SUPERCOM COMPUTER CLUB TECH TIMES

Volume 08 March 21, 2017

Objective:

To bring the latest technology news to you, our members. Tips and suggestions will help you to keep your device(s) running smoothly and help you be aware of threats. Technical tips will be coming to you through our Technical Committee.

Committee Members: (Pictured Below)

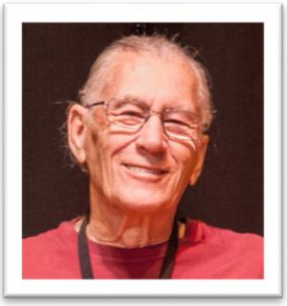
Ben Tarbell, Mike Gerkin, Jim Oliver, Peggy Bullock, Jim Mills, Rick Heesen, Lowell Lee, Steve Andreasen (Apple/Mac), Dick Strong and Art Rice.



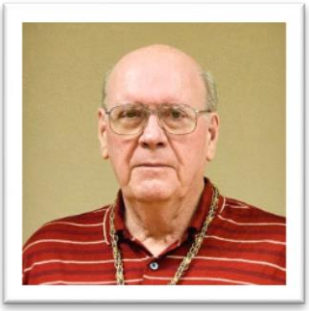








Dick Strong is on “time off” for season 2016-2017.



Greetings

Can you believe it's that time of year again???? Wow! The season at SuperSun sure goes fast! Maybe it's because we are so busy! Or is it the "season of our lives"?? The downhill side seems to go so much faster than it did when I was 18!!

The Tech Committee is keeping me busy sending articles to pass on to you so you will be informed on what is going on in the Technical World. We want you to stay on top of keeping yourself safe while using your computers and other equipment, especially during that time that you are away from us. We know we give you lots of suggestions over the course of the year, now we want to make sure you put those suggestions to use! Remember your maintenance schedule!! Make it a priority!!!

****

Submitted by Mike Gerkin:

Being retired releases one from the daily job, except of course those that the spouse assigns. But being retired also increases your dependence on keeping your financial reserves safe. Protecting your information - financial and personal - is one of your most important retirement roles. Usually, you can use all the help you can find, including listening closely to your financial institution. Below you'll find some easy ways to help keep your accounts safe especially as you begin to use newer technology to communicate and access your financial accounts.

Change Your Password
How many times have we recommended this? Making it a habit to update your Online Banking passwords can be an effective way to help keep unauthorized people from accessing your accounts. Creating a secure password that's composed of an unpredictable sequence of letters and numbers is just as important. Making every password unique is very important.

Keep Your Phone Safe
Your smartphone has much more in common with your computer than with your old mobile phone. For an increasing number of people, a phone has become a device to access almost everything. Criminals know you're literally carrying a small "PC" in your pocket and will do all they can to access your personal information. Following a few simple steps can dramatically reduce your risk of having your money and identity stolen and especially to stay secure for a phone on the go.

Password-protect your smartphone

- Always lock your phone when it's not in use.
- Set your phone to automatically lock after being idle for a set amount of time.
- Set your phone to use a longer and stronger password than the default 4-digit unlock code if this option is available on your phone.
- For even better security, set your phone to erase all data after 10 bad password attempts.

Clear data from your smartphone frequently

- Delete text messages from financial institutions, especially before sharing, discarding, or selling your phone.
- If you visit the bank website using your phone, delete the cookies and cache regularly.
- Better yet, most financial sites use dedicated apps for online banking.

Always download apps from reputable sources

- Criminals try to lure people into signing up for mobile banking using fake apps and/or websites.
- Always visit your bank to verify the sources of your online banking applications.
- If you're considering adding an app to your mobile device, review the app's permissions so you understand what the app is capable of doing before you decide to download it.

Don't fall for phishing scams
Phishing scams attempt to trick you into revealing your bank information or personal information like your Social Security number or Personal Identification Number (PIN).

- Phishers create links that look emails legitimate but instead direct you to malicious websites when you select them.
- Due to the small screen size in smartphones, it's even harder to spot whether a link is legitimate. If you need to access a website, type in the address yourself.

Remove personal information before replacing your smartphone.

- Don't rely on carriers, recycling firms or phone deposit banks to "clean" your phone before disposal or resale to third parties.
- Follow your phone manufacturer's instructions to remove all personal information from your phone before decommissioning it.

If your smartphone is lost or stolen

- First, follow the recommended steps of your mobile service provider to report a lost or stolen phone.
- As always, you'll want to monitor your financial accounts for suspicious activity. If you notice anything that concerns you call your bank right away.

In the end, safety depends a lot on what you do, or don't do.

****

Submitted by Rick Heesen:

Every application adds direct risk

Every application you download and install on your computer – be it your desktop, laptop, tablet, or phone – is an opportunity for your security and privacy to be compromised.

We regularly give applications much broader permissions to operate on our information than they need. In Windows, most programs can read any file, whether they need to or not.

If we want the application at all, we must grant it all the permissions it requests. And that's exactly what most people, including myself, do: zip through the list of permissions requested as if it was a license agreement, and accept it all, without reading or considering.

Any application we install could be malicious. It could be explicitly malicious – meaning malware – or it could be less obviously malicious, sharing more information with third parties than we realize, violating our *assumptions* of privacy.

Even the best-intentioned application includes risk, even if indirectly. The program could have bugs. It could have errors or omissions that, in turn, could be leveraged by other, malicious software. It could "leak" our information unintentionally in ways third parties can intercept and collect.

Again, none of these risks are included purposefully, but rather as a side effect of oversight, poor design, poor coding or other unintentional accidents.

Once again, it all comes back to trust

You and I can't be expected to understand all the details and nuances of software design and marketing. It's too complex and ever-changing.

Instead, we rely on third parties. Or, more correctly, we rely on our trust of third parties to either do or provide the right thing or act as a resource to let us know when the right thing isn't happening.

This is why Leo strongly warns against using download sites. The third parties involved – the download sites themselves – have a poor track record of providing software that can be trusted. Instead, He recommends you take the effort to locate the original vendor of whatever software you're looking for and download directly from that source.

Rule of thumb: don't install what you don't need

Another Rule of Thumb: Make a Restore point before you install any new program

The most secure software of all is the software that isn't on your machine. If it's not there, it can't harm you.

Think carefully before installing any software on your computer or another device. Even the most trustworthy and reputable software comes with side effects of some sort, and in the worst case, as we've seen, there's a risk of more malicious intent as well.

Make sure you need it. Make sure you trust the author. Make sure you get it from a source you trust.

And when in doubt, don't install it. You're safer that way.

- Only install what you need.
- Install only reputable software from well-known sources.
- Download only from the vendor's own download site or instructions.

To read the full article, go to: https://newsletter.askleo.com/ask-leo-642-every-application-adds-risk/

****

Submitted by Ben Tarbell:

We can learn from international attacks

The **Department of Homeland Security** recently released an analysis that they are calling Grizzly Steppe. In reading their analysis, there are clues in how we can better protect and defend ourselves from attacks.

- **Don't open up Word documents you weren't expecting.** So often in these targeted attacks, the attacker uses a Word document attached to an email as an entry point. Modern versions of Outlook no longer are vulnerable in the preview pane, but opening up a document you were not anticipating should never be the first thing you do. I often tell people at ransomware presentations I give that, to the best of my knowledge, I know of no malicious software that goes after both Windows platforms and phone platforms at the same time. Thus if you are ever in doubt over opening an email attachment, take the phone out of your pocket and launch the potentially unknown file on your phone, and not on your computer.

- **Don't follow links to unknown places** Often in these targeted attacks an email will come in enticing the user to click on a link. In the Grizzly Steppe attacks, malicious web pages that were inserted pretending to be Outlook Web access web sites and were used to harvest credentials.

I often see emails coming into my inbox indicating that my apple iTunes need to be reset,
my Google credentials are no good,
or my email access has been limited until I enter in my user name and password.

- **Here's a rule of thumb:** Whenever you get such an email, stop and think if it makes sense to open it.

- **Watch for targeted emails** The Grizzly Steppe attacks used several techniques to target, among them social engineering: sending emails with unique subject lines and attachments that would be enticing to the person that the emails were sent to.

Read and think before you open

Source: http://windowssecrets.com/security-baseline/refresh-your-security-habits-heres-what-you-should-learn-from-recent-attacks/?utm_rid=CPNET000002031327&utm_campaign=4147&utm_medium=email&elq2=a96170167aa14f28ad8c4048e3718946

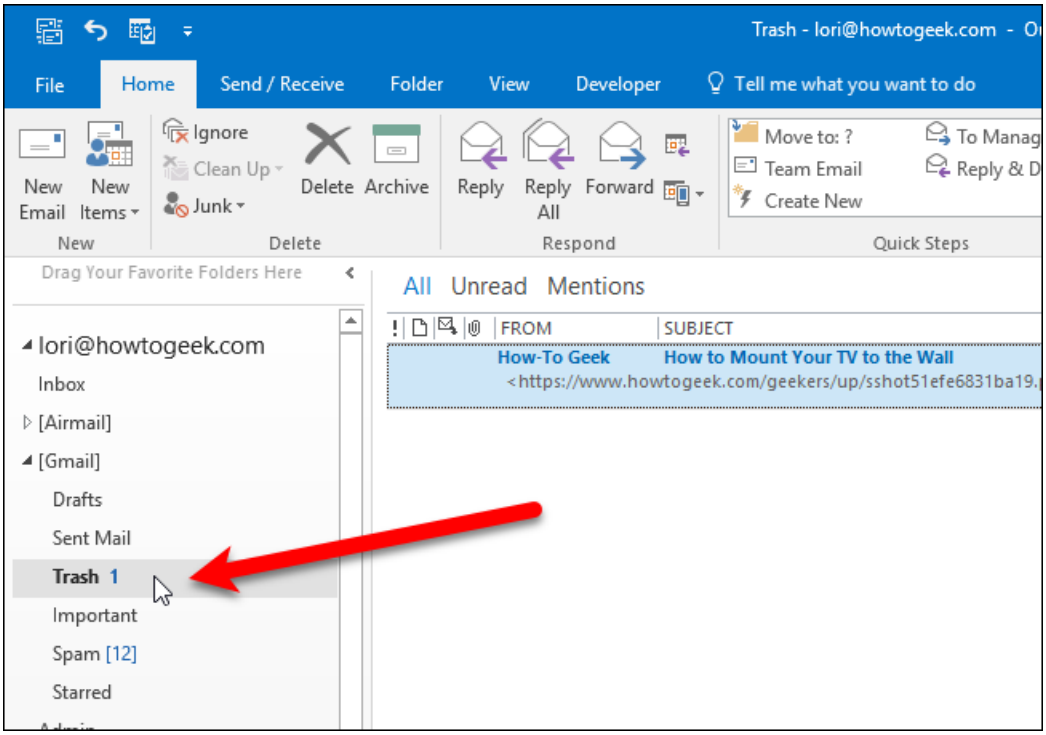
****

Submitted by Ben Tarbell:

How to Mark Messages as Read as Soon as You Click on Them in Outlook

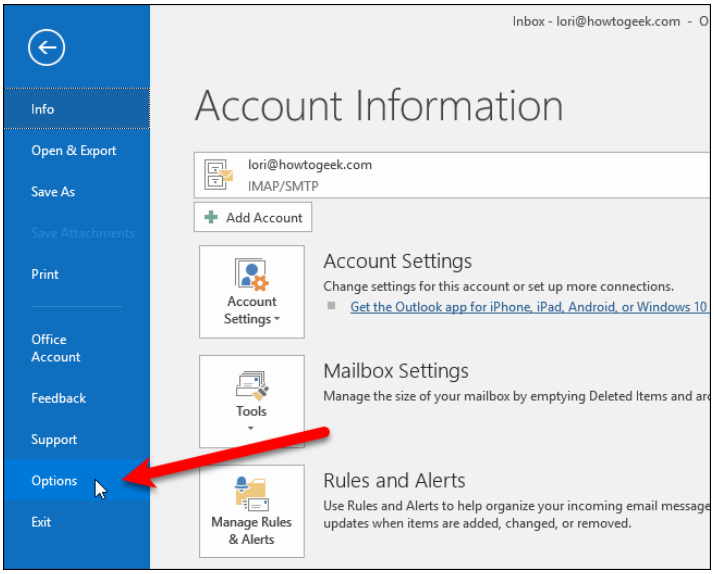
Do you ever feel annoyed that Outlook doesn't mark messages as read as soon as you click and view them in the Reading Pane? Here we show you how to make Outlook mark them as read as soon as they're opened.

By default, Outlook will not mark a message as read until you select another message. This can be annoying, because if you read a message and then immediately delete the message, it shows up as an unread message in your Deleted Items folder.

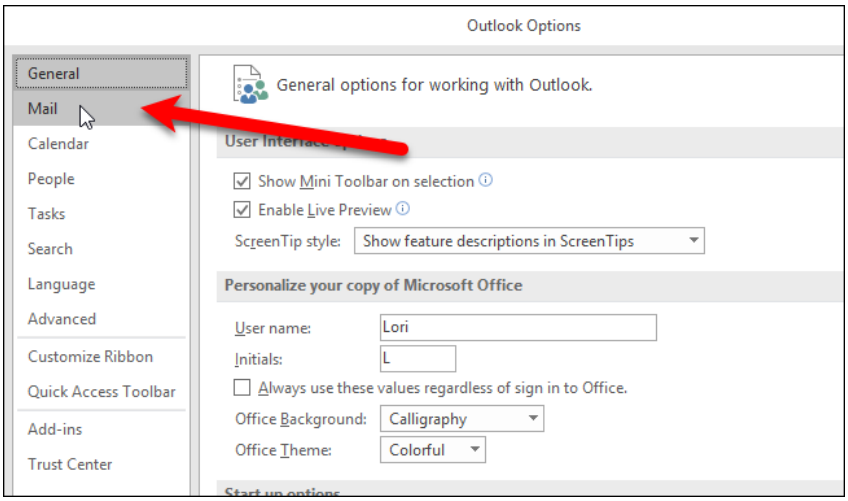


Let's change this to make Outlook mark messages as read as soon as we view them in the Reading Pane. Open Outlook and click the "File" tab.

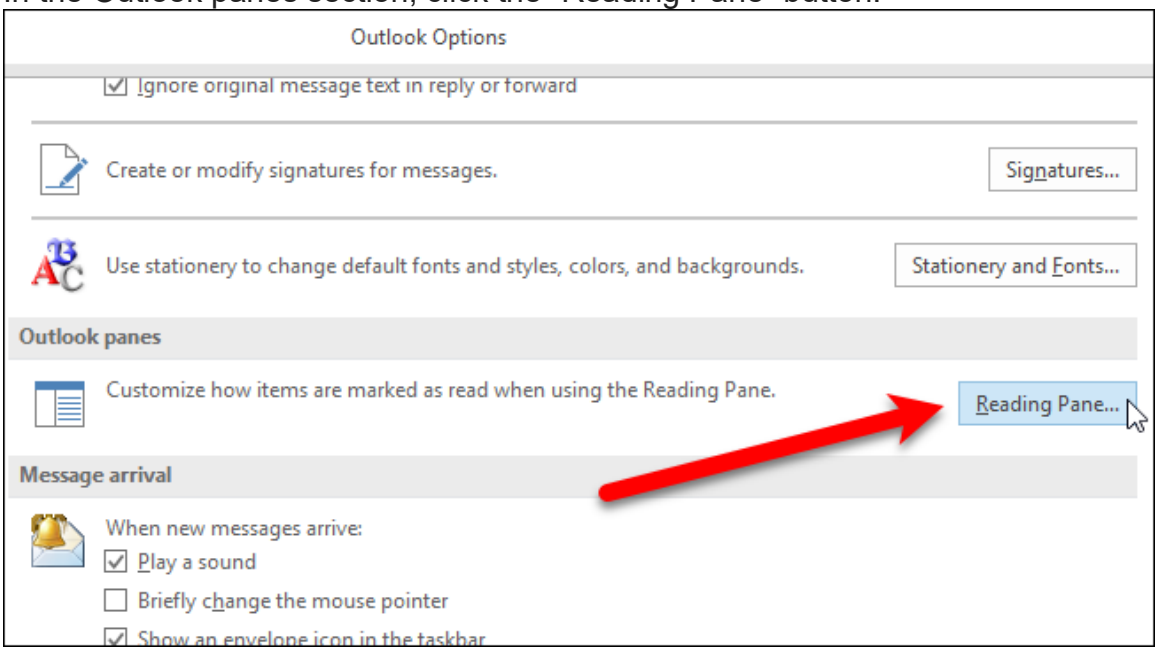
On the backstage screen, click "Options" in the list of items on the left.



On the Options dialog box, click on “Mail” in the list of items on the left.

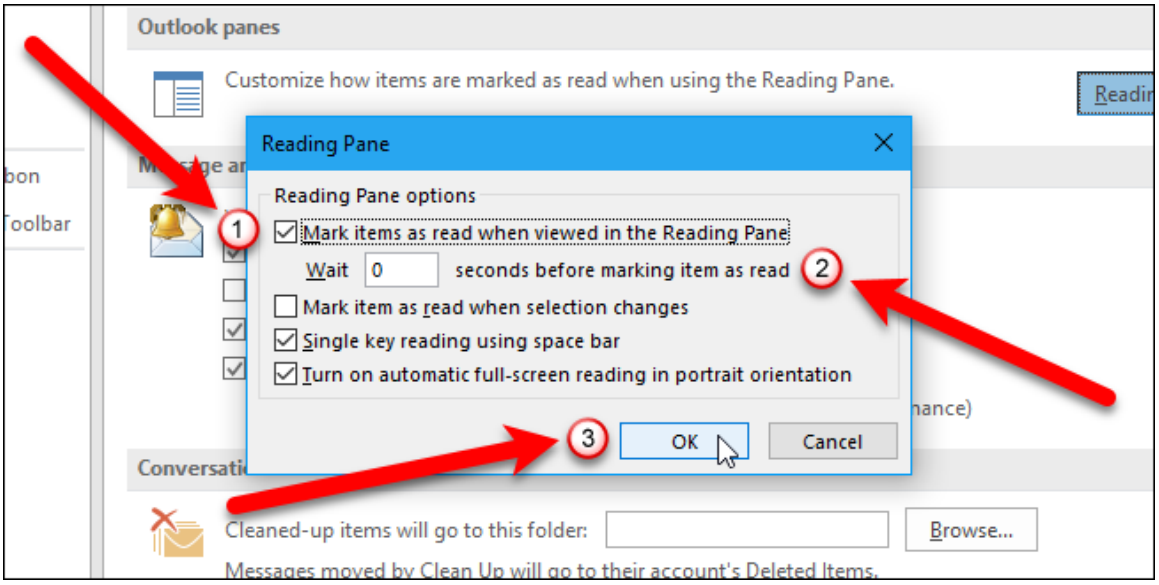


In the Outlook panes section, click the “Reading Pane” button.

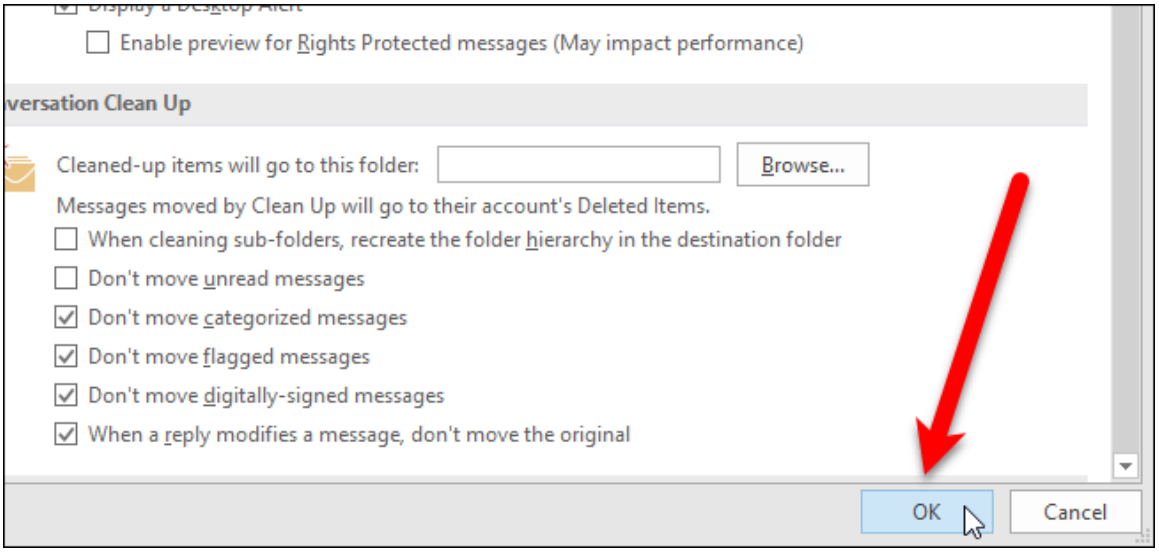


Check the “Mark items as read when viewed in the Reading Pane” box to make Outlook mark your messages as read when you view them in the Reading Pane. By default, Outlook will only mark a message read after you’ve been reading it for 5 seconds, though you can change this. We entered 0 (zero) in the “Wait X seconds before marking item as read” box so our messages would be marked as read as soon as we select them.

Note that the “Mark item as read when selection changes” box is automatically unchecked when you check the “Mark items as read when viewed in the Reading Pane” box. Only one of those two check boxes can be selected at once. Click “OK” to accept your changes and close the dialog box.



Click “OK” on the Options dialog box. Now your messages will be marked as read as soon as you select them in the reading pane, or soon after, depending on how many seconds you told Outlook to wait before marking the item as read.



Outlook is a great email client, but like most programs, it has its quirks. This quick tip can help you get rid of one of Outlook’s annoying features, and make it work like you want it to. You can also disable the Reading Pane if you don’t want messages automatically opened when you select them.

JOIN THE DISCUSSION

Lori Kaufman is a writer who likes to write geeky how-to articles to help make people's lives easier through the use of technology. She loves watching and reading mysteries and is an avid Doctor Who fan.

- **Published 03/9/17**

Source: https://www.howtogeek.com/howto/17948/mark-messages-as-read-in-the-outlook-2010-reading-pane/

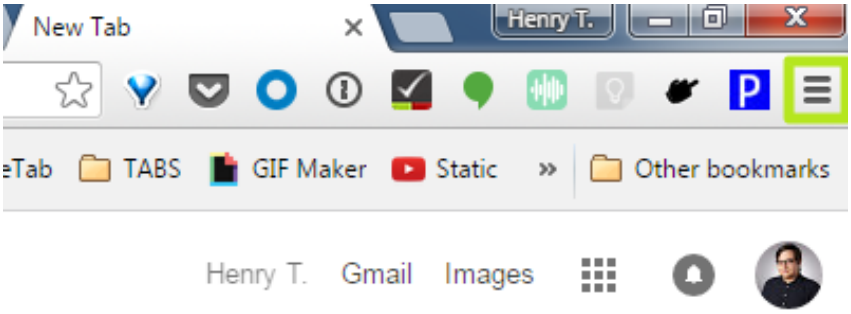
****

Submitted by Ben Tarbell:

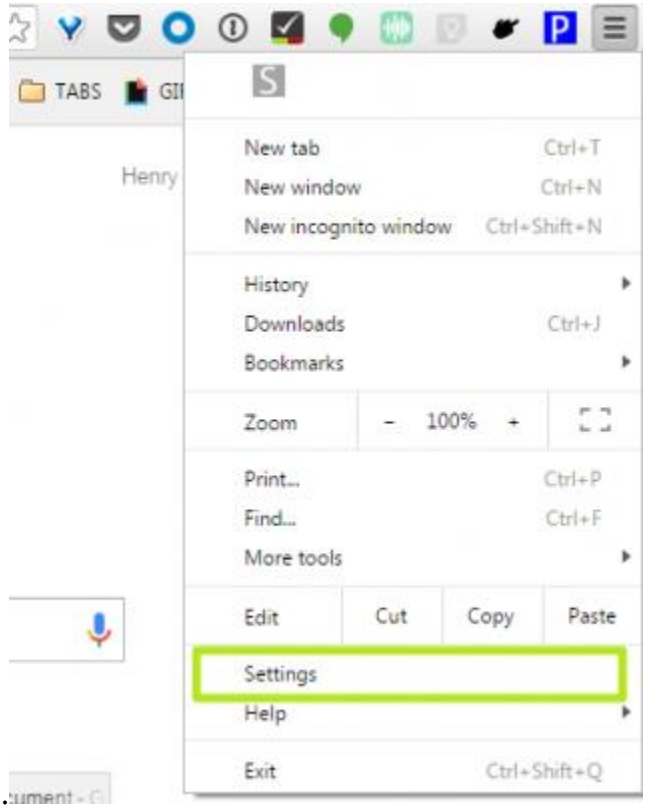
How to Clear Your Internet History in Chrome

Whether you're sharing your computer with your family or giving it away to strangers, there are many reasons to wipe your browser history. Like all web browsers, Google Chrome makes it easy to clear the list of sites you've visited. Here's how.

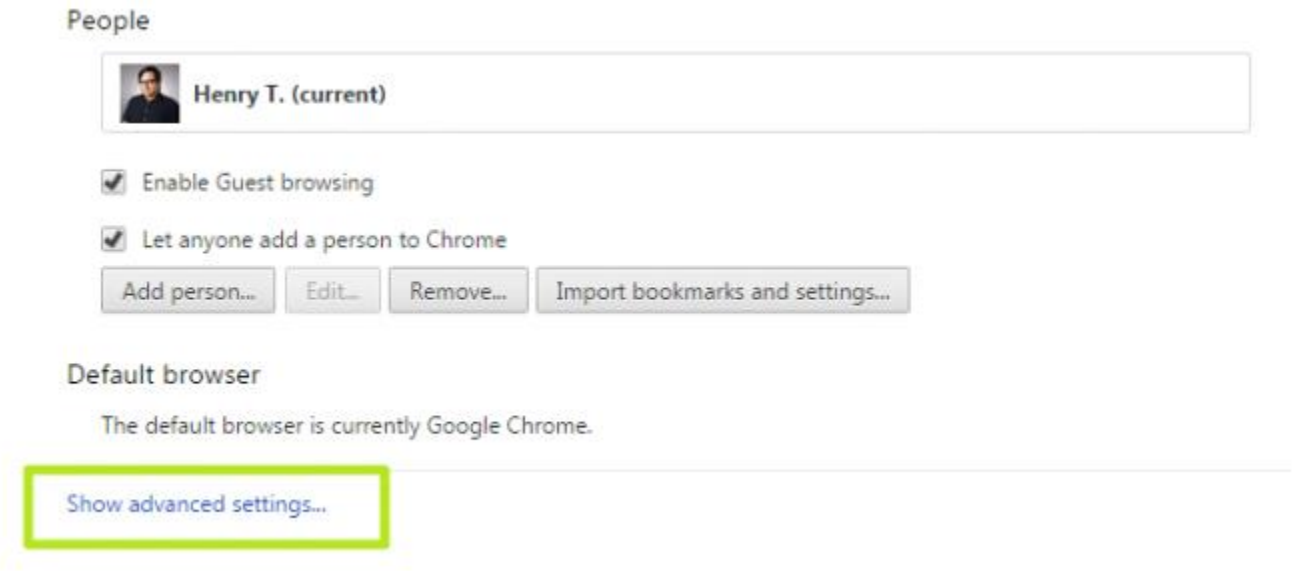
1. Click the Menu icon in the top right corner.



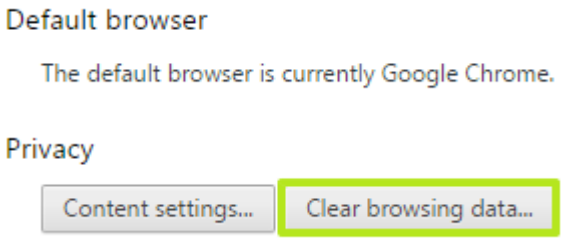
2. Select Settings



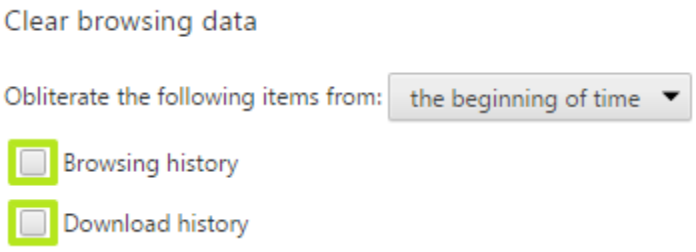
3. Click Show advanced settings



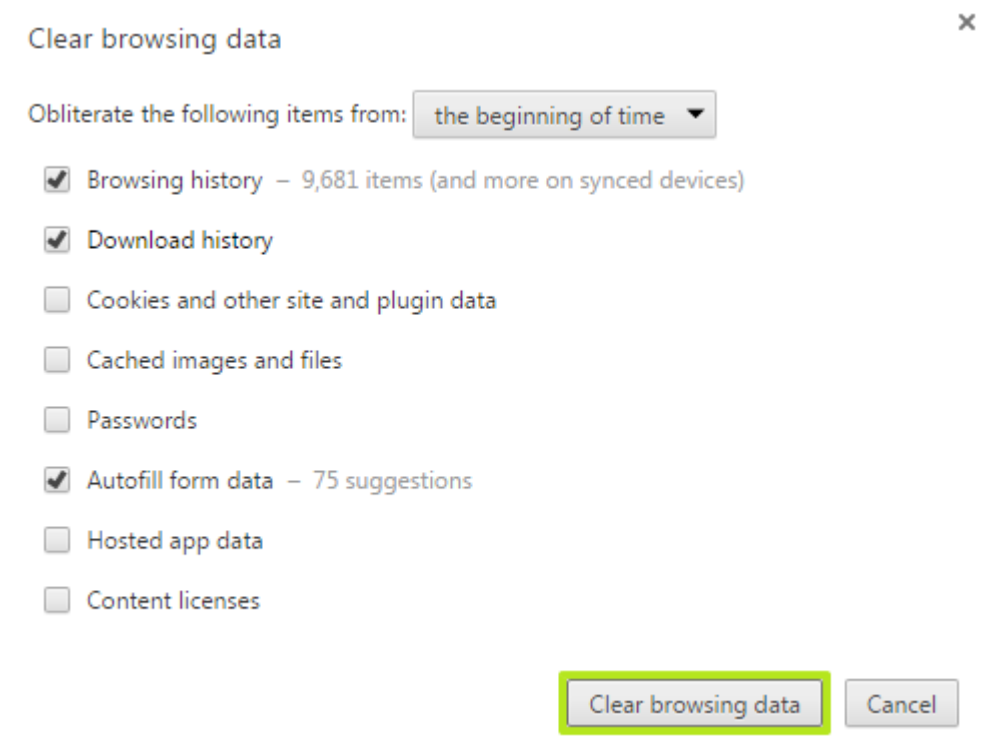
4. Click Clear browsing data…



5. Check the boxes next to Browsing history and Download history. If you want to erase only a specific amount of history, click "the beginning of time" and change it to a different allotment. You can click the other boxes to completely pave your history away, but it just means you'll need to re-login to sites.



6. Click Clear browsing data



You've erased your history in Chrome on this computer.

Credit to: By Henry T. Casey | April 26, 2016 12:30 pm

****

Submitted by Peggy Bullock:

Apple Product users – beware of hackers too! Read this interesting article if you use any sharing or cloud storage. Hackers at work on Apple Products

Source: Kim Komando

****

Submitted by Mike Gerkin:

We are swiftly nearing the time when the computer club season is over for another year. For some who have already left the park we wish you good luck with the snow.

More importantly for those remaining or yet to leave, if your computer does need someone to take a look at it, you had better not wait too long or you will have missed any chance to have the club geeks assist you.

Clean up, problems, questions - your last chance is almost here.

****

Friday Morning Presentations:

March 24	Amazon Echo	Ruth Carpenter
	Google Home "Voice Activated Smart Home Speakers"	Jim Modrell
March 31	Recognition and Farewell	Maurice (Moe) Agnew

****

OPEN LABS

A reminder of the last date for **March Open Labs: March 24th, 10:30am – Noon**. This will be your last opportunity for club members to bring their computer to the Lab to have a member of the Tech Squad help them with something that does not work correctly or some change they need made.

****

A HUGE SHOUT OUT TO ALL THE VOLUNTEERS AND OFFICERS FOR ALL THE WORK THEY HAVE DONE THIS SEASON! WITHOUT YOU, THERE WOULD BE NO SUPERCOM COMPUTER CLUB! TAKE PRIDE IN ALL YOU HAVE ACCOMPLISHED! WE APPRECIATE EACH AND EVERY ONE OF YOU!

Tune in over the summer for more Tech Tips and club announcements. Remember, always check the Website (www.supercomcomputerclub.weebly.com).

Looking forward to another Great Year – 2017 – 2018!!! Hope to see you all back again at SuperCom Computer Club in the Fall. Always something new, always something fun, and always great to see you on Friday mornings!

From Mike Gerkin, Rick Heesen, Ben Tarbell and Peggy Bullock