SENECA FALLS ROTARY

Club Officers (2019-2020)

President-Rhonda Jasper

Pres Elect-Linda Knight

VicePresident-Wendy Freidman-Kolsin

Secretary-Kathy Jans Duffy

Treasurer-Rich Fredenburg

Past President-Dave Markel

Directors

Class of 2020 Liz Becht

Class of 2021 Jolene Steele

Tim Ryan

Class of 2022 Cindy Ody-Ortego

Dave Swenson

Fred Capozzi

Club Committees & Chairs

Administration: Tim Ryan

Community Service: Kathy Jans-Duffy/Linda Knight

Foundation: Tim Ryan

Fundraising: Linda Knight/Wendy Freidman/Kolsin

International: Dave Markel

Literacy: Liz Becht

Membership: Rhonda Jasper

New Generations/Youth-Liz Becht

Public Relations-Jolene Steele/Susan Backlund

Sunshine/Social-Jolene Steele

Weekly Spokes

March 24, 2020

Club Announcements:

Ted and Fred went to Dickman's Farms last week and spoke to Kate Ward, the Green House Manager. To get some ideas for the lower flower bed at Stanton Park. She drew up some designs and suggested some plants for that area.

Chocolate Extravaganza is postponed for now, but the committee is working to secure a new date

Trips & Happy Dollars:

Dave S-Kids threaten they would never see grandkids again if they didn't quarantine, so they are in quarantine! Wandering trails of Seneca Meadows wildlife trails

Kathy-Happy getting in 2 walks per day

Tim - Back from Sanibel. Tough to beat sun and 80 degrees! Had visits by with immediate family as well as friends and Wendy's brother, Phil. Dave and Melissa Markel joined the fun! The Boys went fishing, the Girls went on a shelling trip to Cayo Costa, an outlying island north of Sanibel. Sanibel is one of the shelling capitals of the world. His daughter Emily continues to seek for the rare Junonia.

Mark- Enjoyed lots of sunny weather over the weekend and lots of good crisp fresh air.

Phil-Since I am elderly over 70 with pre-existing conditions person, I no longer have visits with my children and my wonderful granddaughter; but Kate and I are able to laugh and talk with them via Skype. I had never used Skype. I am so grateful for this technology which allows me to share with my family. Now, we need newer tech which will allow hugs and kisses!

Jim S-Happy thought for my wife's 60th birthday on Wednesday, March 25th!

Linda K-Our family instituted the practice of Sunday dinner several years ago. The grandchildren always look forward to this day when all of us get together over a nice dinner. (at least they do for now – when teenagers… not so sure) Anyway, in deference to the state requests, we cancelled Sunday dinner this past Sunday and did "take-out meals" from Nana and Papa's house. I guess it is a sign of the times that the grandchildren have asked that the next Sunday dinner be done with "Zoom" (the online meeting app)…. Happy but sad also.

SENECA FALLS ROTARY

Today's Guests & Visitors

Club Member's Rotary Anniversaries

March
Al Johnson-52 years
Barry Bradshaw-46 years
Susan Backlund-18 years
Jerry Macaluso-18 years
Jamie Damouth-4 years
Jerry Moran-2 years

Club Member's Birthdays

March
Rich Fredenburg
Mike Mirras

Important Dates & Reminders

Upcoming Programs

Today's Program/Speaker info:

During a time of national crisis is when fraudsters try and take advantage and often use a disaster as a tool for instigating attacks. Here are some tips to remember how to continue to focus on online safety!

Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

- Natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- Epidemics and health scares (e.g., H1N1, COVID-19)
- Economic concerns (e.g., IRS scams)
- Major political elections
- Holidays

What are common indicators of phishing attempts?

- **Suspicious sender's address.** The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.
- **Generic greetings and signature.** Both a generic greeting—such as "Dear Valued Customer" or "Sir/Ma'am"—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.
- **Spoofed hyperlinks and websites**. If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.

HOVERING DOES NOT MEAN CLICKING. NEVER CLICK ON LINKS WITHIN AN EMAIL YOU ARE NOT EXPECTING.

SENECA FALLS ROTARY

Covid-19-Know how it spreads!

- There is currently no vaccine to prevent coronavirus disease 2019 (COVID-19).
- **The best way to prevent illness is to avoid being exposed to this virus.**
- The virus is thought to spread mainly from person-to-person.
    - Between people who are in close contact with one another (within about 6 feet).
    - Through respiratory droplets produced when an infected person coughs or sneezes.
- These droplets can land in the mouths or noses of people who are nearby or possibly be inhaled into the lungs.

Take steps to protect yourself and protect others

- Wash your hands with soap and warm water for at least 20 seconds, especially after being in public, after sneezing, coughing or blowing your nose.
- Avoid close contact with people who are sick
- Put distance between yourself and others (at least 6 feet!)
- Stay home if you are sick
- Cover your mouth and nose with a tissue when you sneeze or cough and throw tissue in trash.
- Clean AND disinfect frequently touched surfaces- phones, doorknobs, light switches, counters, desk, toilets, keyboards & faucets

The most important thing to do is to stay home, only going out for essentials keeping that to a minimum. Groceries, Bank, Doctor, etc.

- **Spelling and layout**. Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.
- **Suspicious attachments.** An unsolicited email requesting a user download and open an attachment is a **common delivery mechanism for malware**. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

What is a vishing attack?

Vishing is the social engineering approach that leverages voice communication. This technique can be combined with other forms of social engineering that entice a victim to call a certain number and divulge sensitive information. Advanced vishing attacks can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity (ID) to be spoofed, which can take advantage of the public's misplaced trust in the security of phone services, especially landline services. Landline communication cannot be intercepted without physical access to the line; however, this trait is not beneficial when communicating directly with a malicious actor. This is often attempted with someone trying to pose as a member.

What is a smishing attack?

Smishing is a form of social engineering that exploits SMS, or text, messages. Text messages can contain links to such things as webpages, email addresses or phone numbers that when clicked may automatically open a browser window or email message or dial a number. This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity. There are many different smishing attacks that have already begun. Some examples include a promise of relief funds from the government and links to short term relief loan applications.

It is always important to protect your personal information. Often during these times, the bad guys come out to take advantage of our fear and vulnerabilities. Stay smart, stay safe and share this information with your loved ones.