Be Scam Aware

Lifespan of Greater Rochester Inc.

www.lifespanrochester.org

585-244-8400

About Lifespan

A regional nonprofit organization dedicated to providing information, guidance and 30+ services for older adults and caregivers.

Lifespan helps older adults take on the challenges and opportunities of longer life.

Formed in 1971. 160 staff. $12 million budget.
Federal, state, local funding. Foundations.
United Way, fundraising & service fees.

Lifespan
take it on!

Scam Updates

1. COVID 19 Virus
2. 2020 U.S. Census
3. Federal Stimulus
4. Why older adults are targeted
5. Romance scams – how they work
6. Reporting scams
7. Resources

U.S. Department of Justice COVID-19 Scam Advisory

Verify the identity of any company, charity, or individual contacting you regarding COVID-19.

Check websites & email addresses offering information, products, or services related to COVID-19. Scammers use addresses that differ only slightly from those of the entities they are impersonating. **E.G. “cdc.com” or “cdc.org” instead of “cdc.gov.”**

Be wary of emails offering information, supplies or treatment for COVID-19 or requesting your personal information for medical purposes. Legitimate health authorities do not contact the general public this way.

Do not click on links or open email attachments from unknown or unverified sources. Doing so could result in a malware or virus download.

Make sure your anti-malware and anti-virus software is operating and up to date.

COVID-19 Scam Advisory

Ignore offers for a COVID-19 vaccine, cure, or treatment. If a vaccine becomes available, you won't hear about it for the first time through an email, online ad, or unsolicited sales pitch.

Check online reviews of any company offering COVID-19 products. Avoid companies whose customers have complained about not receiving items.

Research charities or funding sites soliciting donations for COVID-19 causes. An organization may not be legitimate even if it uses words like "CDC" or "government" in its name, or has reputable-looking seals or logos. Visit the Federal Trade Commission website on hints for donating wisely.

Check any business, charity, or individual requesting payments or donations in cash, by wire transfer, gift card, or through the mail. Never send money through any of these channels.

Be cautious of COVID-19 "investment opportunities" based on claims that a company's products or services can help stop the virus. Carefully research before you invest. Avoid investment fraud by visiting the U.S. Securities and Exchange Commission (SEC) website.

Lifespan
take it on!

Beware of:

Individuals and businesses selling fake cures for COVID-19.

“Phishing” emails from scammers posing as the World Health Organization or the Centers for Disease Control and Prevention (CDC).

Malicious websites and apps appearing to share COVID-19 related information but lock your devices until payment is received.

Entities seeking fraudulent donations for illegitimate or non-existent organizations.

Scammers posing as medical providers asking for patient information for COVID-19 testing; then using the information to fraudulently bill for other tests and procedures.

Websites Offering Fake COVID-19 Cures

Court papers filed 3/21/20, the website: “coronavirusmedicalkit.com” engaged in a wire fraud scheme seeking to profit from the confusion and widespread fear surrounding COVID-19.

The website claimed to offer consumers access to World Health Organization vaccine kits for a shipping charge of $4.95, which consumers paid by entering credit card information on website.

For the most up-to-date information on COVID-19, consumers should visit the Centers for Disease Control and Prevention (CDC) and WHO websites

The public is urged to report suspected fraud schemes related to COVID-19 by calling the National Center for Disaster Fraud (NCDF) hotline (1-866-720-5721) or by e-mailing the NCDF at disaster@leo.gov.

For information about the Department of Justice’s efforts to stop COVID-19 fraud, visit www.justice.gov/coronavirus. Additional information about the Consumer Protection Branch and its enforcement efforts may be found at www.justice.gov/civil/consumer-protection-branch.

Census Scams

In March, U.S. households received a Census Bureau mailing on how to do the census online, by phone or by mail.

The Census Bureau won't send an unsolicited email requesting that you answer the census.

The Census Bureau is warning people to avoid fraud and scams online, on the phone or in person.

Beware of phishing emails to get personal information. Stay away from fake websites. Don't click on strange links, which might lead to malware, which is malicious software designed to damage a computer, server or computer network.

If you suspect fraud, call the Census Customer Service Contact Center at 800-923-8282.

April 1 is Census Day. By then, every household should have received an invitation to participate in the count.

Between May 28 and August 14, census workers will visit households that haven't completed the census. For additional information, check out the 2020 census website.

Census Scams

No payment or fee attached to completing the census. The Census Bureau won't ask for:

- A contribution or processing fee.
- Your Social Security number.
- Your credit card number, debit card number, a bank-routing number or account number associated with any of your financial holdings.
- Your computer passwords.
- Your political affiliation or beliefs, or a donation to a political party.
- Your religious affiliation or beliefs.
- Your driver's license number.
- Your citizenship status.
- Your passport number.

Census Scams

Approached by someone about completing the Census?

Verify identity by checking for:

- A valid ID badge with photograph, a US Commerce Department watermark, an expiration date.

Still in doubt?

Close door. Call the Census Bureau at 844-330-2020.

COVID-19 Stimulus Scams

Phony emails or calls asking for personal and banking information to claim $1,200 check.

Government agencies are NOT sending unsolicited emails or calling for private information.

Facebook posts targeting older adults about special grants to pay medical bills from non-existent “U.S. Emergency Grants Federation.”

Scams promising quick grant payment for personal information and a “small processing fee.”

Emails from uscovid19treasure@gmail.com. The subject of the email is COVID-19 PANDEMIC STIMULUS PACKAGE. The email promises a $1,000 check as part of the stimulus package, requires fee and PII.

Report COVID-19 scams to FBI ‘s Internet Crimes Complaint Center at ic3.gov.

Scams Target Older Adults…

Trust – older adults raised in an era of trust.

Isolation – less visible in society.

Loneliness – eager for social contact.

May be less savvy about online and high-tech dangers.

Incidence of dementia; loss of capacity to weigh financial risks.

Older adults usually have more assets than young people. It's where the money is!

Scams Impact on Older Adults

- Loss of trust in others & loss of security.
- Feelings of fear, shame, guilt, anger, self-doubt, remorse, worthlessness.
- Depression, isolation, possible substance abuse, even suicide.
- Financial hardship- inability to replace lost assets through employment.
- Inability to hire attorney to pursue legal protections and remedies.
- Becoming reliant on government ‘safety net’ programs.
- Inability to provide long term care needs.
- Loss of primary residence.

How Criminals Get Information

- Scams
- Google/open source
- Genealogy sites
- Social media
- Data breaches
- Purchase info (often from Dark Web)
- Hacking
- Theft (mail, records, dumpster diving, burglary/robbery, etc.)
- Victim (or family member) supplies it
- Family or associates (including “helpers”)

Romance Scams

- More money is lost in romance scams than any other type of scam.
- Scammers use psychology of loneliness to build hope of a relationship.
- Scammers identify victims through personal profiles posted on internet dating sites, looking for assets.
- Scammer contacts victim, begins grooming process to develop trust.
- After trust forms, scammer invents an endless series of situations requiring money. (Rochester man lost $1.1 million in a romance scam in 2019.)

The FBI says that the common thread running through most romance scams is an open personal profile on an internet dating site ("Tinder," "Plenty of Fish," etc.)

Lifespan
take it on!

Romance Scams

- Too hot to be true – good looking photos with tales of financial success.
- In a hurry to get off the site – trying to move communicating to email, messenger or phone.
- Moving fast – speaking of a future together and falling in love quickly, often saying they have never felt this way before.
- Talk about trust – manipulating victim with talk about trust and how important it is – the first step to asking for money.
- Don’t want to meet – often traveling overseas or in military.
- Suspect language – claims to be from same hometown but has poor spelling and grammar, flowerly language, phrases that don’t make sense.
- Hard luck stories – before asking for money, scammer sets the stage with a tale of woe – car stolen, injury, unfair arrest, illness, etc.

FIGHT IDENTITY THEFT

FREEZE YOUR CREDIT BUREAU ACCOUNTS (FREE)

REQUEST A COPY OF YOUR CREDIT REPORT (FREE)

Equifax
1-800-685-1111
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-680-7289
www.transunion.com

Counties Covered for One-0n One Advocacy by Lifespan

- Monroe
- Chemung
- Genesee
- Livingston
- Ontario
- Orleans
- Steuben
- Schuyler
- Seneca
- Wayne
- Wyoming
- Yates
- Others upon request for phone consults

Fighting Fraud Websites

www.fraud.org
Fraud.org helps protect consumers from being victimized by fraud.

Do Not Call Registry
1-800-382-1222; www.donotcall.gov

Unsolicited credit and insurance offers
1-888-5-OPT-OUT (1-888-567-8688); www.optoutprescreen.com

www.charitywatch.org/charities

www.nomorobo.com

National Do Not Mail List

AARP (www.aarp.org/technology/privacy-security)
The AARP website provides specifics on internet safety, how to protect your privacy, and the most up-to-date virus protections.

U.S. Senate Special Committee on Aging
Fraud Hotline: 1-855-303-9470

FBI (www.fbi.gov/scams-safety/fraud/seniors/)
This is a list of common fraud schemes aimed at older Americans.

www.seniornet.org
SeniorNet offers computer training at senior centers, public libraries, schools, and hospitals as part of their mission to provide older adults computer technology education.

Contacting Lifespan

Monroe, Genesee, Orleans, Wayne, or Ontario Counties:
Leita King, MSW
Office: 585-244-8400, ext. 171
cell: 585-287-6371
lking@lifespanrochester.org

Livingston, Wyoming, Seneca, Schuyler, Steuben, Chemung,
Yates or other New York state counties:
Dave Long, Ed.D.
cell: 585-287-6371
dlong@lifespanrochester.org