



You Heard it through...

THE GRAPEVINE

October, 2017

Vol 90, No. 2

October Meeting, Thursday, Oct 12, 7 PM

District Fall Conference in San Jose, October 28

Once again, the San Jose, a.k.a. Silicon Valley, AHEPA family is hosting the annual Fall Conference. This is a don't-miss event that all brothers and sisters ought to attend. Aside from District Lodge visitations, it is the one occasion when we can get together, compare notes, network, and remind ourselves that there is an entire AHEPA world outside the chapter.

A registration form is included with this newsletter. Be sure to get it in as soon as possible.

WARNING

There is an email going around offering processed pork, gelatin and salt in a can.

If you get this email, do not open it. It's spam.

BEWARE!!! It Never Stops!

We have had occurrences recently of malicious spam attempts. Sometime in August, e-mails were received seemingly from brothers in the district requesting a transfer of money from district funds. Fortunately, the attempts were recognized as being bogus and no damage was done.

More recently however, the "Stuck in Ukraine" scam appeared again, only in a more subtle form. First, a very cryptic

message was received by a number of our chapter members appearing to be from one of our brothers. It only stated that he needed a favor. When anyone responded, a follow-up message was received stating that he was stuck in the Ukraine because he lost his wallet and had to freeze his bank account. A loan of \$1,500 would get him home. Instructions would be sent on how to transfer the money.

The brother who supposedly sent the e-mail was in church the day before and couldn't be in the Ukraine. That should have been the first clue that this was bogus. Other clues

included the fact that no recipient address was given. When the perpetrator responded, his e-mail address had changed. Checking the header showed no other information. To send a message with no recipient requires a fairly sophisticated understanding of the e-mail system. The second message stated that his bank account was frozen. This is never necessary. When cards are lost, cancelling the cards is all that is required. It is a good practice to keep a backup card list in the event you find it necessary to do this. Don't keep it in your wallet, or any bank account numbers.

All of these were clues, but the simple fact is that this is an old scam that has been used for years. There are others, the Nigerian prince comes to mind, and they keep being repeated because, for all the publicity and experience with them, they still work. This is because the victims of these scams forget some basic rules.

First, if it smells like a rat, it sure isn't a swan. The first message was entirely out of character for the purported sender to begin with. A cryptic request for help is dubious on its own merits but it didn't fit his character. Second, if money or account information is requested, **DO NOT RESPOND!!!** I cannot emphasize that enough. The first line of defense is never responding to anything that cannot be independently confirmed. In this particular case, asking the sender to call you, or checking with someone who might know his whereabouts, or even calling him will quickly tell you that it is a scam.

There are many others, I constantly receive e-mails warning me that my e-mail account is frozen because I have too many messages and I must confirm my details with the included link. Or my bank experienced a false access attempt and my bank account is frozen. There are many variations on this, most often for banks where I do not have accounts. Always it includes a link to verify my information. This is always to a site that is not the bank and will simply result in your information falling into unfriendly hands. It is identity theft and you will have willingly made yourself a victim.

If you do not use e-mail, or online banking, do not be smug. There are numerous phone scams. Been called by the IRS lately? Was your grandson stuck in Mexico? Did you get a call to renew a magazine? I have experienced all of these more than once. I know of instances when the grandson scam nearly worked. Typically the caller greets you with, "Hi, Grandpa!" That is a quick tip-off for me as my grandsons always call me Papou. Arranging a code word for such possible events is a good way to protect against scammers. As with the e-mail scams, the most important rule is **NEVER RESPOND, NEVER GIVE ACCOUNT INFORMATION, NEVER, NEVER, NEVER SEND MONEY!!!**

It is disheartening at times to recognize just how much of this there is. The internet is a great tool and I cannot imagine life without it now. At the same time it has made any thoughtful person aware of how far the cheats and con-artists will go. Though we don't hear much about it, there is constant effort being made to block these attempts. You can do your part if you will **be vigilant and be aware** of the possibilities. The best defense is not to respond at all, and if you think you must act, verify independently that is safe to do so. We were lucky this time. I just hope that our luck will hold.

GOLDEN GATE DISTRICT 21 AHEPA FAMILY



FALL CONFERENCE



SATURDAY, OCTOBER 28, 2017
HOSTED BY THE SAN JOSE AHEPA FAMILY
ST. NICHOLAS GREEK ORTHODOX CHURCH
SMALL HALL
1260 DAVIS STREET - SAN JOSE



WELCOME/CONTINENTAL BREAKFAST 9:30AM
COMBINED AHEPA & DAUGHTERS MEETING..... 10:30AM
LUNCHEON 12:00PM
INDIVIDUAL AHEPA & DAUGHTERS MEETINGS..... 1:00PM
ADJOURN ABOUT 4:00PM

RESERVATION FORM - BY MAIL, PHONE OR EMAIL
(PLEASE! RESERVATION DEADLINE MONDAY, OCTOBER 23, 2017)

NAME _____ CHAPTER _____

NAME _____ CHAPTER _____

PHONE (_____) _____ EMAIL _____

NUMBER ATTENDING _____ @ \$35.00 PER PERSON AMOUNT ENCLOSED \$ _____

PLEASE ENCLOSE CHECK PAYABLE TO DOP #21 AND MAIL TO:



LINDA BELBA
107 MIDDLE PARK DRIVE
SAN JOSE, CA 95135
EMAIL: LJBELBA@YAHOO.COM
PHONE: (408) 238 7732