to be fair, cites Tony Atwood, who remains a leading expert on autism.

This isn't to say that the relationship is necessarily one-to-one. Not all technology enthusiasts are on the spectrum, and not everyone on the spectrum is a technology enthusiast. However, to some degree, these identities may have been accidentally conflated in many representations of both groups.

4. Techies Are Uncool (and How They Became Cooler)

The good news is that, as pointed out above, the things that made tech enthusiasts uncool became mainstream. Cultural crazes that used to be the realm of the geek suddenly became pop-culture giants enjoyed by everyone.

Not only did techie things become cool, but people also started realizing that techies themselves are cool. The Urkels and Screeches of the world stopped screwing up and started saving the day, even if they retained their less socially suave depictions.

In 2002, the inventor and super genius Wade helped save the world from a computer chair in Disney's "Kim Possible". In 2007, the same year that the iPod Touch and iPhone launched, Zachary Levi began playing the title role in NBC's "Chuck". At the head of The Nerd

(Continued on page 7..... Techies)

Your Cost for PC Security

News and/or Opinion From the Editor

As we use our computers with the Windows, Apple, or Linux operating systems, security should be our prime concern. We need to keep our devices (computers, tablets, smartphones), and in turn ourselves, protected from the vast variety of threats that populate the web. Even if we choose to connect to the web just to read email or download a document or software program, we are immediately exposed to that dangerous environment known as the Internet. In addition to just common sense (decisions as to where we travel on the web and what we read, watch and do out there), using quality security software helps us along the way.

In my conversations with so many other computer users, I have become aware of the false impressions many of them express that security software needs to be purchased directly from the software's publisher or in a retail store, each often at a premium price. But there are other more money-conscious ways to acquire many of these same products. And any dollars that can be saved here can be spent on other PC accessories, such as flash drives and external hard drives (or services, if you choose) to protect the valuable programs and data files that we have amassed on our devices.

But it's easy to protect our computer systems, by selecting and installing a quality security software package. Microsoft Windows includes security software, known as "Windows Defender" (and sometimes referred to as "Windows Security"). Articles on the web that compare security software choices are often in disagreement as to the quality of "Defender". I choose to acquire software products that are '*dedicated to a particular purpose*', whether they are free (usually) or at cost, so I often choose to use/purchase so-called "third-party" (meaning not from the computer's or the operating system's manufacturer) software packages for most of my computing needs, and that includes security software for my Windows PCs. Windows Defender is certainly a decent free option, but I want the extra degree of protection and certain options that are available in some non-Microsoft security software.

How to choose security software is not too difficult, since there are quite a few high-quality choices available for purchase. *For purchase?* But what about "free" opportunities? And what about those constant reminders you get that they offer a paid version as well -- so, what is really missing in a free version? In my opinion, with security, you pretty much get what you pay for. Look at the small details of what a good *free* product gives you versus a good *at-cost* product. For less than \$2.50/month, I believe that free choices just aren't worth it. Good, perhaps; great -- well, your research will help you with that decision. Two presumably-unbiased places on the web to help with your decision are **AV Test** and **AV Comparatives** (also can be found in the WebPageReviews section of your SHCC web site). Each site tests various security softwares *multiple times each year* to arrive at the best of the current bunch. And there are so many articles on the web, comparing the

various security products, but be aware of potential motives for recommending one product over another -- try to determine whether the article you are reading is really unbiased (sometimes difficult to do -- some web sites do deserve to be trusted). (My recommendation: Stay away from Avast's free offering due to their past anti-privacy practices, and also avoid the terribly poor-performing PC Matic product.)

But how much should you PAY for security software? Many local stores 'push' certain software titles. How do they select what to 'push' on customers? How do retail establishments in ANY shopping environment choose what to 'push' to their shoppers? Decisions on quality? Or perhaps decisions on what the manufacturers and suppliers of those pushed products are paying the retail stores to push them? (I think that this is called "payola" in the music industry.) You'll probably never really know. But you can do your own homework to arrive at a fine security product that matches or exceeds those pushed products. These pushed products are certainly at least satisfactory in their protection support, but are they the best for your money? And are the prices at local stores competitive?

(Continued on page 11.....Cost)

(Techies.....Continued from page 6)

Herd, the computer augmented IT guy regularly saved the world.

The trend is true for films as well. In 2001, "A Beautiful Mind" told the dramatized but mostly true story of mathematician John Nash, played by Russel Crowe. In 2014, Benedict Cumberbatch played real-life super-nerd Alan Turing in "The Imitation Game." That same year, Eddie Redmayne played Stephen Hawking in "The Theory of Everything."

In all of these shows and movies, it's the math, science, and technology figures either saving the world or at least helping us to understand it. Some of them perpetuate some of the stereotypes and misconceptions that this article has detailed. Still, the films, in particular, do so in a way that is nuanced, humanizing, and realistic.

After All, Who Isn't a Tech-Enthusiast These Days?

You may have some typical ideas about "techies." Some of them may be based on general truths, and some of them might not be.

The takeaway is that tech enthusiasts and experts aren't cut from a single cloth. Fortunately, the way that we as a culture represent and understand this group is changing for the better. After all, who of us can avoid being tech experts these days?

This article is republished, with permission, from the MakeUseOf web site.



How Latency Can Make Even A Fast Internet Connection Feel Slow

by Chris Hoffman

<https://www.howtogeek.com>

There is more to an Internet connection's speed than just its bandwidth. This is especially true with satellite Internet connections, which can offer speeds of up to 15 Mbps – but will still feel slow.

Latency can be an issue with all Internet connections and networks. Wired network connections tend to have the lowest latency, while wireless connections generally have higher latency.

Latency vs. Bandwidth

Internet connections, including satellite Internet connections, are advertised with speeds like “up to 15 Mbps.” You may look at a satellite Internet connection offering this speed and assume the experience of using it would be comparable to the experience of using a 15 Mbps cable Internet connection, but you would be wrong.

- **Bandwidth:** Bandwidth determines how fast data can be transferred over time. Bandwidth is the amount of data that can be transferred per second.
- **Latency:** Latency is delay. Latency is how long it takes data to travel between its source and destination, measured in milliseconds.

Latency in the Real World

Let's say you are browsing the web on different types of connections. Here's how latency would “feel”:

- **Satellite Internet Connection (High Speed, High Latency):** You would click a link on a web page and, after a noticeable delay, the web page would start downloading and show up almost all at once.
- **Theoretical Connection (Low Speed, Low Latency):** You would click a link on a web page and the web page would start loading immediately. However, it would take a while to load completely and you would see images load one-by-one.
- **Cable Internet Connection (High Speed, Low Latency):** You would click a link on a web page and the web page would appear almost immediately, downloading all at once.

Latency always manifests as a delay. For example, if you are having a Skype chat with someone on a high-latency Internet connection, you would be out of sync with each other. You would have to pause in between sentences or you would end up talking over each other thanks to the delay.

If you were playing an online game, your actions would be delayed and events happening in the game would have a noticeable delay before they reached your computer, rather than feeling near-instantaneous. For example, if you were playing a first-person shooter game on a high-latency connection, you would shoot at someone on your screen, but

the delay means they would be long gone by the time your projectile got there.

What Causes Latency

Both bandwidth and latency depend on more than your Internet connection – they are affected by your network hardware, the remote server's location and connection, and the Internet routers between your computer and the server.

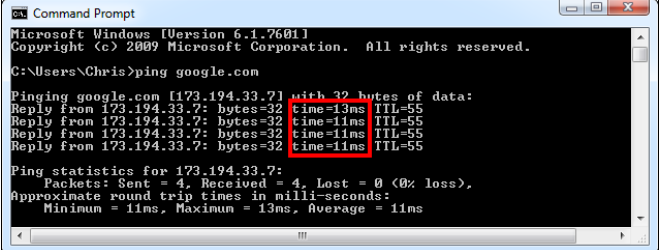
Packets don't travel through routers instantly. Each router a packet has to travel through introduces a delay of a few milliseconds, which can add up if the packet has to travel through many routers to reach the other side of the world.

However, some types of connections – like satellite Internet connections – have high latency even in the best conditions. It generally takes between 500 and 700ms for a packet to reach an Internet service provider over a satellite Internet connection.

Latency isn't just a problem for satellite Internet connections, however. You can probably browse a website hosted on another continent without noticing latency very much, but if you are in California and playing an online game with servers located in Europe, the latency may be more perceptible.

Measuring Latency

You can measure the latency between your computer and a web address with [the ping command](#). In our example, it takes 11 milliseconds for traffic to go between our computer and Google's servers. If we had a satellite Internet connection, this could be as high as 700ms.



```

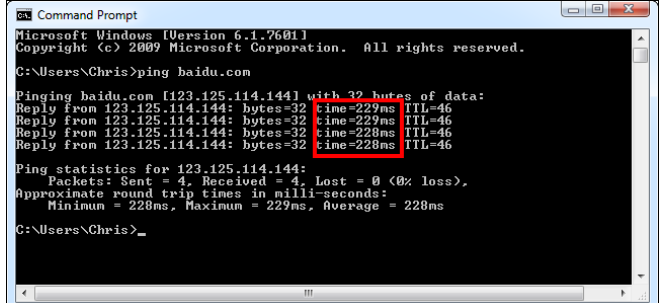
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Chris>ping google.com

Pinging google.com [173.194.33.7] with 32 bytes of data:
Reply from 173.194.33.7: bytes=32 time=13ms TTL=55
Reply from 173.194.33.7: bytes=32 time=11ms TTL=55
Reply from 173.194.33.7: bytes=32 time=11ms TTL=55
Reply from 173.194.33.7: bytes=32 time=11ms TTL=55

Ping statistics for 173.194.33.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 13ms, Average = 11ms
  
```

To show the impact of distance on latency, we can ping Baidu – a Chinese search engine. Baidu doesn't have any servers in North America, so our computer has to communicate with its servers in China. The latency between our computer and Baidu's servers is 228ms.



```

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Chris>ping baidu.com

Pinging baidu.com [123.125.114.144] with 32 bytes of data:
Reply from 123.125.114.144: bytes=32 time=229ms TTL=46
Reply from 123.125.114.144: bytes=32 time=229ms TTL=46
Reply from 123.125.114.144: bytes=32 time=228ms TTL=46
Reply from 123.125.114.144: bytes=32 time=228ms TTL=46

Ping statistics for 123.125.114.144:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 228ms, Maximum = 229ms, Average = 228ms

C:\Users\Chris>
  
```

(Continued on page 10.....Latency)

What is Network Congestion, and How Can You Work Around It?

By Michael Franco

<https://www.howtogeek.com>

Congestion is never good. Whether it's on the roads, in your lungs, or plaguing your home's internet connection, it's best eliminated. Here's what you need to know about **network congestion** and what you can do to deal with it.

What Is Network Congestion?

Put simply, network congestion involves too many transmissions traveling over the internet at once. Doubtless, you've heard the internet referred to as "the information superhighway," and this is a common (and handy) way to think of its functionality. So, network congestion is like a traffic jam.

When you do something on the internet, like Google a fact, read the news, or buy something from an online retailer, the data involved in the transaction gets divided into packets—think of these like cars on a highway. Those packets zip along the most efficient routes on the internet to reach their destination. Then, the computer or server receiving the data reassembles the packets into a cohesive message and responds appropriately.

To route all of this traffic, a system known as TCP/IP (Transmission Control Protocol/Internet Protocol) is used. This system establishes a connection between the transmitting and receiving computers or servers known as a handshake. Once the handshake is established, data packets can begin flowing. The TCP/IP protocol has an in-built error detection mechanism so that if one end of the connection detects an error in one of the transmission packets, it will request a replacement packet.

So, if you think of each packet as a car on the information superhighway, you can begin to understand how at peak times, internet traffic can lead to congestion. Not only do initial transmissions involve packets, but also, errors lead to more packets being transmitted, which increases traffic even more.

Why Congested Networks Are Slower

Again, just like traffic on a road, all of those packets traveling along the various routes that comprise the internet can lead to slowdowns in your surfing speed. Your internet service provider (ISP) only has so much bandwidth that it can offer customers. When it's all being used at once, those data packets simply take longer to make their way to and from their destination, so your connection will begin to lag.

You might have noticed that your internet speed occasionally slows down between the hours of about 6 and 11 p.m. In keeping with the traffic analogy, this is known as "internet rush hour," and is the time when people are getting home from work, hopping online, and beginning to place a big demand on the internet. Emails are checked,

shopping is done, and bandwidth-intensive activities like gaming and streaming video content get underway.

Of course, now that more and more people are learning and working from home, congestion can really take place at just about any time of the day.

Congestion at Home

Network congestion doesn't only happen at the ISP level, but at your home level as well. If you have too many devices in your home using your bandwidth, you could experience slowdowns as well. If the internet is a superhighway, then the bandwidth pipeline to your home is like your driveway. If too many people are trying to pull in or out at the same time, congestion is bound to happen.

What You Can Do About Network Congestion

If you're noticing reduced internet speeds due to congestion on your home network, there are a few things that you can try.

The first step is to check what speed you're actually getting by using a free speed-test service like fast.com. Try the test a few times a day, write down the numbers that you get, and take the average. Then, check with your ISP plan and see whether the values match up with the speed that you're paying for. If they don't, call your provider and let them know. They might tell you that you have an older router or modem that needs to be upgraded. If the numbers do match up, though, you might need to increase the bandwidth coming into your home. This will cost you more each month, but it could open the data hose wide enough that you no longer experience lags. Going back to the traffic analogy, it would be like putting in a big, circular driveway where cars could get past each other and flow better.

Another option for helping to alleviate slowdowns from network congestion is to connect important devices directly to your router using an Ethernet cable, which delivers the fastest and most stable connection to your devices. Even if your computer doesn't have an Ethernet port, it's possible to buy USB adaptors that facilitate the connection.

Also, most modern routers are now broadcasting in two different bandwidths: 2.4 GHz and 5 GHz. The 2.4 GHz bandwidth is slower than the 5 GHz spectrum, but it can travel further. Yet, most common Wi-Fi devices still operate over the 2.4 GHz bandwidth, so it can simply get more crowded. So, if you have any devices that are in range of your router and can pick up a reliable 5 GHz signal, you can log in to your router and assign these devices that section of bandwidth. You'll need to follow the specific instructions for your modem, but the process isn't complicated and can usually be found by searching online, using your modem's app, or checking out the user manual if you still have it.

Finally, if you're still seeing slowdowns, you can create an internet schedule for your home outlining who can use your connection for different activities at different times. By spreading out the demand for data-intensive tasks, you might just experience a speed improvement. Also, while

some family members might have to wait to hop online until it's their turn, if you have a good cellular connection at your home, they can use that to surf, chat, and stream, taking even more pressure off of your home's bandwidth pipeline.

Your Router Can Help, Too

Want to skip the negotiation and tell your router which devices should be slower? The best routers have "quality of service" (QoS) features that let you prioritize specific devices and applications on your local network. For example, you might want to prioritize a work PC over a gaming PC—or a gaming PC over a work PC.

This article is republished, with permission, from the How-To Geek web site.



(Latency.....Continued from page 8)

When we ping our local router, we see a latency of 1ms. Our router is close and we can connect directly without going through other routers.

```

C:\Users\Chris>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Chris>

```

You can see how much latency each router – or “hop” – is adding with [the traceroute command](#).

```

C:\Users\Chris>tracert baidu.com

Tracing route to baidu.com [123.125.114.144]
over a maximum of 30 hops:
  0  2 ms  1 ms  1 ms  192.168.1.254
  1  9 ms  7 ms  8 ms  18.246.112.1
  2  9 ms  8 ms  11 ms  96.1.253.134
  3  8 ms  8 ms  7 ms  173.182.214.134
  4  *  *  *  Request timed out.
  5  36 ms  36 ms  35 ms  154.11.10.165
  6  35 ms  40 ms  37 ms  219.158.33.249
  7  180 ms  180 ms  180 ms  219.158.30.253
  8  178 ms  178 ms  177 ms  219.158.19.193
  9  173 ms  192 ms  192 ms  219.158.23.17
 10  216 ms  216 ms  215 ms  219.158.101.121
 11  225 ms  228 ms  224 ms  123.126.0.70
 12  212 ms  211 ms  212 ms  bt-227-018.bta.net.cn [202.106.227.181]
 13  230 ms  228 ms  228 ms  202.106.43.66
 14  *  *  *  Request timed out.
 15  *  *  *  Request timed out.
 16  *  *  *  Request timed out.
 17  229 ms  229 ms  228 ms  123.125.114.144

Trace complete.

```

tracert baidu.com

Latency is always with us; it's just a matter of how significant it is. At low latencies, data should transfer almost instantaneously and we shouldn't be able to notice a delay. As latencies increase, we begin to notice more of a delay. Low latency is good, higher latency not so good.

This article is republished, with permission, from the How-To Geek web site.



(Spammers.....Continued from page 5)

from businesses who should know better. In addition to revealing their customer/contact lists to everyone else in the distribution list, it's really bad form. I recommend using the BCC: (blind carbon copy) option instead of putting multiple addresses in the TO: or CC: lines of your outbound emails.

Data Breaches: An Ongoing Privacy Menace

Hacking into a major company's databases can yield millions of high-quality email addresses at once, not to mention even more valuable data such as credit card numbers, Social Security Numbers, etc. In December 2016, Yahoo confessed that over one BILLION of its users' accounts had been hacked three years prior. Target, Chase Bank, American Express, Home Depot, Apple, Sony and other large companies have reported hacks in recent years, resulting in many millions of accounts being compromised.

The Big Kahuna of Data Breaches was reported in September 2017. The [Equifax hack](#) was especially damaging, because it revealed names, addresses, Social Security Numbers, birth dates, driver's license data, credit card numbers, and email addresses. By combining all of that data, Bad Guys can create much more sophisticated and compelling email scams. See my article [Which Privacy Tools Do You Need \(and which should be avoided\)?](#) for some tips on how to protect your privacy in the age of constant data breaches.

Spammers also trade in lists of email addresses. A list of a million addresses gleaned from a data breach might go for as little as \$100. Some online crooks don't even mail spam, but make their living harvesting and trading email addresses.

You supposedly legitimate business associates (or any website where you hand out your email address) may be selling you out to spammers, though they may think of the spammers as "trusted partners." Before signing up to any mailing list, make sure you know what the email privacy policy is. Opt out of allowing your email address to be shared with third parties for any reason, if possible.

It's almost impossible to hide your email address from spammers completely. At the least, you'll probably get a blind dictionary attack spam, eventually. But you can reduce the attack surfaces. The fewer entities that have your email address, the less spam you will receive. Think (and read the privacy policy) before you give your email address to any website. Using a *disposable email address*, keeping your own computer secured, and encouraging your friends and family to do likewise will also help.

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



(Cost.....Continued from page 7)

Security software products increasingly appear to include auto-renewal requirements (you can often read this in their advertising and on their packaging, although it might be in the very fine print). This should not stop you from considering any of them. By including this auto-renewal, they have your purchasing credentials (credit card) and can renew their product automatically when the current subscription is about to expire (usually the subscriptions are for 1 year, but some offer 2-year lengths). But you usually have the option to opt-out of their auto-renewal scam in the online account that you create when you install their software. "Usually", because I recently saw on someone's PC that their security product did NOT have this opt-out option, and the user had to call the software producer to cancel the renewal push, because the user chose to switch to a different, at-least-as-good and more-cost-effective product. A software product that does not offer such an opt-out without the necessity of a phone call (whether high-pressured or not) ought to be removed from any consideration for purchase.

You need to be sure of what you are buying. Often, store or publisher sales include 1 subscription for only 1 device (and again, often at an inflated price). Other purchasing locations may offer you the identical security product, but include multiple subscriptions and at lower cost. Getting a multi-device subscription in one purchase can allow you to protect multiple devices (PCs, phones, tablets). I have several PCs (who's surprised??), so a multi-device subscription serves my purposes exactly. Perhaps just 1 device, or 3, or 5, or even 10 in one software purchase. Even share such a subscription with family members or friends. Sharing the cost among them will certainly be a great service to them. Or share a subscription as a gift.

So where do you purchase the same security software at a savings, and still know that you have legitimate stuff? Online sites such as Newegg (my preference) and Amazon. The security software industry is very competitive, so sometimes you'll find unbeatable sales on the software publisher web sites, too, but not too often. Sometimes purchasing directly from a publisher requires you to install the product and start the subscription immediately, so read the details. Purchasing the software from Newegg or Amazon doesn't require that. The subscription period starts when you apply the license. When I see a terrific price for my chosen product (like a holiday or Black Friday sale event), I can purchase another subscription, but start to use it when I decide that it's time.

When you purchase on sites like these, you often have two choices: purchase the software in a box that is mailed to you (the box only includes a card with the license for the software), or purchase the product and have the license e-mailed to you. In either case, you will download the security software from the publisher's web site (from the 'horse's mouth', so to say), and then just apply the license when you are ready to use it. So, if your current software expires in two months, you can purchase a license now for use when you apply it in two months. In this way, you can gain the advantage of very

cost-effective sales events.

I have used Norton products since we were first warned about software threats, even before the days of the Internet (remember the days of [Prodigy](#) and dial-up modems??). Does the fact that not one of my PCs has ever been bitten by a virus infection make Norton products the best of the best? Not necessarily. Perhaps my (claim to some) smarts and a generous dose of luck have helped, but I stick with their products because they have not failed me over 30 years on these toys, and their products continue to be measured and reported among the very best. Occasionally, I've used non-Norton products, many of which work just as, or almost as, well.

But now the Norton folks (the Symantec corporation) include an auto-renewal requirement on their products, as do so many other similar security products. It doesn't please me, but everyone's starting to do it, so it's part of the industry. OK, but I can opt-out. Good. But even if one of their products was available for as little as \$15 for 1 year recently (for Comcast users), the associated auto-renewal price is quoted to be \$105 per year. *That's outrageous!!* So, what do I do? If I choose to stick with this product line, I'll just watch for a good sale price for the same product (or a competitor's product, if I choose to switch), and purchase a new license and store it for when my current subscription runs out. If I were to choose to switch to a different company, then I would just uninstall my current security product at the appropriate time, and install the new product. If I choose to stick with the current product, I would just enter the license number into the currently-installed product when the time comes, to extend my protection for another period. (Remember, you can use as many *anti-spyware/malware* products on your PC as you wish, but only one so-called "*anti-virus*" product on the device. The presence of two such anti-virus products will render each of them as incapable of performing properly.)

So what's the real point of all of this, you may be asking by now? Being frugal. Last time I checked, money still isn't growing anywhere in my back yard (with the weeds). I choose to save a bit here and a bit there, and purchasing security software smartly is easy and can make a difference. The user I mentioned earlier had a subscription to Vipre, which is also a fine security product. But they wanted \$37 for a 1-year *renewal* that included only 1 license. With my coaching (but not being *too* pushy), the user switched to one of the top Norton products. If I recall correctly, it cost \$29 for 1 year (at Newegg), and it includes 5 licenses, which the user can use on other devices or share (free or otherwise) with others who need device security. The Norton product also includes other bells/whistles, some of which are certainly worth using (such as free VPN with no download restrictions — Bitdefender's free VPN is limited to 200 MB/day!).

Just do not have the impression that you MUST purchase from a local retail store or directly from the software publisher (when your current software pushes you to purchase from them as your software approaches its expiration date). And when you go to a store to purchase a device or to get one serviced, do not be pushed into buying the store's 'recommended' software choice. You can usually do much better elsewhere, and retain at least the quality of those higher-priced options.



How to Archive Facebook Posts (without Deleting Them)

By Tim Brookes

<https://www.howtogeek.com>

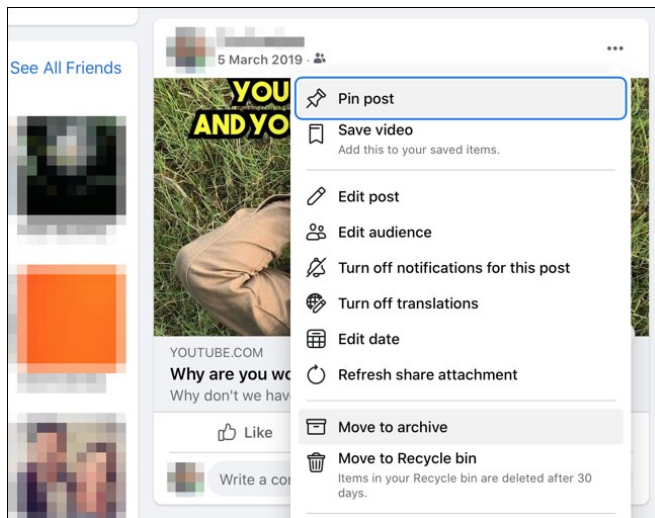
Worried your past posts will come back to haunt you? Fortunately for you, Facebook has a tool that lets you archive your old Facebook posts in bulk so that they're hidden from everyone but yourself. Here's how it works.

Rather than only [restricting certain people](#), the Archive function on Facebook effectively reduces the audience that can see the post to just you. Even if someone else has the direct URL to a post you are made, the content will be inaccessible. Conveniently, the instructions for doing this are virtually identical whether you're using Facebook on the web or via a mobile app.

** Note: You can only archive your own posts on Facebook.

How to Hide Posts From Everyone with Archive

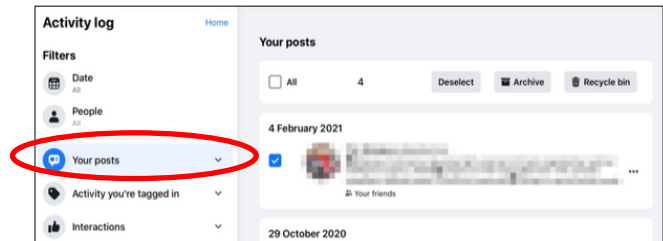
To hide an individual post, you first need to find it on your profile. Click or tap on the ellipsis "... " in the top-right corner of the post box, then choose "Move to archive" in the drop-down menu. The post will disappear and you'll see a notification that it was moved to your archive, with a link to follow if you want.



You can also do this to multiple posts at once, making it easy to manage a backlog of posts that you no longer want friends to see. You can do this via the Manage Posts tool on your [Activity Log](#).

To access this on the web version of Facebook, click on the downward-facing arrow in the top-right corner of any page, then choose Settings & Privacy > Activity Log. Click on "Your posts" in the left-hand menu to see a list of posts. You can use the checkboxes next to posts to select

as many as you like, then click "Archive" to send them to the archive.

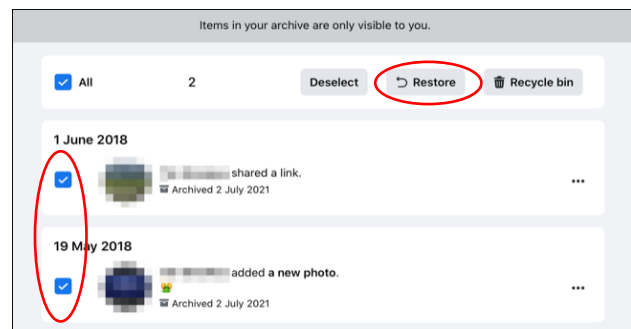


This works virtually identical on Facebook's mobile apps. To get to Activity Log, however, you'll need to tap on the "More" tab (it looks like three horizontal lines), then tap on Settings & Privacy > Settings and choose "Activity Log" under the "Your Facebook information" section. You can now tap "Manage Your Posts" to bulk-archive or delete.

How to Restore Archived Posts

While posts are archived, they are only visible to you. You can make any of these posts visible again by visiting your Archive, accessible via the Activity Log.

To get there on the web version of Facebook, click on the downward-facing arrow in the top-right corner of your feed then choose Settings & Privacy > Activity Log. From here you can click on "Archive" in the left-hand menu to see your posts. Use the checkboxes to select them and, and click the "Restore" button to move them out of the archive.



On mobile, hit the "More" tab (it looks like three horizontal lines) then Settings & Privacy > Settings. Scroll down and tap on "Activity Log" then choose "Archive" to see your posts. Use the checkboxes to select and restore them.

How to Permanently Delete Posts

If you do want to get rid of posts permanently, choose "Move to Recycle bin" instead of "Archive" when managing posts. Anything in the Recycle bin (also accessible from Activity Log) will be permanently deleted after 30 days.

This article is republished, with permission, from the How-To Geek web site.



Web Page Reviews Overload

(Web sites that did not fit on page 14)

Changing the **DNS settings** on your Windows 10 PC can result in faster Internet travels and improved online safety/security. Here is how to change DNS settings on your PC running Windows 10.

<https://www.windowscentral.com/how-change-your-pcs-dns-settings-windows-10>

DNS performance analytics and comparison -- Find the fastest *and* most reliable DNS for free based on millions of tests.

<https://www.dnsperf.com/>

Read about Cloudflare's free **DNS service** which replaces the connection between your device (Windows, Mac, Linux) and the Internet with a modern, optimized protocol.

<https://1.1.1.1/>

Replacing the mechanical hard disk drive (HDD) in your desktop or laptop computer with a solid state drive (SSD) can dramatically improve its overall performance/speed, and make an old slow device so much more pleasant to use. Here are tips about what to look for when shopping for an **SSD**.

<https://www.maketecheasier.com/buying-ssd-guide>

Old games don't work in modern OS's because their codes are obsolete and are no longer supported. But here are a few tricks to play old games in Windows 10.

<https://www.maketecheasier.com/run-old-games-on-windows>

Toppling a massive **domino design** with 32,000 domino pieces that took 89 days to build. (5 min. video)

<https://www.youtube.com/watch?v=FWgH0hXZKrE>

As of May 25, 2021, Microsoft started to roll out an update that installs (pushes) the "**News and Interests**" widget onto the Windows 10 taskbar. How to get it, configure it...or disable it!

<https://www.digitalcitizen.life/news-and-interests/>

Did you ever wonder how to play a song backwards, and how it would sound, and even whether any hidden messages are there? Here's how to use **Audacity** to reverse audio in Windows.

<https://www.digitalcitizen.life/how-play-song-reverse-windows-audacity/>

When combined, the 'Facebook companies' know a huge amount about you. Here's the data that "**WhatsApp**" and "**Instagram**" send to Facebook.

<https://www.wired.co.uk/article/whatsapp-instagram-facebook-data>

Have an **analog camera** lying around? This Raspberry Pi can make it digital.

<https://www.reviewgeek.com/93416/have-an-analog-camera-this-raspberry-pi-can-make-it-digital/>

The Windows 10 **Battery Report** feature measures whether your PC's power source is ready to give out or has some life left in it. Here's how to monitor your laptop's battery life.

<https://www.pcmag.com/how-to/how-to-check-your-laptops-battery-health-in-windows-10>

Think your **laptop battery** is running down quicker than it should? Here's how to check laptop battery health in Linux.

<https://www.makeuseof.com/how-to-check-your-laptops-battery-health-in-linux/>

TPM 2.0 (Trusted Platform Module technology) appears to be the prime requirement for Windows 11 to install and run on a PC. If your PC does not have TPM 2.0, Win11 will not install on it.

<https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview>

From idea to icon: 50 years of the **floppy disk**.

<https://www.howtogeek.com/740436/from-idea-to-icon-50-years-of-the-floppy-disk/>

How to bulk-delete messages from **Facebook Messenger**.

<https://www.maketecheasier.com/bulk-delete-messages-facebook-messenger/>

What does this **emoji** mean? Emoji face meanings explained here.

<https://www.makeuseof.com/tag/emoji-english-dictionary-emoji-faces-meaning-explained/>

How do "**frame rates**" affect the gaming experience?

<https://www.howtogeek.com/731943/how-do-frame-rates-affect-the-gaming-experience/>

What is a **web crawler**, and how does it work?

<https://www.howtogeek.com/731787/what-is-a-web-crawler-and-how-does-it-work/>

9 things with Microsoft **OneNote** to improve your productivity.

<https://www.businessinsider.com/microsoft-onenote-tips-tricks>

Download the desktop version of MS **OneNote** for free.

<https://www.onenote.com/download>

Brave vs. **Firefox**: Your ultimate browser choice for a private web experience.

<https://itsfoss.com/brave-vs-firefox/>

Ransomware — what it is, how it works, types and examples.

<https://phoenixnap.com/blog/ransomware-examples-types#>

How to upgrade from Windows 10 Home to Pro for free (well, for *some* Windows users).

<https://www.zdnet.com/article/going-pro-how-to-upgrade-windows-10-home-without-hassles/>

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.

How to fix “This PC Can’t Run Windows 11”: TPM and Secure Boot.

<https://www.howtogeek.com/737171/how-to-fix-this-pc-cant-run-windows-11/>

Increase your phone’s security by locking apps to the screen on Android.

<https://www.howtogeek.com/712730/how-to-lock-apps-to-the-screen-on-android/>

The **Senior Safe Act** law encourages employees of financial services firms to report cases of suspected elder financial abuse, hopefully leading to more prosecutions of the criminals involved.

<https://www.kiplinger.com/personal-finance/banking/602818/how-the-senior-safe-act-protects-your-finances>

Best tools for **ripping** DVDs and Blu-rays to your computer.

<https://www.makeuseof.com/tag/9-tools-easily-rip-dvds-blu-rays-computer/>

5 shady Google Chrome extensions you should uninstall ASAP.

<https://www.makeuseof.com/tag/chrome-extensions-uninstall-right-now>

Learn how to customize Windows 10 with these powerful **tweak tools**.

<https://www.makeuseof.com/tag/7-best-tools-tweak-customize-windows-10>

Buying a hard drive (HDD or SSD) is easy if you know some basic tips. Here's a guide to understanding the most important hard drive features.

<https://www.makeuseof.com/tag/5-things-need-consider-buying-hard-drive>

What are **brute-force and dictionary attacks**?

<https://www.rapid7.com/fundamentals/brute-force-and-dictionary-attacks/>

How to play Flash files in the flashless age (since Microsoft deleted the Adobe Flash Player tool in mid-2021).

<https://davescomputertips.com/how-to-play-flash-files-in-the-flashless-age>

A sure fire way to protect against **ransomware**.

<https://davescomputertips.com/a-sure-fire-way-to-protect-against-ransomware>

7 steps to your online privacy — The ultimate guide to replace Big Tech with “Free and Open Source Software” (= “FOSS”).

<https://gofoss.today/>

Watch the skin-crawling activity as various **hornets** build, populate, and protect their nests in this video collection.

<https://www.youtube.com/hashtag/hornetqueen>

“I put a hornets nest in a box, and THIS happened!!” **Hornets** as “pets”.

<https://www.youtube.com/watch?v=80Mvn5qHjkw>

Using **Snip & Sketch** (aka the **Snipping Tool**), **Clipboard History**, **Battery Report**, Free **OneDrive** Storage, and **Touchpad Shortcuts** in Windows 10.

<https://www.zdnet.com/article/five-windows-10-features-you-really-should-be-using/>

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.