



THE WYSIWYG



October 2019

Volume 31 Issue 8

STERLING HEIGHTS COMPUTER CLUB

PO Box 385

Sterling Heights, Michigan 48311-0385

MAIN MEETING: TUESDAY OCT. 1

7:00 PM

(doors open at 6:30 PM)

Baker College

34950 Little Mack Ave.

in Clinton Township

Located at the southeast corner of Little Mack Avenue and 15 Mile Road (Enter at the main entrance on Little Mack Ave. The meeting room is then straight ahead.)



IN THIS ISSUE:

About SHCC	2
The President's Pen	3
Don't Lose Your Phone: Here's What Can Happen (and How to Prepare)	4
Is "Refurbished" Worth the Price?	6
Try This, For Faster and Safer Internet	7
My Windows 10 Reset On Its Own to Empty Folders!	8
Why Free OTA TV Beats Cable on Picture Quality	9
Need to Email a Big File? Try "Firefox Send"	10
Six Little Word Problems and Their Solutions	11
Why You Shouldn't Trust Free VPNs	12
Life Without the Internet	13
Web Page Reviews	14

This Month's Main Meeting Topic:



"Build a Low Cost Computer Using the Raspberry Pi"

by Jeff Pynnonen

Jeff is an Embedded System Engineer, and has worked primarily in the automotive industry. One of his interests is the Raspberry Pi, a \$35 - \$55 credit-card-sized computer that runs a version of Linux. He has been programming for 50 years and is currently writing Python code for a kiln controller using a Raspberry Pi. His talk will be about setting up the latest Raspberry Pi 4 device as a desktop system and the free software that comes with it.

Don't know what a Raspberry Pi is, or is for? There are many web site links in the **Web Page Reviews** section of your club's web site (including some videos) which give you a sort of pre-introduction to this month's presentation topic, and perhaps help to kindle pertinent questions for our presenter. (Select **Reviews by Key Word**, then **Computers**, then **Raspberry Pi**.)

Guests and visitors are welcome. People can attend any SHCC meetings during two consecutive months before deciding whether to become a member or not. July and August don't 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 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>

2019 SHCC Officers

President	Don VanSyckel	President@SterlingHeightsComputerClub.org
Vice President	Mike Bader	VP@SterlingHeightsComputerClub.org
Secretary	Martee Held	Secretary@SterlingHeightsComputerClub.org
Treasurer	Bernie DeFazio	Treasurer@SterlingHeightsComputerClub.org

Resource People

Firefox	Don VanSyckel
General Computer Questions	Jack Vander-Schrier
Hardware	(open)
MS Publisher	(open)
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 Page Reviews column	Paul Baecker

Contact Information

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

Mike Bader	586-447-6683	programs@sterlingheightscomputerclub.org
Paul Baecker	586-286-2314	newsletter@sterlingheightscomputerclub.org webwatch@sterlingheightscomputerclub.org
Patrick Little	586-264-1497	publicity@sterlingheightscomputerclub.org
Phil Reynaud	586-212-2848	publicity@sterlingheightscomputerclub.org
Rick Schummer	586-254-2530	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.

Four-Month Meeting Schedule

NOVEMBER 2019
5 - SHCC Main Meeting
 10 - SEMCO Meeting

JANUARY 2020
7 - SHCC Main Meeting
 12 - SEMCO Meeting

DECEMBER 2019
3 - SHCC Main Meeting
 8 - SEMCO Meeting

FEBRUARY 2020
4 - SHCC Main Meeting
 9 - 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



As you probably heard or read by now, SHCC will continue meeting at Baker College at least through June 2020. As of writing this I have not heard any new information about Baker's plans for the Clinton Township campus. We do have a contingency plan, but keep your eyes open for possible meeting sites.

The phone industry, or should I say the communications industry, has and is moving rapidly. To review, we've moved through:

- * telegraph
- * telegram
- * telephone
- * pager (short text)
- * cell phone (voice)
- * cell phone (text)
- * cell phone (pictures and video)
- * wearables (watches etc.)

Be careful, as we rush towards technology for convenience, we are slowly but surely giving away our privacy. Back a few years ago if someone, such as the government, told you that you had to carry something, even if they supplied it, so your movements could be tracked, you would have pushed back and refused. But now you voluntarily pay hundreds of dollars to carry such a device that tracks your movements and monitors your conversations.

I have been told that all new cell phones have a GPS trackable feature that can't be turned off. There's good news and bad news in this. Good news is in emergencies you can dial 911 and the system can report your location to emergency responder personnel. Bad news is the government can now track your every movement, when your phone is with you. Currently the government is mostly benign but things can change drastically and quickly. Just investigate the platforms of some of the current national political candidates. The other abuse that can and has happened is someone in the system with an ax to grind, such as going through a divorce, in a neighborhood dispute, or in a legal dispute, can procure information about your movements and there by who you're contacting. Any system involving people has flaws. People being people are susceptible to people doing the wrong thing whether purposefully or accidentally.

Now consider that every time you Google something the Google company records your searches. Haven't you noticed all the advertisements for stuff you recently searched for? The other way Google manipulates you is in the presentation of search results. Not only does Google take money to put listings first in the returned list, it has been documented that Google also arranged search results in some cases (both order of results and leaving out some results) to support their ideological agenda. This is a very subtle thing since you sit in the comfort and security of your own home and have your private web activity tracked, recorded, and manipulated and you don't even know it's happening. So if you like being manipulated continue using

Google. If you want to live free and untracked, consider using a different search engine such as [DuckDuckGo](https://duckduckgo.com/) or others that don't track and manipulate. *{Ed note: In the same vein, consider switching from Google Chrome to a much more pro-privacy web browser such as [Mozilla Firefox](https://www.mozilla.org/en-US/firefox/).}*

As you might have concluded from the above, I consider personal privacy a necessity, if not a right; it's a part of being a free society and not just a member of a registered herd.

This month's presentation will be of interest to many. "Build a Low Cost Computer using the Raspberry Pi" will be presented by Jeff Pynnonen. This new small and affordable technology might be the wave of the future. Come see all the great things you can do with a Raspberry Pi; a computer is just the beginning.

Last Month's Meeting:

Last month we were pleased to have new SHCC member Chita Hunter from Hunter Designs present "The Apple Watch". Chita did a great job and I'll bet at least a couple people went out the next day and bought an Apple Watch. This new wearable technology might be the wave of the future and it was very interesting exploring it's capabilities and features with Chita's unique presentation style.



Door Prize Winners!

September 2019

Evelyn Cherson — paper ream
 Irene Kramer — Linux laptop
 Walter Jendhoff — wireless mouse
 Mike Galat — digital multi-timer
 Paul Baecker — DVD spindle
 Richard Katnik — Maximum PC magazine
 Bernard DeFazio — CD case
 Priscilla Galat — Coast inspection flashlight
 Richard Jackson — paper ream
 Ron Linsley — Sharpie pen set
 James Waldrop — tally counter

If your e-mail or USPS mailing address changes, please send the details via e-mail to: *Secretary*
[@SterlingHeightsComputerClub.org](mailto:Secretary@SterlingHeightsComputerClub.org)

Don't Lose Your Phone: Here's What Can Happen (and How to Prepare)

By Leo A. Notenboom
<https://askleo.com>

Given how much we've come to rely on them, are you prepared to lose your mobile device?

Mobile phones are amazing devices. They're much more than just having your email or social media at your fingertips; they're truly portable general-purpose computers that also happen to be able to make phone calls.

We do a lot with our phones. Because they're always with us, they're one of our primary means of content consumption — everything from social media to news to maps to ebooks and more — as well as our primary means of communication (though ironically, rarely by actually using the telephone) and one of our primary content-creation devices as well, in the form of photos and videos.

As tiny computers, we've come to rely on them to store data, act as security keys, wallets, fitness trackers, automotive trackers, and dozens of things I can't even think of right now.

Given everything we use our phones for, to say that we shouldn't lose them is stating the obvious. And yet lose them we do. I'm going to review some of the things you need to be aware of when (not if) you lose your phone, and some of the ways you can mitigate the damage when it happens.

Summary:

- You lose access to data on the phone.
- You lose control of data that can be accessed by the phone.
- You risk losing access to any account that can be accessed by the phone.
- You risk losing access to your accounts via other means.
- You risk someone being able to impersonate you.
- Back up all data on your phone.
- Set a PIN
- Use a tracking service, ideally with remote-wipe.
- Have backup mechanisms in place for two-factor authentication.
- Contact your carrier immediately.

If it's in only one place

The first thing most people think of when they lose their phone is the collection of photographs and videos they keep on it. Most commonly, these are images they've taken using the device and haven't bothered to copy

anywhere else.

In other words, they're not backed up. They exist only on the phone. When the phone is lost or stolen, so are all the photos.

While a few items might have been shared either directly or via social media or other means, you can't count on it. You also can't count on those that were shared having been saved, or having been shared in original quality.

Remember, of all the other data you keep, particularly on your phone, photos and videos are the only ones that cannot be re-created.

If it's on your phone, it's in their hands

If your phone is stolen, the data on it is now in someone else's hands. All of the data stored on your phone: your emails, contacts, texts, chats, documents, photos and videos, and everything else.



And yes, it's sometime difficult to know what's on the phone and what's online in "the cloud". As a result, you must assume it's all been handed to the person now holding your phone. Besides, as we'll see shortly, the distinction between what's on your phone and what's online may well be irrelevant.

If your phone is your key

Security experts and not-so-experts strongly recommend two-factor authentication as a means of securing your online accounts. Without a doubt, for maximum security you should avail yourself of this option if it's available for any account you consider important.

Phones are common and convenient two-factor authentication devices. Be it via code-generating apps that run on the phone, to codes in text messages that you receive when logging on elsewhere, your ability to provide those codes on demand "proves" you have the phone — the second factor — in your possession. Thus, you must be who you claim to be.

When a phone is stolen, the first thing people worry about with two-factor authentication is that the thief now has their second factor. That's typically not as huge a problem as you might think: they need both factors — your password and the phone — in order to sign in as you elsewhere. Typically, getting access to the phone won't gain them access to your passwords as well.

The real, larger problem is you no longer have your second factor. Unless you've prepared, you may not be able to log in to the accounts so protected.

Your phone becomes their portal

If your phone is stolen and it's likely your email account has been compromised, you'll want to check out [Email Hacked? 7 Things You Need to Do NOW](#).

Much of the data we access using our phone is not actually stored on the phone. Using various apps and interfaces, our phone is a portable gateway to our online world. Email is the most obvious, but cloud-storage services, note-taking apps, music players and more all work primarily by fetching your information from your accounts online.

Once a thief has access to your phone, they have access to this portal. They can — and often do — proceed to immediately change your email password so as to take control of that account, and at the same time remove their need for your phone to continue; they can access your email anywhere now. Since your email is also often your backup/recovery account for other online services, just getting access to that opens a second portal for the thief to then wrest control of those accounts as well.

They might become you

Stealing your mobile device is one of the best ways hackers and thieves begin to impersonate you, possibly even leading to outright identity theft. Not only by stealing your accounts, as I've discussed above, but by literally impersonating you. Calls they make, or perhaps more realistically, text messages they send, appear to have come from you. They can use that ability to fool everyone from online services and banks to your friends and family.

So, what to do?

Now that I've laid out the great risk we embrace by relying so heavily on these portable and easily lost or stolen devices, what should we do?

Certainly returning to luddite ways and abandoning the technology is not an option. Oh, I know it will be for some people, but it's their loss.

And there's no need. There are several simple steps you can take to protect yourself.

Back up your phone

Particularly when it comes to photos and videos, there's simply no excuse. Most cloud storage apps like Dropbox, OneDrive, and others offer to automatically upload the photos and videos you take. Depending on your choice, they can upload immediately regardless of where you are as long as you have an internet connection, or they can upload the next time

you're connected to Wi-Fi, so as to save on your mobile data plan.

If you do nothing else, back up your photos.

When it comes to the rest of the information on your phone, solutions vary. By virtue of being linked to an online account, for example, email and contacts are often automatically backed up. Many mobile providers automatically track which apps you have installed and reinstall them if you move to a replacement phone.

The data stored by the various apps you have installed, however, is a wild card. For each app with which you have a significant investment of data, make sure you understand where that data is stored and what happens if your device disappears. If additional backups are called for, look to the app developer for guidance.

Set a PIN

One very simple step to protecting the information on your phone is to set an unlock code or PIN, and make sure your phone automatically locks after some amount of time.

In order to access the device, the correct PIN must be entered. Without it, accessing what's on your phone becomes difficult, if not impossible.

Also, consider configuring your phone such that if the wrong PIN is entered too many times — say ten times — then the phone automatically wipes all data.

A PIN isn't perfect — it's sometimes easy to guess or "shoulder surf" (watch someone enter their pin) — but it's an excellent first level of defense when it comes to protecting the information on and accessible by your mobile device.

Consider a tracking service

You may or may not need an additional tracking service for your phone — you may already have one, courtesy of your platform (iPhone or Android) or your mobile carrier. In my opinion, it's important that such a service have the following features:

- The ability to locate your phone using its GPS.
- The ability to remotely lock and/or wipe your phone of all data.
- The ability to display a message on the phone's screen.

Remote wipe is critical, in my opinion, as it's the only way to protect yourself should a thief gain access to your device.

Personally, in addition to the facilities made available via Android and my carrier, I use Prey to protect my phone,

my wife's phone, and the laptop with which I travel most.

Set up two-factor properly

It's not enough to set up two-factor authentication. Whenever possible, you need to set up a recovery mechanism.

Most services that use two-factor have alternate approaches available when your second factor, such as your phone, isn't available. They're often more cumbersome and time consuming, but they're infinitely preferable to not being able to access your account at all. Some of the recovery mechanisms include:

- Additional second factors, such as additional devices or text-message numbers to which a code can be sent.
- One-time passwords. These are created and saved somewhere safe. Should you not be able to log in using your second factor, you can use a one-time password instead. As the name implies, each can be used exactly once. If you run out of these passwords, you return to the service to generate more. The critical thing to realize is that you need to create one-time passwords before you need them, and keep them in a safe place.
- Recovery email address(es). Again, these must be set up beforehand, but they act as a type of second factor: prove you can access this pre-defined account, and you must be who you say you are.

Regardless, make absolutely certain that if you lose your two-factor device, you have an alternate way in.

Contact your mobile provider as soon as possible

Finally, if your phone has been lost or stolen, contact your mobile provider as quickly as possible. There are two reasons you don't want to waste time on this:

- They can disable the phone, preventing it from accessing the mobile network (though the phone will likely still be able to access the internet via a Wi-Fi connection).
- They will be aware of all the security options — from remote wipe to simply locating the phone — that may be preinstalled, and be able to help you make the wisest decisions about what steps you need to take.

Given how much we use them and what we use them for, losing your mobile device is no small matter. It pays to prepare beforehand and act quickly when disaster strikes.

This article is republished, with permission, from the Ask Leo! Web site.



Is “Refurbished” Worth the Price?

News and/or Opinion from Paul Baecker

I recently went shopping for a cable modem to eliminate the rental cost of the one supplied by my ISP. After doing some online research, I decided on a capable Arris model, and found it at a local retailer. The store had some new ones, but also had some *refurbished* ones for about half the price of the new ones. I thought to myself, well, they've simply been returned by shoppers who had changed their minds because they didn't like the color or style, and the units were probably basically unused. I inquired and learned that they had previously been used in a business somewhere (how would the salesman know?). So next I thought, well, do I want to save a few bucks by buying this so-called refurbished unit? Surely the items would have been repaired (if necessary) and tested by an OEM (Original Equipment Manufacturer) facility, so that they operated as though they were new, even if they did have some wear marks on them. A no brainer to save the money, right?

But for whatever reason, I got a bit more inquisitive and asked about to what extent these items were refurbished. To the original manufacturer's specifications? In this case, nope. Well, then, surely the store could vouch for the level of refurbishment done by the third party. Nope again. I learned that there are businesses that exist to refurbish electronic products to *their own specifications*, and they are not necessarily noted as to their relationship to the *product's original specs*. My excitement in getting a great deal was gradually waning. Finally, the store rep tells me that they offer a 14-day return on a purchase of this item, but no warranty beyond that return option. I eventually passed on this offer. I figured that with my luck, the item would last past those 14 days, but die too soon thereafter.

I also checked the details on the web site of a popular online retailer of computers and accessories. I found similar statements about refurbished products being refurbished to the specs of the refurbishing organization. Some refurbished items came with warranties, some could be warranted at extra cost, and some items were 'as is' (such as demos) with no right to complain after the purchase.

So, what this adventure taught me is to carefully vet the retailer of any refurbished item you're considering (whether electronics, furniture, appliances, etc.) and carefully study the purchase agreement and any (often hidden) disclaimers that apply to the purchase.

A definition I found online for the term “refurbish” is “to brighten or freshen up”. *Yikes!!!*

You'll find a link in this issue's Web Page Reviews collection (page 14) to an online article about doing your homework when shopping for refurbished products.



Try This, For Faster and Safer Internet

By Bob Rankin

<https://askbobrankin.com>

On occasion, I have recommended using alternative DNS as a means to a faster and more reliable Web browsing experience. But faster Web surfing isn't the only benefit of switching your DNS servers. I know it sounds geeky, but I'll explain it all in plain English and show you how to make Internet usage both faster and safer, for both adults and curious kids. Read on...

Speed and Safety

Let's start by de-geekifying the DNS acronym. DNS stands for "Domain Name Service" and it's a service normally provided by your Internet Service Provider (ISP). Here's why it's necessary... Humans refer to websites by their common "dot com" names, but the computers that run things on the Internet know them only by numbers known as IP (internet protocol) addresses. When you tell your browser you want to visit a certain website, it must connect to a DNS server to translate that website name into an IP address.

Normally, that DNS server is operated by your ISP, but there's no technical reason why that must be so. Alternate DNS services can be used to speed up web surfing, provide an additional layer of security, correct typos, or assign shortcuts to commonly-typed website names. Here are some free alternative DNS services you can try.

[OpenDNS Home](#) is one such service, used by over 30 million people at Fortune 50 companies, small businesses, schools, and homes. The free service doesn't require you to sign up for anything, or install any software. By twiddling a few numbers in your router's setup screens, you can speed up web surfing. But you can also filter out malware, phishing sites, botnets, If you also want to filter out adult content, use the [OpenDNS Family Shield](#) instead. It works exactly the same as the OpenDNS Home service, but is preconfigured to block sites that may not be appropriate for younger users.

OpenDNS includes one of the leading anti-phishing projects on the Internet. [PhishTank.com](#) is a collaborate effort to identify and block phishing Web sites one bogus URL at a time. Any registered user can submit a suspected phish to PhishTank via email or the site's "Add A Phish" uploading feature.

Each suspect URL is evaluated by a worldwide community of security consultants, academics, and registered users. When at least two users agree it's a phish, the bogus URL is added to PhishTank's database of verified

phishing links. The number of votes needed to verify a phish varies depending on the reputations of the voters. Reputation is established by being right more often than you are wrong. Users who submit lots of false positives – URLs that turn out not to be phishing sites – and who, more often than not, incorrectly label others' submissions as phish or not-phish, will have lower reputation ratings.

False positives – URLs incorrectly labeled "phish" by the community – can also be reported. PhishTank's staff will review the classification and revise it if warranted. OpenDNS draws upon many resources such as PhishTank to decide which URLs and IP addresses to blocks for its users who have phishing protection enabled. It's possible that a URL labeled "phish by the PhishTank community will not be blocked by OpenDNS.

Separately, [OpenDNS Domain Tagging](#) offers users the option to label websites with tags such as "adult," "violence," "social network," "gambling," and so on. Registered users can tag a domain, but it takes a consensus of the community to make that tag "stick." OpenDNS users can use the tagging system to block selected categories of content, if desired.

But Does It Work?

You have options when it comes to selecting an alternate to your ISP's DNS servers. Google Public DNS is similar to OpenDNS, promising increased security and better performance. Which is best? My answer is try them both! You can compare the speed of OpenDNS, Google and other DNS servers with the DNS Benchmark tool.

There's really no downside to switching your DNS nameservers from the ones provided by your Internet Service Provider to the OpenDNS ones. Most users will see slightly improved page loading time, less "lag" when contacting a website, and fewer errors with unreachable websites.

I am skeptical about the "wisdom of the crowd" method used by PhishTank and OpenDNS. Phishing sites come and go rapidly, and I can't believe that a "committee" of tens of thousands can keep up with the bad guys on every front. But if it blocks the most common phishing attacks, there's value in that. Just don't assume it will protect you from EVERY known phishing threat, and continue to use caution about clicking links you see in emails.

The "parental controls" offered by OpenDNS are probably more effective; p**n, piracy and social media sites don't change domain names nearly as often as phishing sites do. But like every parental-control program ever created, OpenDNS blocks some sites that arguably are not harmful to children. Also, its blocking applies to one's entire network, so Mom and Dad have to give

themselves permission to view "adult" sites like La Leche League, or shop at Victoria's Secret.

If you configure your Internet router with the OpenDNS nameservers, it's important to remember that it can protect only the computers, laptops and other devices that are connected to your router, via a wired or wireless connection. When outside of WiFi range, OpenDNS can't protect mobile devices such as laptops, smartphones or tablets. However, you also have the option to modify the DNS settings on individual devices, rather than (or in addition to) your router. This [OpenDNS setup guide](#) will walk you through the steps to make it happen. Just remember to record your current name-server settings somewhere as a backup, in case you want or need to switch back.

You have options when it comes to selecting an alternate to your ISP's DNS servers. [Google Public DNS](#) is similar to OpenDNS, promising increased security and better performance. Which is best? My answer is try them both! You can compare the speed of OpenDNS, Google and other DNS servers with the [DNS Benchmark tool](#).

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



My Windows 10 Reset On Its Own to Empty Folders!

By Sheila Swaikowski, Webmaster
The PCUG of Connecticut, www.tpcug-ct.org
sswaikowski@yahoo.com

A strange thing happened to my computer recently. I have both Linux Mint and Windows 10 on my computer (dual boot). After I chose to boot into Windows 10, the sign-in for Windows 10 didn't appear on the screen, it was a blank screen. I wanted to watch Timothy Kearn's 17th web design video about .dwt files (dynamic web templates) for updating multiple web pages' header and footer sections more easily. The only way I could sign off of this blank screen was to do a forced shutdown by holding down the off/on button for a few seconds.

I turned the computer on again and watched the video on Linux Mint, signed off using the restart option, and this time chose to boot into Windows 10, hoping that the sign-in would be there. I needed to start working on my template project using my web editor program, Microsoft Expression Web 4.

I was able to sign into Windows, but my icons were arranged alphabetically - not at all like my cluttered desk-

top - there were fewer icons, my short-cuts were missing and all of my folders were empty! What an unpleasant surprise!

I started to think about all the ways to fix this:

- Some of this info was on a second computer and could be copied over.
- I did a system image backup three weeks ago.
- I discovered that I could get to my original files if I clicked on 'This PC, Gateway(C:), Users, Sheila', but couldn't work with them.
- Presently Windows was using the 'TEMP.Sheila-PC.000' folder instead of the Sheila folder and there was no way I could repoint it back to the Sheila folder. I even copied all the Sheila folder stuff into the TEMP.SheilaPC.000 folder, but on second thought, didn't think that was a good idea.

It was time for a coffee break.

After I took a break, it dawned on me to Google the problem. I did find that other people experienced the same thing and there were suggestions on how to solve this. I tried the first suggestion and it worked! It was to sign off the computer and back on again several times if needed. I was very lucky — on my first sign-off/sign-on I got my normal desktop and files back along with all my data. It was as simple as signing off and signing back on! I could have saved a lot of time if I Googled for the problem sooner!

This has never happened to me before and I've never heard about it happening to anyone else. I hope you benefit from getting a heads up on this strange Windows reset, and if it happens to you, you won't panic or waste a lot of time trying to get back your normal desktop and data, like I did, but will know what to do! First, Google for the problem, sometimes it helps — if you're lucky.

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



SHCC Emergency Cancellation

Sterling Heights Computer Club meets at Baker College in Clinton Twp. We will meet if Baker College is open and we will not meet if Baker College is closed. Baker College closure is announced with other school closings on many local TV/radio stations and on their web site. All members of SHCC have an email address. An SHCC officer will send an email to the addresses SHCC has on file alerting members to the event cancellation. If your email is broken, call an officer; and don't leave a message. Call another officer if you don't talk to someone live. It is your responsibility to keep the email address you have listed with your SHCC current.

Why Free OTA TV Beats Cable on Picture Quality

By Andrew Heinzman
<https://www.howtogeek.com>



Legs of two athletes playing soccer in a stadium. We put one of these athletes through heavy compression to show the difference between OTA and cable quality.

It sounds ridiculous, but free broadcast TV offers noticeably higher visual quality than expensive cable. But they both operate at a 1080p resolution, so what gives? Why does a simple antenna get you a better picture than pricey cable TV?

Free TV Isn't Just Sesame Street

Before we get into why OTA TV looks better than cable, we need to understand that OTA TV isn't as useless as people like to imagine. In fact, there's a chance [OTA TV can comfortably replace your cable subscription](#).

Free TV isn't just PBS and local news. Most of the major television channels (especially sports channels) simultaneously broadcast on OTA and cable TV. So, if you're only using cable to watch networks like ABC, FOX, CBS, and NBC, you're wasting [about \\$1,000 a year](#) on content you can get in higher quality with a \$15 digital antenna. And in most cases, [a cheap streaming service](#) can supplement the channels you might lose by ditching cable.

Now that we've cleared the air let's get down to the nitty-gritty. Why does cable look worse than free TV?

Compression Kills Cable Quality

The obvious difference between cable and OTA TV is channel-density. Cable TV is comprised of a few thousand channels, while OTA TV only broadcasts (at max) 69 channels for each locality. This difference in channel-density is the big reason why cable doesn't look as good as OTA TV.

Most OTA channels (55 of the 69) sit comfortably on the 470 to 806 MHz UHF spectrum. This spectrum is divided for each channel, so each one has its own 6 MHz band. But 6 MHz isn't nearly enough bandwidth for HD TV

transmissions. So, broadcasters compress their video (reduce the file size) using the lightweight MPEG-2 codec, which leads to only a [tiny loss in visual quality](#).



Two identical images of a woman wearing sunglasses and a sunhat holding lotion; image on the right is blurry and pixelated. The image on the right is an example of how heavy compression leads to quality loss.

Cable TV occupies the 54 to 1000 MHz frequency range, with a big emphasis on the [750 MHz and 860 MHz bands](#). This giant frequency range (with a focus on high bands) translates to a lot of bandwidth—which means cable TV should look better than OTA TV, right?

The problem is the extra bandwidth is only used to host more channels. While OTA TV places just one channel on each 6 MHz band, cable companies use aggressive compression algorithms (like [MPEG-4](#)) to shove [around 20 channels](#) on each 6 MHz band. As you'd expect, this aggressive compression leads to a dramatic loss in quality. It's kind of like shoving 20 movies on a single DVD.

If you're having trouble understanding all this tech jargon (you're not alone), think of radio frequency (expressed here as MHz) in terms of internet speed (Mbps). Generally, 1 MHz is equal to 1 Mbps. We would need to know what encoding schemes are being used by broadcasters to make an accurate translation, but this simple comparison can make things easier to digest.

Transmission Kills Cable Quality

You probably already know this, but OTA TV is just a local radio transmission that you pick up with a receiver. And while radio signals can technically travel forever, their intensity degrades over time. This degradation can lead to some quality loss, but if you have a correctly set up antenna (and maybe a [signal amplifier](#) to boot), the quality loss will hardly be noticeable.

Cable TV, though, isn't exactly a local operation. It starts with the TV networks, which transmit their programs to local cable companies via satellite. (If you see a plot of land full of satellite dishes, it's probably operated by your local cable company.)

The cable companies then compress these video signals and send them through the city via a network of coaxial cables. These video signals degrade as they travel

through town, so they're boosted by amplifiers along the way. Then, when the signal finally reaches your home, it has to be decoded by your TV. As you can imagine, each step in this messy process leads to quality loss. When paired with the aggressive compression used by cable companies, it's a wonder cable TV looks good at all.

OTA TV Will Have 4K Before Cable

OTA TV already looks better than cable. But the difference might not be a game-changer for you—at least, not yet.

Right now, the FCC is transitioning OTA TV from [ATSC 1.0 to ATSC 3.0](#) (we're skipping the number 2). This change comes with a ton of upgrades, including the ability to watch TV on your cellphone to automatic channel scanning. But arguably, the biggest change is that ATSC 3.0 will support 4K TV. In case you've forgotten, cable TV is still stuck at 1080p.



Why doesn't cable TV support 4K yet? Well, because cable providers got themselves into trouble by offering too many channels. There simply isn't enough bandwidth on the cable spectrum to offer 4K TV. Cable companies are already compressing the hell out of their 1080p content, and 4K is twice the resolution of 1080p. If cable companies decided to shove 20 different 4K channels onto a single 6 MHz band, they'd have to double down on compression, and the quality would look like absolute garbage.

So, if cable companies want to offer 4K, they're going to have to either slim down their library of channels or buy up some more frequency bands. The FCC is currently licensing its available frequency bands to cellphone carriers in anticipation of 5G. The future doesn't look too bright for cable.

Make the Most of OTA TV

There are some obvious drawbacks to OTA TV. Most of these will be solved after we've fully transitioned to [ATSC 3.0](#). Until then, you're just gonna have to work with what you've got. Here are some tips on how to make the most of OTA TV until ATSC 3.0 comes around:

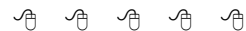
- Use an OTA Box: Like the [TiVo Bolt](#), these add grid guides, DVR functionality, and smart apps to your antenna TV. Essentially, they make free TV [more like cable](#).
- Buy a Good Antenna: Cheap or built-in TV antennas work fine, but they don't have a lot of range. We

suggest buying a [high-range digital antenna](#) that's ready for ATSC 3.0. This way, you get a lot of channels, and you won't need a new antenna when ATSC 3.0 rolls out.

- **Check What's Available In Your Area:** Use a [TV signal locator](#) to check which OTA channels are available in your area. This way, you can adjust your antenna until you receive the channels you want.
- **Try a Signal Amplifier:** If you're not happy with your channel selection (or the channels you do receive look like crap), try a [signal amplifier](#). These, essentially, boost the signals you receive. Just be careful, as signal amplifiers can over-amplify (and distort) good signals.
- **Rescan Often:** As we transition to ATSC 3.0, every channel will move to a new frequency. If you don't [rescan your TV once a month](#), you're going to lose channels.

Of course, you can always supplement your OTA TV with some streaming services. Netflix and Hulu are great, but you can also subscribe to [streaming TV services](#) — like Hulu Live and YouTube TV — if you want a more cable-like experience.

This article is republished, with permission, from the [How-To Geek](#) web site.



Need to Email a Big File? Try "Firefox Send"

By Steve Shank, Board of Directors/Steering Committee
Golden Gate Computer Society, CA
<https://www.ggcs.org/>
editor@ggcs.org

Almost all email providers have a size limit for attachments. If you need to send someone large files too big for email attachments, or you want to encrypt the files for privacy, Mozilla is offering a better, easier way to do this compared with uploading to Google/Dropbox/etc., then following up afterward with the recipient to see when it is okay to delete the files from where they were temporarily stored.

Go to send.firefox.com using any browser; it does not need to be Firefox. No need to signup if your file(s) are less than 1GB per transmission. If you do sign up, the limit goes up to 2.5GB per upload. Your files are uploaded to the cloud and disappear after X downloads or X minutes/hours/days.

You receive a link you can email to the recipient. If you choose to encrypt the file (wise!), you also need to provide the recipient the password, preferably using a separate channel (phone, text, different email service, etc.).

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



Six Little Word Problems and Their Solutions

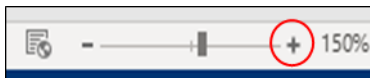
By Nancy DeMarte, 1st Vice President
Sarasota Technology User Group, FL
www.thestug.org
ndemarte@verizon.net

1. You print a multi-page Word document and get an unexpected blank page at the end of the document. Because it has a footer, you won't be able to use that sheet for anything except scrap paper.



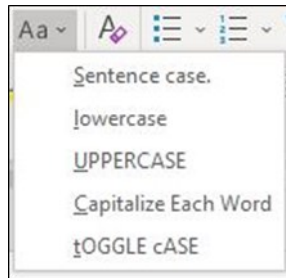
Solution 1: Before you click Print, press the Show/Hide key on the Home tab > Paragraph group and scroll or press the Ctrl+End keys to get to the end of the document. You will see one or more paragraph icons on the last blank page. Select them and press Delete. Then save the document to avoid the blank page in future printings.

2. You open a document and find you have to squint to see the small type.



Solution 2: Go to the Zoom slider at the bottom right of the screen and click the + sign a few times until the document text is large enough to be comfortable for your eyes. This will not affect the text size when printed.

3. You are just about done typing a Word document and notice that all the text in the last couple of sentences is in upper case. You had pressed the Caps Lock key on the keyboard accidentally.



Solution 3: First select the text you want to reformat. Then click the Change Case tool (Aa) on the Home tab > Font group. Click the case pattern you want from the list, which in this situation is probably "Sentence case."

4. Sometimes you forget what version of Windows you have on your computer. "Version" includes the operating system (Windows 7, 8.1, or 10) and the Windows update version number, such as the recent update, 1803. But you're not sure how to find the answer.

Solution: 4 To find the version of your Windows operating system,

type in the Search box at the bot-



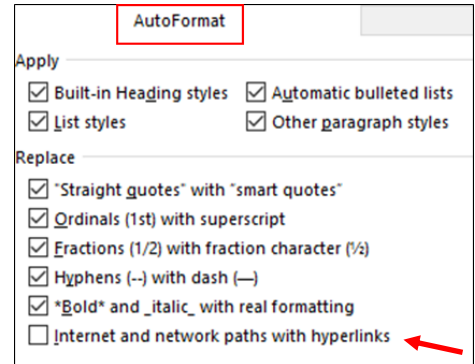
tom left of the taskbar the word *winver*. Then click the

winver run command to see your computer's details.

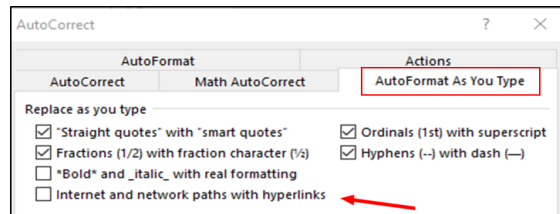
5. When you enter an email or web address in a document, by default Word automatically adds a hyperlink to the address. You can identify a hyperlink by its blue text and underline. Many times, you don't want the hyperlink included.

Solution 5: There is a way to change the setting to stop the automatic hyperlink from being added. Click the File tab (top left of the ribbon), then click Options (last item on the menu).

Click Proofing > AutoCorrect options > AutoFormat and uncheck the last item on the Replace list, "*Internet and network paths with hyperlinks*" then click OK.



Just to be safe, also click "Auto Format As You Type" and uncheck the same box there, followed by OK.



While you are in the Word AutoCorrect area, check to see if

you are being bothered by any other automatic action. If so, uncheck it and click OK.

If you change your mind, return to this screen and recheck the boxes.

6. You have typed a long list of items, such as book titles, taking up several pages of a Word document. Each title is on a separate line. You would like to find out how many items there are in the list, but counting them would be tedious.

Solution 6: Select the entire list using Ctrl+A. Then on the Home tab - Paragraph group, click the numbering tool (top row, second from left) to place a number in front of each item. Then press Ctrl+End to jump to the end of the list, where you can view the last number. If you wish, then press Ctrl+Z or Undo to remove the numbering.

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



Why You Shouldn't Trust Free VPNs

By Chris Hoffman, Editor in Chief
<https://www.howtogeek.com>

Free VPNs are too good to be true. You can download a variety of free VPN apps from Google Play or Apple's App Store, but you shouldn't. These apps aren't worthy of your trust.

How a VPN Works

A [Virtual Private Network](#), or VPN, encrypts all the traffic sent over your Internet connection and sends it to a remote VPN server. Everything goes through the VPN server.

For example, let's say you're in the USA and you connect to a VPN server located in the UK. Then, you access websites like Google and Facebook. Your web browsing traffic is sent over the Internet through an encrypted connection to the VPN server. Your local network operator or Internet service provider can't see you're connecting to Google or Facebook. They just see an encrypted connection going to an IP address in the UK. Google and Facebook just see you as someone located in the UK.

People use VPN servers for a variety of reasons. They keep your browsing activity private from your Internet service provider, for example. If your local government censors the Internet, a VPN would let you bypass the censorship and browse as if you were in whatever country the VPN server is located in. VPNs would also let you use public Wi-Fi hotspots without the threat of snooping.

Many people use VPNs to hide BitTorrent traffic for legal reasons, making their torrenting activity appear to occur in another country. A VPN could also let you access geographically restricted services. For example, if you were in the USA and connected to a VPN server in the UK, you could access the BBC. If you were in the UK and connected to a VPN server in the USA, you could access the USA's Netflix library.

You're Placing a Lot of Trust in Your VPN Operator

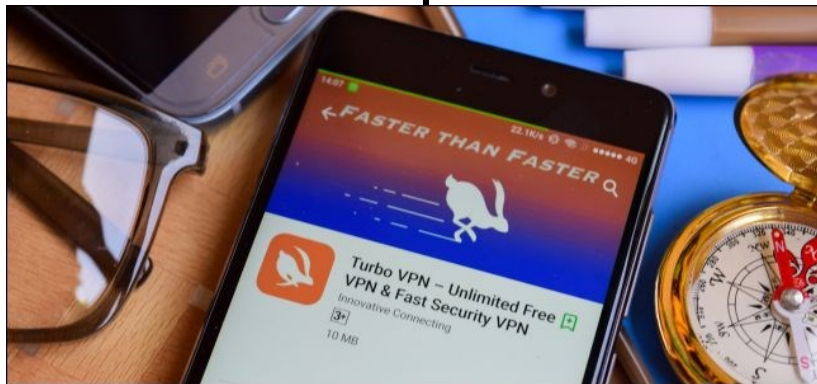
While using a VPN, you're placing an immense amount

of trust in the VPN operator. Sure, a VPN prevents your Internet service provider or Wi-Fi hotspot operator from snooping on your browsing. But it doesn't stop the operator of the VPN server from snooping.

When your traffic leaves the VPN, the operator of the VPN server can see the websites you're accessing. If you're accessing [unencrypted HTTP websites](#), the VPN operator can see the full content of the pages. The operator could keep logs on this data, or sell it for advertising purposes.

Let's put it this way: When you use a VPN, you're preventing the hotspot at the hotel or airport and your Internet service provider from spying on your traffic. But you're letting the VPN provider spy on your traffic instead. Why would you trust a free VPN provider you've never heard of?

A recent investigation by [Metric Labs](#) spotted by [The Register](#) drew attention to this problem, discovering the



majority of free VPN apps have links to China and 86% of them had unsatisfactory privacy policies. Some explicitly stated they transfer user data to China. Most of them had customer support emails pointing to generic personal email accounts on services like Gmail or Hotmail. These don't sound like

services worthy of your trust.

If you're using a VPN for privacy or escaping Internet censorship, you probably don't want to use a VPN based in China.

China aside, you wouldn't want to use a shady VPN hosted in a country with a less repressive government either. The VPN company may just be capturing and selling your data. Or they may keep lots of logs—and, if you're using a VPN for something like BitTorrent, you probably don't want to choose a VPN that logs all your traffic.

What You Should Use Instead

Stay away from free VPNs. It costs a company money to host a VPN server and pay for traffic, so why would that company give you a free service without getting something out of it?

As a free VPN for occasional use, we recommend [Tunnelbear](#). This service only gives you 500 MB of data every month, which isn't much. But it's well-regarded, and the company's business model is selling you unlim-

ited VPN data. It's like a free sample every month, but it can do if you only occasionally need VPN service in a pinch.

If you're serious about using a VPN for privacy, torrenting, bypassing censorship, or getting around geographical restrictions online, we recommend doing some research and paying for a service you feel is trustworthy. We have a [guide for selecting a VPN service](#). You don't have to use our top picks but do some research. Your VPN provider sits between you and all your online traffic, and they can see it. You should find a company with a solid privacy policy and reputation. You'll have to pay for that.

For [serious privacy and anonymity](#), you should check out [Tor](#). Tor is free, but it's nowhere near as speedy as a VPN. It's not something you'd want to use for all your Internet traffic.

If you're an advanced user, you should seriously consider setting up your own VPN. Pay for hosting on a server or cloud service somewhere, install a VPN server, and connect to it. You're now your own VPN operator — although the hosting service could potentially spy on you. There's no escaping it.

You're always placing trust in someone, so choose your VPN service (or hosting company) carefully.

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



Dan's Desk:

Life Without the Internet

By Dan Douglas, President, Space Coast PCUG, FL
<http://scpcug.com/>
 datadan@msn.com

Have you wondered what life would be like without the Internet at our fingertips anymore? Having experienced this very situation recently, due to an extensive outage at our office complex, I can tell you it would take some adjustment. If you ever watch shows like 'The Walking Dead,' then you get an idea of what a disconnected society would be like, but hopefully minus the zombies!

Now, I will be the first to admit that I may be out of the ordinary with my dependency upon the Internet, due to the main nature of my business; repairing and upgrading computers. But I would bet that most of my time on the Internet is like yours; surfing the web, communicating with friends and family via Skype etc., doing email, streaming movies and performing financial transactions. I do the extra tasks of downloading programs/updates,

performing product activations, locating drivers and Windows fixes more than the normal person, along with the research required to solve various error messages and program version incompatibilities. So, when my Internet is unavailable, I'm really limited in the functions that can be performed.

Let's look at those functions that we take for granted while using the Internet and what alternatives we have:

Surfing the web – this is the main information source for most people today, I would guess. So back to TV, radio, the library and reading daily newspapers. The previous generation of Wikipedia – Encyclopedia Britannica is back! I can get my first and worst job back - selling them door to door. Remember the Microsoft (Encarta?) annual encyclopedia on CDs?

Communicating – Cell phones will get really streamlined without all the Internet and related display functions and just back to basic phone call capabilities.

Email – back to the delay of mailing and receiving letters. Typewriters and carbon paper will come back from the dead to provide the capabilities of writing legibly and multiple copies (that is what CC means after all – carbon copy for additional parties). Actually, I can still use the PC and a printer for the main reason PCs were first justified in businesses – word processing.

Streaming movies – check your local theatre for playing times – you can no longer watch your show on demand. Or you can use that DVD/ Blu-ray player for more than streaming – back to discs. Maybe I can restart the movie rental business that I was in back in 1979!

Financial transactions – remember standing in long lines at the bank? Having to access your money only at the branch where your account is based? How about ticker tape machines for those who are addicted to following the stock market?

Well my Internet is back now, so back to work I must go.

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



Member Ads

Ads are available for free to SHCC members, and are limited to computer-related items for non-commercial purposes. Any ad shall be a maximum of twelve newsletter lines of text. Deadline is two weeks before the next main meeting date.

Web Page Reviews

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.

Club members 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.

Sausage making is a lot of fun. It's pretty easy, too, as long as you've got the basics down. Here they are.

<http://www.lets-make-sausage.com/>

Buddy Greene plays his ‘sophisticated’ instrument at Carnegie Hall. (5-min. video)

<https://www.youtube.com/watch?v=xjcA6PuoCfs>

VPN services for privacy-minded Linux users.

<https://itsfoss.com/best-vpn-linux/>

How to create a bootable Windows 10 USB in Linux.

<https://itsfoss.com/bootable-windows-usb-linux/>

Equifax data breach settlement: How to file a claim for \$125 or free credit reporting for 10 years. Deadline is Jan. 22, 2020.

<https://finance.yahoo.com/news/equifax-data-breach-settlement-file-044304302.html>

June was **Internet Safety Month**. But it's always a good time to take action and protect your mobile devices, no matter whether you are traveling or staying local.

<https://staysafeonline.org/press-release/stay-cyber-aware-internet-safety-month/>

10 free spreadsheet templates to organize your life (use with MS Excel, LibreOffice Calc, and similar programs).

<https://www.makeuseof.com/tag/10-amazingly-useful-spreadsheet-templates-organise-life/>

Logitech wireless USB dongles are vulnerable to new hijacking flaws.

<https://www.zdnet.com/article/logitech-wireless-usb-dongles-vulnerable-to-new-hijacking-flaws/>

Why are we addicted to our smartphones? Is it for ‘fear of missing out’? How are we kept coming back for more? What about the degree of distraction, and overall health concerns, not to even mention security? Who is winning and who is being manipulated? (Article includes 22-min. video)

<https://articles.mercola.com/sites/articles/archive/2019/08/24/addicted-to-cellphones.aspx>

You can snag discounts as high as 50% off on smartphones, tablets, computers and associated devices when looking for a *refurbished* unit, but you've got to do your homework.

<https://lifelife.com/when-should-i-buy-refurbished-electronics-5885492>

What is USB-C, the next generation of USB technology? Why is it so confusing? (11-min. video)

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

10 computer myths and lies explained. (12-min. video)

<https://www.youtube.com/watch?v=Lgw3D2KKqDQ>

Things to do before installing Windows 10 May 2019 update version 1903. Although the author's skill of the English language adds a small challenge to reading it (such as “lake” = “lack”), there are many wise cautions in this article that apply to ANY update from Microsoft.

<https://howtofixwindows.com/things-to-do-before-windows-10-upgrade/>

Tool that allows you to split, merge, rotate and reorder one or multiple PDF files in Linux.

<https://itsfoss.com/pdfarranger-app/>

6 types of Google search results you shouldn't trust blindly.

<https://www.makeuseof.com/tag/google-search-results-trust/>

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 Page Reviews 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.