



Cathay April 2022

www.cathayradio.org

President: George Chong, W6BUR **email:** W6BUR@comcast.net
Vice President North: Leonard Tom, NX6E **email:** nx6e@hotmail.com
Vice President South: Bill Fong, W6BBA - **email:** w6bba@arrl.net
Secretary/Membership: Rodney Yee, KJ6DZI - **email:** rodyee2000@yahoo.com
Editor: Rodney Yee, KJ6DZI - **email:** rodyee2000@yahoo.com
Treasurer: Vince Chinn aka Mingie, W6EE - **email:** vince@vincechinncpa.com
Web Master: Edison Fong – WB6IQN - **email:** edison_fong@hotmail.com
Mission: The Cathay Amateur Radio Club is basically an active social club of Ham Radio Operators and their spouses. We support local community requests for HAM emergency communications. Several of us are trained in CPR/ First Aid and are involved with community disaster preparedness.

Monday Night Net Time: 9 PM Local Time/PST, Repeater: WB6TCS - RX 147.210, TX 147.810, Offset +0.6 MHz, CTCSS/Tone PL100 Hz

Please note: Repeater: N6MNV UHF 442.700 Mhz, Offset +5MHz, CTCSS/Tone PL 173.8 Hz in South San Francisco is cross linked every Monday Night Net at 9 p.m. to WB6TCS 2-meter repeater.

The CARC Monday night net is the best way to find out the latest club news. All check-ins are welcome.

Message from the President: George Chong, W6BUR

Hello CARC Members and Friends;

Many thanks to Mr. Denis L. Moore – WB6TCS for the use of his repeater for our CARC Monday Night Net.

I wish to thank our CARC members that set aside their valuable time to participate in our Monday night's nets.

COVID-19 Vaccine Update:

On Tuesday March 29, 2022 the FDA has approved a 2nd COVID-19 Booster shot for folks that are age 50 +, that are immunocompromised and previous booster shot taken at least 4 months prior.

For additional information, see link below:

<https://www.fda.gov/news-events/press-announcements/coronavirus-covid-19-update-fda-authorizes-second-booster-dose-two-covid-19-vaccines-older-and>

Chat sub s'em to all you CARC members! - George W6BUR.

Tech Article Introduction:

We have all been bombarded by unwanted cellular/landline phone calls. There are two articles about what you can do about it and about being careful to return calls out of curiosity.

Please go the Tech Article Section for more information.

On a side note: Russian Armed Forces in the Ukraine are using unencrypted civilian cellular phones and unencrypted high frequency (HF) radio to conduct military operations. It seems that the Russian Era encrypted communications are dependent upon local 4G/3G cellular towers that were targeted and destroyed early on in Ukraine special operations. This resulted in Ukrainian Ham operators being able to listen in and record unencrypted tactical Russian military cellular phone / HF radio calls.

Public Service Announcements

HAM CRAM / HAM Licensing

For upcoming HAM Licensing locations please refer to:

<http://www.arrl.org/find-an-amateur-radio-license-exam-session>

Auxiliary Communications Service (ACS)

The Auxiliary Communications Service (ACS) is a unit of trained professionals who supply communications support to the agencies of the City and County of San Francisco, particularly during major events/incidents. ACS goals are the support of gathering and distribution of information necessary to respond to and recover from a disaster.

The ACS Net begins at 1930 hours (7:30 p.m. PT) local time each Thursday evening, on the WA6GG repeater at 442.050 MHz, positive offset, tone 127.3 Hz. The purpose of this net is to practice Net Control skills, practice checking in with deployment status in a formal net, and to share information regarding upcoming ACS events. Guests are welcome to check in. ACS members perform Net Control duty on a regular basis. On the second Thursday of each month, the net is conducted in simplex mode on the output frequency of the WA6GG repeater, 442.050 MHz no offset, tone 127.3 Hz.

ACS holds its General Meetings on the third Tuesday of each month from 1900 hours to 2100 hours local time. Currently meetings are exclusively conducted over Zoom during the COVID-19 pandemic, ACS looks forward to meeting in person again as soon as possible.

Upcoming meeting dates in 2022 are:

- April 19, 2022
- May 17, 2022
- June 21, 2022

Location of in person future ACS meetings are yet to be determined as the regular location is under reconstruction until January 2023. All interested persons are welcome to attend. For further information, contact Corey Siegel KJ6LDJ <kj6ldj@gmail.com>.

For more information, please attend an ACS meeting, check in on the ACS radio net, or call 415-558-2717.

Free Disaster Preparedness Classes In San Francisco – NERT Taught by San Francisco Fire Department (SFFD).

<http://sf-fire.org/calendar-special-events>

NERT APRIL 2022 CITYWIDE DRILL

REGISTRATION: <https://www.eventbrite.com/e/nert-graduates-citywide-drill-tickets-305909693127>

WHEN: Saturday April 16, 2022, 8:30 am-1:00pm **(sign -in from 8:30-9:00a)**

WHERE: 19TH STREET AND FOLSOM STREET, SFFD DIVISION OF TRAINING

WHAT: NERT APRIL CITYWIDE DRILL! Join together with your Team and NERTs from all over the city for the annual April Drill. Bring NERT issued safety gear and wear appropriate safety clothing/shoes, a response “go bag” with flashlight, water bottle, snack etc. Please also bring a filled in [Volunteer Intake Card!](#) PARKING IS

EXTREMELY LIMITED. Further information about the drill will be forthcoming via email to registrants.

+ Recertifications - Coming Soon!

Now that San Francisco has entered the Red Tier for COVID-19 Transmission (see <https://covid19.ca.gov/safer-economy/#county-status> for more details), we are working to schedule recertification trainings for NERTs who were current as of December 2019 or later. Stay tuned for details and times over the next month! jl(At this time, all class 5&6 recerts will take place outdoors only, at the SFFD Division of Training at 19th St & Folsom St in the Mission.)

***SFFD DOT** is the Fire Department Division of Training. All participants walking, biking or driving **enter through the driveway gate on 19th St.** between Folsom and Shotwell. Parking is allowed along the back toward the cinderblock wall.

Visit www.sfgov.org/sffdnert to learn more about the training, other locations, and register on line. Upcoming Special NERT Events.

San Francisco Police Department: Auxiliary Law Enforcement Response Team (ALERT)

The Auxiliary Law Enforcement Response Team (ALERT) is a citizen disaster preparedness program designed. The ALERT program is for volunteers 16 years of age or older, who live, work, or attend high school in San Francisco.

Graduates of the San Francisco Police Activities League (P.A.L) Law Enforcement Cadet Academy are also eligible to join.

ALERT volunteers will no longer need to complete the Fire Department's Neighborhood Emergency Response Team (NERT) (www.sfgov.org/sfnert) training and then graduate into two 8 hour Police Department course specifically designed for ALERT team members.

ALERT members will work closely with full-time and/or Reserve Police Officers in the event they are deployed after a disaster. The Basic ALERT volunteer will have no law enforcement powers other than those available to all citizens.

SFPD ALERT Training (New Members)

The next SFPD ALERT training class has been scheduled for: TBD

* Class date indicated are only for new members

IMPORTANT- All participants must complete the background interview process in order to be eligible to attend the ALERT training class.

Eligible ALERT participants may register for a training class by contacting the ALERT Program Coordinator, Marina at sfpdalert@sfgov.org, or by telephone at 415-401-4615.

SFPD ALERT Practice/Training Drill

All active/trained ALERT members are asked to join us for our next training drill, via scheduled for on

TBD

For more information on the San Francisco Police Department ALERT Program, email us at sfpdalert@sfgov.org, or call Lt. Marina Chacon (SFPD Ret.), SFPD ALERT Program Coordinator, at (415) 401-4615.

For additional information on the web please refer to:

<https://sfgov.org/policecommission/alert>

Tech Article



1. Area Codes You Never Want to Call Back and Why

May 14, 2021

<https://www.thepolicecu.org/blog/blog-detail/the-police-credit-union-blog/2021/05/14/area-codes-you-never-want-to-call-back-and-why>



Given the high volume of robocall disruptions and phone scams that occur every day, most of us know that the most logical, safe response to a call from an unfamiliar phone number generally does not involve answering our smartphone or landline with a warm greeting.

Unfortunately, fraudsters realize that there are times when circumstances may compel us to accept or return a call from a phone number that we don't recognize. By adjusting their methods, they've found new inroads for engaging with potential victims, sparking just enough intrigue or concern to get past the initial distrust.

To stop phone scammers in their tracks, familiarize yourself with these popular tactics to steal your money or personal information, along with the area codes that may alert you to these schemes:

The one-ring scam

Relying heavily on our natural curiosity, this common scam is simple. The phone rings, but before you have a chance to answer it, the call stops. This may happen several times before you respond. If you do answer the phone, the caller drops the line.

But if you call back, you'll likely hear a recorded message, while you're charged expensive international fees that can cost you upwards of \$20 in the first minute. Meanwhile, the criminal collects all or a part of these fees, then moves on to more victims using robocall autodialers that can make millions of calls per day.

Ring and run

Although there are different variations of this con, the common thread is that the scammer attempts to create a sense of urgency. Once you pick up the phone, the caller blurts out a time-sensitive emergency, feigning to represent an agency or organization that can help get you or a friend or relative out of a bind. For instance, they may tell you

that they are a bail bondsman or collection agent, or a member of law enforcement or a hospital's staff.

Once the caller is satisfied that they have your attention, they may hang up the phone suddenly, or request that you call them back. In either case, the goal may be to get you to place a call to a premium-rate phone number, or to deceive you into giving them money directly or access to personal information, such as your bank account or credit card numbers.

Whatever their end game, these scams operate by instilling the need for immediate action. The so-called "grandparent scam" makes use of this strategy, with the caller purporting to be a grandchild who is in jail and needs money for bail fast, or in some other kind of trouble that requires assistance right away.

Watch out for calls from the Caribbean

Criminals often perpetrate the "one-ring" and "ring and run" scam using area codes originating from the Caribbean Area. This is largely because phone numbers from this region may appear to be domestic, since, like the U.S., many of these countries and territories use the country code +1.

As [Inc.](#) magazine explains, the numerous new area codes that have been added in the past twenty years or so have made it easier than ever for criminals to create confusion about which phone numbers are domestic, and which aren't.

[Reader's Digest](#) has provided a helpful list of potentially problematic area codes. Unless you know that a call is legitimate, it's best to avoid calls from the following international area codes with a +1-country code:

- 232: Sierra Leone
- 242: Bahamas
- 246: Barbados
- 284: British Virgin Islands
- 268: Antigua and Barbuda
- 345: Cayman Islands
- 441: Bermuda
- 473: Grenada, Carriacou and Petite Martinique
- 664: Montserrat
- 649: Turks and the Caicos Islands
- 758: Saint Lucia
- 767: Commonwealth of Dominica
- 721: Sint Maarten
- 784: Saint Vincent and Grenadines
- 809, 829 and 849 : The Dominican Republic
- 868: Trinidad and Tobago
- 876: Jamaica

- 869: Saint Kitts and Nevis

Keep your guard up with area codes 712 and 218 — or for that matter, any number you don't recognize

Phone numbers with international area codes aren't the only ones to regard with suspicion. The consumer advice website Clark.com points to a practice among certain rural carriers called "[traffic pumping](#)." Using this controversial practice, certain providers in underpopulated regions charge wireless and long-distance carriers outrageously high fees for calls to local numbers. To ease the burden, providers will share these fees with their subscribers.

The area codes of **712** and **218**, serving Western Iowa and Northern Minnesota respectively, have become notorious for this practice. According to Clark.com, an indication that you're about to be "traffic-pumped" is a message that the call you are trying to place is outside your plan. If this occurs, hang up before the call connects, and you won't be billed.

Because it's easy for criminal callers to use spoofing technology to display a fake phone number on your Caller ID, it's generally advisable to screen any calls or texts from unknown callers. If you do get charged for a fraudulent call, it may be worthwhile to contact your carrier to try to resolve the matter. If the caller persists, file a complaint with the [FCC](#).

To minimize intrusions from scam callers, it can be helpful to use a combination of strategies, such as registering with the FTC's [Do Not Call](#) list, using the call-blocking function on your phone, and even downloading a mobile app to filter out calls that have been previously identified as spam or fraudulent.

Find more tips in our blog post "[Effective Solutions to Stop Spam Calls](#)."

2. Effective Solutions to Stop Spam Callers

Apr 19, 2019

<https://www.thepolicecu.org/blog/blog-detail/the-police-credit-union-blog/2019/04/19/effective-solutions-to-stop-spam-callers/>



Getting fed up with disruptions from robocalls, scammers and telemarketing calls to your mobile phone that encroach on an otherwise productive day?

That stands to reason, given that a March 2019 article from the [USA Today](#) network estimated that unwanted phone calls comprised nearly 30 percent of all calls made in 2018. The same source projects that these calls will surge to roughly fifty percent over the course of 2019, driven largely by the availability of technology that has made it cheap, easy and lucrative to place a large volume of calls in a short timeframe, often using fake (spoofed) numbers.

To defend your sanity, time and security, try using a combination of these strategies to greatly reduce unsolicited calls.

Get on the FTC's National Do Not Call Registry: No one would suggest that you can completely eliminate unwanted calls by registering with the Federal Trade Commission's [Do Not Call list](#), but it won't cost you anything to do it, and it's a good place to start. You can also place your number on this list by calling 1-888-382-1222 from the phone you want to register.

You'll need to wait 31 days for your number to be processed with the registry. As [ConsumerAffairs](#) points out, there are exceptions that make it legal for certain organizations to continue to call you, as in cases involving charitable nonprofits, political campaigns, organizations that are conducting surveys, and companies you've had a relationship with in the last 18 months.

In reality, the Do Not Call Registry works best for filtering out calls from legitimate marketing companies that comply with FTC regulations. Clearly, this does not include fraudulent callers outside of the U.S.

Answer the phone, but say nothing: According to AARP's author of "Scam-Proof Your Life," Sid Kirchheimer, ignoring an unwanted call won't solve the problem if the call gets directed to your voicemail. With a voicemail greeting, it becomes clear to the caller that your number is, in fact, in operation, which won't protect you against future calls.

An option that he recommends instead is to simply answer the phone with silence. Just by saying “hello,” or anything else, auto dialers are prompted to either launch a pre-recorded message (as in a robocall) or to connect you to a live operator, which may use any number of ruses to get you to reveal sensitive identifiable information.

On the other hand, if you say nothing, the call usually disconnects. And if you get a “live” caller?

Kirchheimer suggests waiting for the person to speak, then hanging up if you don’t recognize the voice.

Block the number using your phone’s settings or by contacting your service provider: When you’ve been getting repeat calls from the same offender, easy-to-use call blocking features on your phone come in handy, as they do when you want to avoid calls from a difficult family member or former significant other.

To block a number using your iPhone, tap the small, circled “i” icon to the right of the number you want to block, then you can scroll down to tap “Block this Caller.” If you have an Android, tap the number you want to block, select “Details,” and then “Block Number.”

Another method is to contact your service provider with the specific phone numbers you wish to block. Some providers charge a small monthly fee for this service, while others will do it for free, at least for a short list of numbers.

For details on how to block a number using either your specific phone model’s calling features or your service provider, visit wikiHow’s [“How to Block a Number on a Cell Phone.”](#)

Turn on the “Do Not Disturb” feature: [Forbes](#) suggests this clever tactic for blocking cold calls and fraudulent calls from scam artists before they can start. Just turn on “Do Not Disturb” in your phone’s settings, but select exceptions for your contacts. This is super easy to do from an iPhone. You simply go to Settings, tap “Do Not Disturb,” then select Allow Calls From” then “All Contacts.”

Of course, this means that your phone won’t ring if any new caller reaches out to you, including ones you may actually want to talk to. And you won’t see notifications from these calls either. But you will generally see them as a missed call or voicemail, and you can easily turn this feature on and off. “Do Not Disturb” may not be the solution you employ all of the time, but it could make sense for days when you need to stay on task and steer clear of any extra calls.

For helpful tips on using this feature, check out The New York Times’ article [“How to Use ‘Do Not Disturb’ On Your Phone \(While Still Letting Important Calls Through\).”](#) You can also click [here](#) to find instructions on using “Do Not Disturb” with your Android phone, or [here](#) for an iPhone.

Consider a call-blocking app: There are plenty of useful call-blocking services on the market, which can be great for filtering out calls that have been previously identified as spam or fraudulent calls. Some of these services are offered free, while others charge a low monthly fee.

An excellent choice recommended by [Lifewire](#) for Android users is PrivacyStar. This app not only automatically blocks any number listed in its crowdsourced scam database, but it also lets you blacklist numbers, perform reverse number lookups and quickly file complaints directly with the FTC. You can also use PrivacyStar with an iPhone, but without all of the capabilities available with an Android phone.

A few more suggestions for either iOS or Android: YouMail, RoboKiller and Nomorobo. The FTC also provides the following links to call-blocking apps for specific devices through the CTIA website: [Android](#), [BlackBerry](#), [iOS](#) (Apple), [Windows](#).

Although you may not be able to prevent every nuisance call from reaching you using the tactics listed above, using a mix of the ones that fit best for your situation will go a long way toward minimizing these disruptions. The tips below can also help you handle unwanted calls with finesse:

- Don't take action based on prompts from an unwanted call. For instance, don't press a number to opt out of future calls, because this just validates that the number is current.
- Don't respond to any unsolicited text messages or click on their links (hackers often use texts that look as though they come from legitimate companies).
- Beware of calls that are dropped or just ring once—this is a popular ploy to get you to call back.
- Beware the following area codes, which are from Caribbean countries that charge high rates: 268, 284, 876 and 809.
- You can report unwanted calls at [ftc.gov/complaint](https://www.ftc.gov/complaint). Keep in mind that the more complaints there are, the more likely a phone number will be blocked from all phones.