EMAIL SAFETY TIPS

As Newcomers Club becomes more digital in our communications, we want to share with you some email safety tips.

DO:

- Only open emails from someone you know. Common scams can look like official sites (phishing). See note below for more information.
- Always confirm that the incoming email address is truly official.
  Newcomers Club publishes email addresses in the Roster. If you are unsure of an incoming email but you think it may be a member, you can double check an email address by checking the Roster.
- Use an anti-virus software and/or a spam filter.
- Remember to sign out, especially if you are using a public computer.
- Change your password frequently and do not share it with anyone. Use strong passwords.

DON'T:

- Never open an attachment within an email from an unfamiliar person or company.
- Do not reply to or click on links or attachments inside unexpected (spam) emails. Instead, on a separate browser tab, enter the official URL for the site you intend to visit.
- Never send sensitive information such as passwords, social security number, or bank account numbers via email.

Phishing /fishing/ noun
DEFINITION: a scam by which an Internet user is duped (as by a deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly

HOW TO RECOGNIZE PHISHING ATTEMPTS:

- Messages that contain threats to shut your account down
- Requests for personal information such as Passwords or Social Security numbers
- Words like "Urgent" – false sense of urgency
- Forged email addresses
- Poor writing or bad grammar

MAKE SURE YOU IDENTIFY THE "REAL" SENDER ADDRESS:
Although most email programs (like Yahoo, Gmail, and Apple Mail) now do reveal the sender's actual email address, some still do not. To find out how to see your email carrier header, click https://whatismyipaddress.com/find-headers for more information.