TC/PC Exists to Facilitate and Encourage the Cooperative Exchange of PC Knowledge and Information Across All Levels of Experience

March 2022

General Meeting
Tuesday, March 8, 2022
7:00 PM

Headless Raspberry Pi, Pi-hole and More

Presenter: Curt Trout

Via Zoom Only

Curt's going to setup a headless (no monitor, keyboard or mouse) Raspberry Pi without ever connecting it to more than a power cord and maybe a networking cable. Then he's going to install Pi-hole, and maybe more. Along the way he'll show a simple way to see what's on your home network.

The Raspberry Pi is celebrating its tenth anniversary and Pi Day is just around the corner. Let's celebrate by taking a look at this useful computer. 🖥

Note: All TC/PC Meetings and SIG Groups will be virtual until further notice. Visit tcpc.com for info.

Tech Topics with Jack Ungerleider via Zoom at 6pm before the General Meeting.

The Digital Viking

Advertising

Full page (7½ x 9½)	**$100.00**
Two-thirds page (7½ x 6)	**80.00**
Half page (7½ x 4¾)	**65.00**
One-third page (7½ x 3)	**50.00**
Quarter page (3½ x 4¾)	**40.00**
Member Bus. Card (2 x 3½)	**10.00**

Multiple insertion discounts available.

Contact Sharon Walbran at:: SQWalbran@yahoo.com

Deadline for ad placement is the 1st of the month prior to publication. All rates are per issue and for digital or camera-ready ads. Typesetting and other services are extra and must be requested in advance of submission deadlines.

Payment must accompany order unless other arrangements are made in advance. Place make checks payable to: **Twin Cities PC User Group**

TC/PC 2021-2022 Board of Directors

Meets once or twice per year. All members welcome to attend.
Visit www.tcpc.com for meeting details.

President —Lee Kaphingst	leekap@comcast.net
Vice President —Curtiss Trout	ctrout@troutreach.com
Secretary - Sharon Walbran	sharon.walbran@gmail.com
Treasurer - Sharon Trout	strout@troutreach.com
Newsletter Publisher Sharon Walbran	952-925-2726 sharon.walbran@gmail.com
Web Master Curt Trout	ctrout@troutreach.com

Board Members:

Steve Kuhlmey	skuhlmey@hotmail.com
Lon Ortner	612-824-4946 lon@csacomp.com
Lee Kaphingst	leekap@comcast.net
Jeannine Sloan	Ambassador for Friendship Village
Curtiss Trout	ctrout@troutreach.com
Sharon Trout	strout@troutreach.com
Jack Ungerleider	jack@jacku.com
Sharon Walbran	sharon.walbran@gmail.com

Newsletter Staff
Editor Sharon Walbran

The Anatomy of a Scam: Ransom for My Files
By Kurt Jefferson, Editor, Central Kentucky Computer Society
https://www.ckcs.org
lextown2 (at) gmail.com

In mid–February, I checked my Gmail account as I do several times a day. Lurking in my Junk folder was a mysterious email message that appeared to come from Germany.

The email address used to send the message might be stolen or forged. But the subject is clear:

Payment for your account.

This is a new form of what's called "ransomware." It used to be that criminals would install software on a user's computer and encrypt all the files – basically locking them so the user can't read them. The victim would get his or her data back after meeting ransom demands.

Hospitals and other health care facilities have been targeted in recent years, and these attacks have escalated.

Now scammers are sending emails containing ransom demands – even without installing any software.

That is the gist of the email I received in my Gmail account. So, it appeared on both my Macs and iPad.

I'm sharing the message with readers of this newsletter to alert you – should you receive a similar threat.

Payment for your account
Feb. 17, 2021 at 4:33 P.M.
From: webmaster@dreirad*******.de
To: Kurt

Greetings!

I have to share bad news with you. Approximately few months ago I have gained access to your devices, which you use for internet browsing.

After that, I have started tracking your internet activities.

Here is the sequence of events:

Some time ago I have purchased access to email accounts from hackers (nowadays, it is quite simple to purchase such thing online).

Obviously, I have easily managed to log in to your email account [email account name deleted].

Obviously, I have easily managed to log in to your email account [email account name deleted].

One week later, I have already installed a Trojan virus to Operating Systems of all the devices that you use to access your email.

In fact, it was not really hard at all (since you were following the links from your inbox emails). All ingenious is simple. =)

This software provides me with access to all the controllers of your devices (e.g., your microphone, video camera and keyboard).

I have downloaded all your information, data, photos, web browsing history to my servers.

I have access to all your messengers, social networks, emails, chat history and contacts list.

My virus continuously refreshes the signatures (it is driver-based), and hence remains invisible for antivirus software.

Likewise, I guess by now you understand why I have stayed undetected until this letter...

While gathering information about you, I have discovered that you are a big fan of adult websites.

You really love visiting porn websites and watching exciting videos, while enduring an enormous amount of pleasure.

Well, I have managed to record a number of your dirty scenes and montaged a few videos...

If you have doubts, I can make a few clicks of my mouse and all your videos will be shared to your friends, colleagues and relatives.

I have also no issue at all to make them available for public access.

I guess, you really don't want that to happen, considering the specificity of the videos you like to watch, (you perfectly know what I mean) it will cause a true catastrophe for you.

Let's settle it this way:

You transfer $950 USD to me (in bitcoin equivalent according to the exchange rate at the moment of funds transfer), and once the transfer is received, I will delete all this dirty stuff right away.

After that we will forget about each other. I also promise to deactivate and delete all the harmful software from your devices. Trust me, I keep my word.

This is a fair deal and the price is quite low, considering that I have been checking out your profile and traffic for some time by now.

In case, if you don't know how to purchase and transfer the bitcoins - you can use any modern search engine.

Here is my bitcoin wallet: (Bitcoin wallet deleted)

You have less than 48 hours from the moment you
opened this email (precisely 2 days).

Things you need to avoid from doing:

*Do not reply me (I have created this email inside your inbox and generated the return address).

*Do not try to contact police and other security services. In addition, forget about telling this to you friends. If I discover that (as you can see, it is really not so hard, considering that I control all your systems) - your video will be shared to public right away.

*Don't try to find me – it is absolutely pointless. All the cryptocurrency transactions are anonymous.

*Don't try to reinstall the OS on your devices or throw them away. It is pointless as well, since all the videos have already been saved at remote servers.

Things you don't need to worry about:

• That I won't be able to receive your funds transfer.

• Don't worry, I will see it right away, once you complete the transfer, since I continuously track all your activities (my trojan virus has got a remote-control feature, something like TeamViewer).

• That I will share your videos anyway after you complete the funds transfer.

• Trust me, I have no point to continue creating troubles in your life. If I really wanted that, I would do it long time ago!

Everything will be done in a fair manner!

One more thing... Don't get caught in similar kind of situations anymore in future!

My advice - keep changing all your passwords on a frequent basis
————————

So there you have it. Obviously, I'm not about to pay a ransom. And my files have not been locked.

Hucksters are sending out these emails worldwide, hoping someone will be terrified and meet their demands. It makes the Nigerian email scams and pleas for help via email (please send money now – John or Mary has been hurt while visiting London or Paris or Sydney or Madrid or…) seem rather tame, doesn't it?

🖥
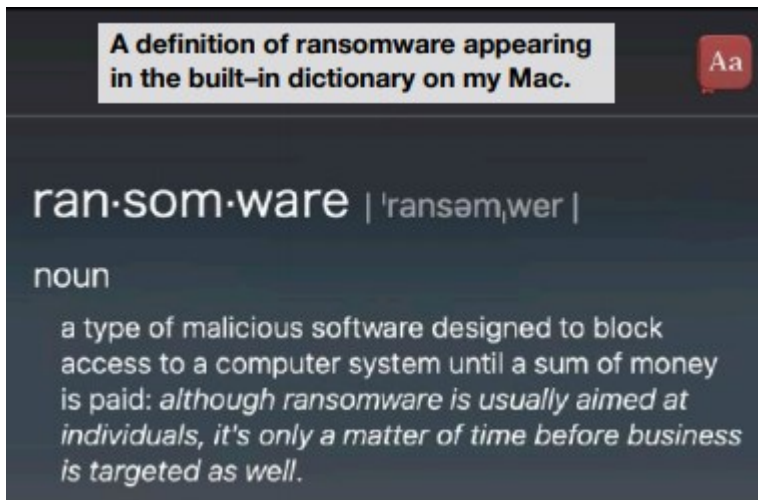
The DealDash (Penny Auction) Scam

By David Kretchmar, Computer Technician
Sun City Summerlin Computer Club
https://www.scscc.club
dkretch (at) gmail.com

If you watch much TV or surf the internet, you've seen ads promising products as much as 95 percent off retail at DealDash.com or other penny auction sites. DealDash advertises itself as offering fair and honest auctions, but is it really? Millions of people have signed up for a chance to buy items at penny auctions at a fraction of the retail price. Who wouldn't want to buy a new iPad for $30? But think about it; who would want to sell that iPad for $30 when it cost several hundred dollars wholesale? It is worth noting that the "penny" in penny auctions refers to the bid increments, but your actual cost could be many dollars.

Consumers are buying more items online every year and appreciate the convenience, selection, and often substantial cost savings. So, these penny auctions would appear to be an extension of that money-saving online buying concept.

Most consumers are familiar with online auctions at sites such as eBay, where interested individuals bid up the price of an item until time expires. The high bidder at the end of the auction wins the item at the winning bid price.

However, another form of online auctions, internet penny auctions, has expanded in recent years. While some of these sites are *technically* legitimate, many of their business practices are questionable, and most consumers would be better off avoiding them altogether.

How penny auctions work

In some ways, online penny auctions are internet bidding sites that share some similarities with legitimate auction sites like eBay. However, the BIG difference is that consumers who bid on penny auctions must pay for each bid they make regardless of whether they win or lose the auction.

Generally, anyone interested in bidding in a penny auction must pay a registration fee before gaining access to bidding. While not required by all penny auction websites, this fee is often described and charged in what many consider an underhanded way. For example, it is typical for a consumer to make a query regarding online penny auctions. If the consumer provides credit card information, that credit card is immediately charged $60 - $99 as part of the registration process. Often consumers provide credit card information without realizing they are authorizing any payment.

An Auction Example

As stated above, penny auctions' business model immediately charges anyone furnishing them a credit card number of at least $60, which buys 100 bids.

Most new bidders bid on one or two auctions, lose their 100 bids ($60), and quickly realize getting a bargain wasn't as easy as it looked. These sites count on the addictive nature of *almost* winning an auction, maybe losing by a penny or two, to encourage a percentage of bidders to buy more bids. Sometimes a substantial discount is offered - i.e., if you sign up right now, you can get 200 bids for the same $60.
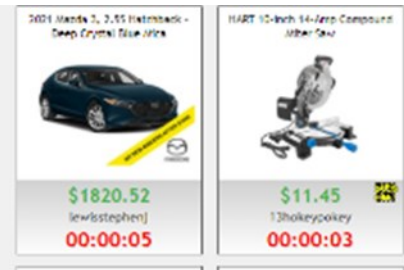
Penny auctions usually allow losing bidders to apply at least part of the money spent on bidding towards buying the product at *their* retail price. However, penny auction sites, including DealDash, often substantially overstate the retail price of items, so buyers are usually either overpaying or perhaps getting completely ripped off.

How the Auction Works

The bidding for an item typically begins at $0 and then increases by one cent each time someone bids. There is a countdown clock that restarts every time someone places a new bid. Some websites even allow users to set up automatic rebids if they are outbid. The total price of the item "won" is determined by the number of bids, so you could end up paying well over the retail value of the item you're bidding on. Generally, you have also lost the money spent on the used bids if you lose the bid.

Let's say the auction is for a new computer with a stated retail value of $599. The bidding starts at $0, increases in 1 cent increments, and one "lucky" bidder "wins" the computer for $30. The winning bidder is given credit for the bids he has "spent" at $0.60 each. It is not unusual to see individuals bidding hundreds of times, so if the winner in this example bid 300 times, that winner paid $180 for their 300 bids, if each bid cost $0.60. Still, this does not seem like a bad deal for the winner; $180 for a $599 computer, even if it is a system, you could get on Amazon for $399.

If a penny auction item sells for $180, the auction site has received 18000 incremental 1 cent bids, which cost the bidders as much as $10,800! Penny auction sites often promote themselves as "social media" buying and stress the social nature of their sites. What they don't advertise is how addicting these sites can be. $10 gift cards can go for over $20 when bidders' egos apparently overrule all common sense. And I can virtually guarantee that YOU will not get that computer for $180.

An individual cannot determine which penny auction sites are "legitimate." Some state attorney generals have found that some penny auction websites use "shills" that automatically outbid people, making it virtually impossible to win items at a reasonable price. Some of these shills are software programs that show a fake username to persuade consumers that they are bidding against a real person. As a result, several penny auction

sites have disappeared, never shipping items won. Other sites have sold financial information about users or put additional charges on credit cards without permission.

Conclusion and Recommendation: Avoid Penny Auctions

While online penny auctions may sound like an attractive deal at first, consumers should be very wary before handing over any money or credit card information. It is doubtful that consumers will save any money by using the service to purchase goods, and much more probable they will be ripped off.
💻

What Is a VPN, and Do I Need One?

By Joel Ewing, President, Bella Vista Computer Club
March 2021 issue, *Bits & Bytes*
www.bvcomputerclub.org
president (at) bvcomputerclub.org

VPN stands for Virtual Private Network. When your computer or mobile device uses a connection to a VPN service, your device behaves as if it were connected to the Internet at the remote VPN service location, and all your traffic on the Internet appears to others as if it originates at that remote location.

In actuality, the Internet service to which you are physically connected is used to establish a secure encrypted connection to your remote VPN service over the Internet. While the VPN service connection is active, your device is configured to reject any other direct network connections, so all inbound and outbound data flows through that encrypted VPN "tunnel" to the VPN server. The VPN server then establishes the final part of the path to the data's intended destination. Data that needs to be returned to your device flows over the Internet to the VPN server and then passes hidden over the VPN tunnel back to your device.

The logical behavior from the viewpoint of your device is as if your device were directly connected to the Internet through an Ethernet cable at the remote VPN server location. Your device is even assigned a LAN IP address on the remote site LAN. Others on the Local Area Network to which your device has physical attachment will be unable to establish connections in or out to your device while the VPN connection is active, and anyone seeing your data traffic either on your physical LAN or as it passes through any routers and the associated Internet Service Provider, will only see that you are communicating with your VPN service and be unable to read the encrypted data content. Note that if you are communicating insecurely with some website (like http vs. https), your communications will still be vulnerable on the Internet between the VPN Service and the destination website.

Reason for Using a VPN

Businesses that allow employees to work from remote locations may host their own VPN

service to allow employees to access corporate network resources securely from a remote location. Suitable restrictions and conventions must be in place to ensure that devices that are not under direct corporate control that connects to the corporate network through VPN are suitably protected so they can't introduce malware into the corporate network.

People who do not use a corporate VPN service to work remotely use a VPN service, not to access resources in the remote network, but to use the remote network merely as a gateway to connect back to the Internet.

If you choose to utilize insecure public Wi-Fi connections with your devices, then by default, anyone else connected to that same Wi-Fi LAN could potentially observe your data traffic, see what Internet sites you are contacting, and observe any un-encrypted data coming from or to your device. If the Wi-Fi network is compromised or misconfigured and there are any security flaws in your device vulnerable to network attacks, your device could also become compromised by malware. The use of a VPN greatly reduces the risks. If your device immediately enters VPN mode upon connecting to a public Wi-Fi, then attacks from other devices on the same local network are blocked, and the most someone else will be able to observe locally about your activity is that you are communicating with and sending unknown data to some specific VPN server.

If you are planning on traveling to a foreign country, you will probably discover that your email services block direct access from a foreign country to reduce spam abuse and that your favorite streaming services have region-specific content restrictions. If you have a VPN Service, you can circumvent those problems by using a VPN server in this country to make it appear you are still in-country, so normal email and streaming services still work. If you have a legitimate need to access foreign-only content, or perhaps a need to verify that some service is indeed blocked in a foreign county, then you can deliberately choose to connect to one of the servers your VPN service provides that is located in a foreign country.

If you are accessing the Internet in a country under an authoritarian government that regards visiting some Internet sites as unacceptable, a VPN service could be part of a means to disguise unacceptable behavior; but under those circumstances, more than just a VPN may be required, as any obvious use of a VPN service could by itself be regarded as an intent to violate restrictions.

Available VPN Services

A search for "VPN services" will locate the most popular services. You may even locate some free services, but I would not be inclined to trust them. Remember that whoever is running the VPN service is the one who CAN observe all the Internet sites you are actually connecting to and any data you might send in un-encrypted form, and they have to fund their service somehow. That would have to be either by data mining for advertisers or restricting service in some way to encourage you to move to a paid plan.

Avast currently provides Avast SecureLine VPN service at an introductory rate of $3.99 /

month or $47.88 for the first year (it looks like their regular price is $89.99/year). Their service supports Windows, Mac, Android, and iOS devices on five devices concurrently.

NordVPN is a very popular service, currently available for a 2-year introductory offer of $3.71/month, $89.00 /2- years. Their regular price appears to be $143.40 / year, making them much pricier down the road, but NordVPN also supports Linux operating systems and allows use on up to 6 devices concurrently.

Unlike an email service or an ISP service, which are a pain to change, changing a VPN service should be simple -- no identity change to communicate to others. Perhaps the best strategy is to use one VPN service provider until their introductory rate expires and then shop for the best offer available at that time.

Caveat Utilitor

Cautionary Tale about Free VPNs
By Joel Ewing, President, Bella Vista Computer Club
April 2021 issue, *Bits & Bytes*
www.bvcomputerclub.org
president (at) bvcomputerclub.org

One of the caveats in the VPN article in the March 2021 *Bits & Bytes*, also mentioned at the March General Meeting, was that free VPN services were not recommended. As if on cue, see the following article recently published by Malwarebytes Labs on "21 million free VPN users' data exposed."

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

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

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

The possibility that a free VPN service may be engaging in questionable behavior and be holding sensitive user data on its servers makes it an extremely attractive target for hackers and data thieves, who can justify spending much time and effort to break in. That makes any collection of sensitive information by a VPN service a more serious concern. One of the suggestions made is that you should look for reviews of a VPN service by known and trusted organizations before deciding on a VPN service. One of the interesting things that this data leak revealed was that there were several differently-named free VPN services that all appear to be run by the same company. These were all supported by mobile apps that were gathering inappropriate data, combined with the attempt to disguise the company's true identity, suggest that this was a deliberate attempt to engage in unethical behavior.

Caveat Utilitor
💻

Special Interest Groups (SIGs)

Most SIGs will meet at Edina Executive Plaza, Conference Room #102, 5200 Willson Road, Edina, MN
Confirm with a SIG group if they meet elsewhere.
For more info contact the SIG Leader(s) listed here.

Get SIG announcements!
Link from www.tcpc.com

Board of Directors*
All members are welcome! Check www.tcpc.com for location.
Selected Saturday mornings

Linux on Saturday
This is for the Linux newbie and those trying to come over from Microsoft to a different operating system.
Second Saturday @ 9 AM-Noon
Note: No Meetings June-August

Jack Ungerleider   612/418-3494 c
jack@jacku.com

Tech Topics
Technical presentation/discussion on various technical topics from the following areas:
- **Web/Internet**
- **Mobile Devices and Apps**
- **Playing with Programming**
- **DIY (3D Printing, R-Pi, other hobby electronics, etc.)**

Second Tuesday @ 6:00-7:00 PM
Every month
Right before the general meeting.

Jack Ungerleider   612/418-3494 c
jack@jacku.com

Microsoft Access
All levels. Presentations by expert developers within the group and by MS reps.
Third Saturday 9:00 AM—Noon
Note: No Meetings June-August

Steve Kuhlmey   952/934-8492
skuhlmey@hotmail.com

Microsoft Office
Addresses the use, integration, and nuances of the Microsoft Office applications.
Combined with Systems on Saturday
Third Saturday of the Month
9:00 AM—Noon
Note: No Meetings June-August

Steve Kuhlmey   952/934-8492
skuhlmey@hotmail.com

Directions to **Accord, 1515 Energy Park Drive** for **General Meetings**:
From I-94 in St. Paul, take the Snelling Avenue exit, then go north on Snelling Avenue about one mile to Energy Park Drive. Take Energy Park Drive and take the first left into the driveway to 1515 Energy Park Drive.
From I-694 or Hwy 36 in St. Paul, take the Snelling Avenue exit, then go south on Snelling Avenue past Como Avenue to Energy Park Drive. Take Energy Park Drive and take the first left into the driveway to 1515 Energy Park Drive.

Directions to **Edina Executive Plaza** for **Systems on Saturday, Access, Word and Picture Perfect SIGs**: Take Highway 100 to the 50th Street/Vernon exit. [If you have come from the north, cross back over Highway 100 to the east side.] Take the first right and go past Perkins [The golf course will be on your left.] and continue on the east frontage road (Willson Road) to the next building—5200 . There is ample parking in the building's lot. Conference Room #102 is on 1st floor.

Help yourself by helping others!
Join the team & share your knowledge with others.

Contact TC/PC at www.tcpc.com

Meetings start at 7:00 PM (9:00 AM on Saturday) unless otherwise noted. *Virtual Meetings during Covid pandemic..

March

April

SUN	MON	TUES	WED	THU	FRI	SAT
		1	2	3	4	5
6	7	8 7pm General Mtg Headless Rasp- berry Pi 6pm Tech Topics	9	10	11	12 Linux on Sat- urday SIG 9am-Noon
13	14	15	16	17	18	19 Microsoft Office SIG (including Access) 9am-Noon
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9 Linux on Sat- urday SIG 9am-Noon
10	11	12 7pm General Mtg TBA 6pm Tech Topics	13	14	15	16 Microsoft Office SIG (including Access) 9am-Noon
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Twin Cities PC USER GROUP

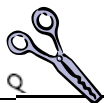## You have just read an issue of The Digital Viking.

Would you like to receive this delivered directly to your email or business each month?

As a member of TC/PC, the Twin Cities Personal Computer Group, one of the benefits
is reading this monthly publication at www.tcpc.com..

As a member of TC/PC, you may attend any or all of the monthly Special Interest Group (SIG) meetings and be eligible for
software drawings. The small membership fee also includes
access to real-live people with answers via our helplines, discounts, and various other perks.

Does membership in this group sound like a good way to increase your computer knowledge?

It's easy to do! Simply fill in the form below and mail it to the address shown.
(If you use the form in this issue, you will receive an extra month for joining now.)

3/22

Here's the info for my TC/PC Membership:

Full name_____

Company name_____

Address_____

City_____ State_____ Zip_____

❍Home ❍Business ❍Change address: ❍Perm. ❍Temp. 'til _____

Home phone_____ Work phone_____

Online address(es) _____

Where did you hear about TC/PC? _____

❍ I DO NOT want any of my information disclosed.
❍ I DO NOT want to receive any mailings

I'm signing up for:

❍ Individual/Family Membership ($18)
❍ Business Membership ($100)
If an existing member your # _____
Make checks payable to:
Twin Cities PC User Group
341 County Rd C2 W
Roseville, MN 55113

http://www.tcpc.com

❍ Check #_____ ❍ Bill me
❍ New member ❍ Renewal ❍ Prior member
I'm interested in:
❍ Training classes ❍ Volunteering
❍ Special Interest Groups: New User, Access, etc.
List here:

Administrative Use Only   Rec'd_____   Chk#_____

March 8, 2022
7:00 pm
General Meeting

Headless Raspberry Pi, Pi-hole and More

Presenter: Curt Trout

Via Zoom Only

Twin Cities
PC USER GROUP

341 County Rd C2 W
Roseville, MN 55113

FIRST CLASS MAIL