

# S C A M S

---

## What to Avoid!

Presented by:

Linda-Lee “L-L” DiVecchia & Wolfgang Druen

# NOTE:

Some presentation materials were excerpts  
from the following web links:

---

<https://www.slideshare.net/Roel6865/scams-andfraudpresentation>

(noted by “R” on bottom left corner of slide)

and

<https://www.slideshare.net/hstallard/frauds-and-scams-autosaved>

(noted by “H” on bottom left corner of slide)

# FRAUDS & SCAMS

---

Anyone can be victim of a fraud or scam,

**BUT**

**9 out of 10** times the **elderly** are targeted because they have:

**Pensions**

**Saving Accounts**

**Money Marketing Accounts**

**Jewelry**

**And.....**

**Are Usually More Trusting !**

# General Tip-Offs to a Fraud or Scam

---

- 1. They Contact You First.**
- 2. Information that Only You Know.**
- 3. They Use Phrases Like : Hurray, Today Only, Last Chance!**
- 4. It Is a Get Rich Quick Thing.**
- 5. Sounds Too Good to be True.**
- 6. They Want Money Up Front.**
- 7. They Need Your Credit Card Number, Bank Account Number, or Check Number.**
- 8. They Use Scare Tactics ... If You Don't Do This Now, It Will Cost You Later!**
- 9. They'll Say You Don't Need to Check This Offer Out with Your Family, Lawyer, Accountant, or Better Business Bureau**

# What is a Scammer's GOAL ?

---

## MONEY !

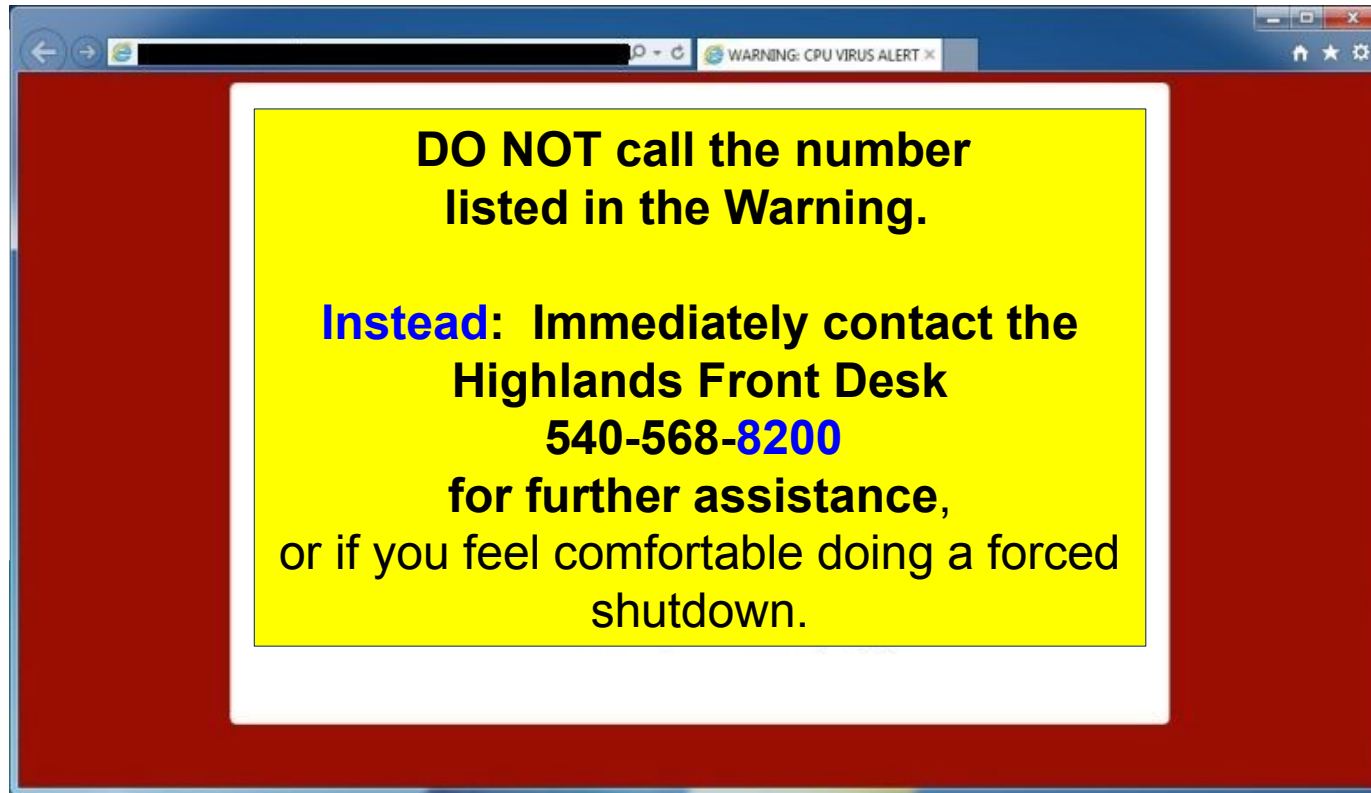
- Money They Can Get Directly from You
- Information that Can Be Sold for Money (**Think Identity Theft!** )
- Control of Your PC that Could Be Used to Generate Money By:
  - Using Your PC to Send **Spam**
  - Hold Your PC Hostage  
(Lock You Out from Using Your Keyboard, etc.)

**NOTE: SPAM is like Digital Junk Mail that Comes in Your E-mail Inbox,  
BUT SPAM Can also Have a Link to a SCAM!**

# Scareware AKA Rogue Software

- **FAKE security software**
  - **Gets You to Load Malicious Software AND**
  - **Gets Your Personal / Credit Card Info !**

Nearly Half Of  
Tech Support  
Scams  
Begin With an  
Alert on the  
Victim's  
Computer  
Screen.



# WINDOWS Service Center Call

---

- You receive a phone call from a man claiming to be from Microsoft's "Window Service Center" (usually has an Accent!)
  - Caller states your computer has lots of malware on it which is showing up at Microsoft
- Talks you through opening a Windows Viewer to see errors and warnings "proving your PC needs his help."



**One response is to ask which computer – as you have several !**  
**Sometimes they will ask for an IP address on your computer.**  
**Tell them you don't know what that is, and then say "GOOD-BY!"**

## Windows Defender - Security Warning

\*\* ACCESS TO THIS PC HAS BEEN BLOCKED FOR SECURITY REASONS \*\*

Your computer has alerted us that it has been infected with a Trojan Spyware. The following data has been compromised.

- > Email Credentials
- > Banking Passwords
- > Facebook Login
- > Pictures & Documents

Windows Defender Scan has found potentially unwanted Adware on this device that can steal your passwords, online identity, financial information, personal files, pictures or documents.

You must contact us immediately so that our engineers can walk you through the removal process over the phone.

Call Microsoft Support immediately to report this threat, prevent identity theft and unlock access to this device.

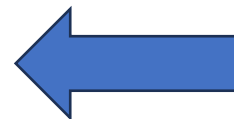
Closing this window will put your personal information at risk and lead to a suspension of your Windows Registration.

Call Microsoft Support **1-855-630-5187 (Toll Free)**

## Is an 855 Area Code a Scam or Fraud?

- **855 Area Codes Have a Reputation for Being Used in Scam Calls—and, Sadly, This is Not Unfounded.**
- **The 855 Area Code Number and Other Similar Toll-free Codes are Very Popular Amongst Fraudsters.**
- **Be Careful; Don't Give Out Any Information Until You Know the Person You're Speaking to Is Absolutely Legit.**

**This 855 Area Code and Phone # is a SCAM !**





# PHISHING

---

- **Phishing – “Spoofed” E-mails and Fraudulent Websites Designed to Fool Recipients into Divulging Personal Information**
- **E-mails Look VERY Authentic with Company Logos and Link to Authentic Looking Web Sites**
- **According to the FBI, Phishing Scams Led to Losses of More Than \$43 Billion Between 2016 and 2021.**

**8.8 Billion in 2022 Alone**

# Report the SCAM

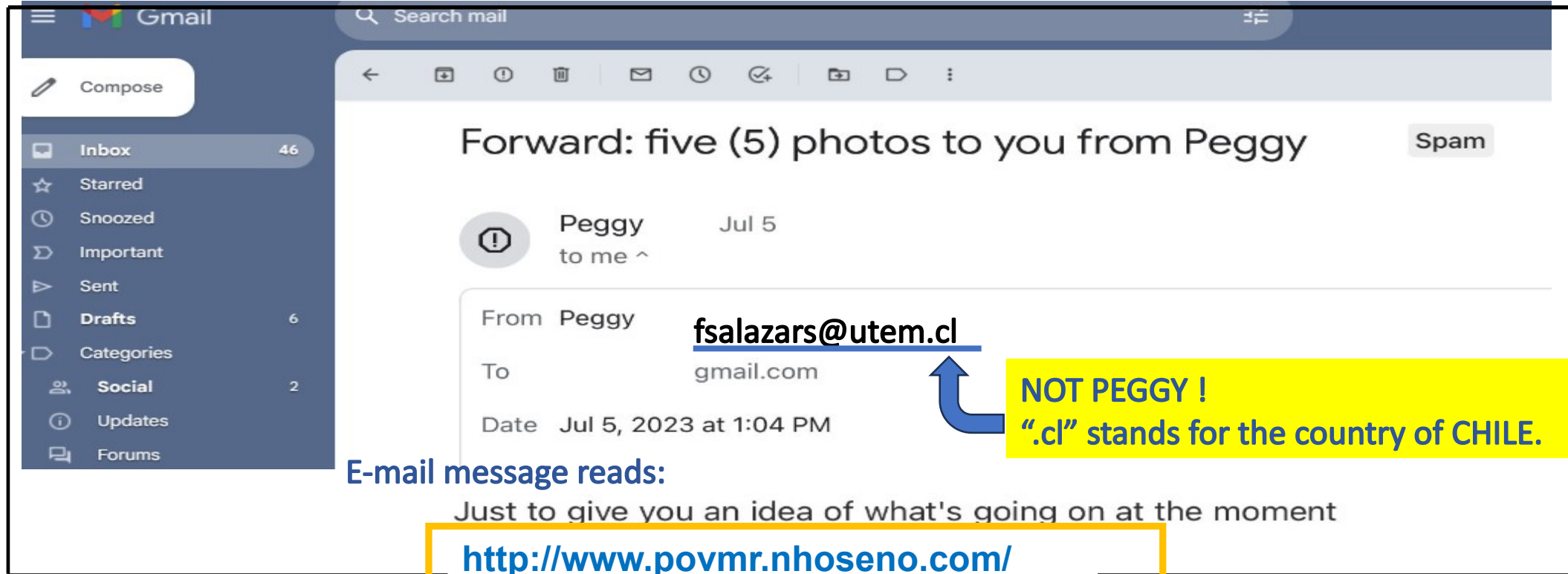
---

- The FTC : [report-fraud.ftc.gov](https://report-fraud.ftc.gov)
- The FTC's identity theft site: [identifytheft.gov](https://identifytheft.gov)
- The FBI's Internet Crime Complaint Center: [ic3.gov/Home/ComplaintChoice](https://ic3.gov/Home/ComplaintChoice)
- The Better Business Bureau: [bbb.org/scamtracker/reportscam](https://bbb.org/scamtracker/reportscam)
- Others : [Fraud.org](https://Fraud.org)  
[aarp.org](https://aarp.org)

# “CLICK HERE” Scams

This e-mail appears to come from my friend “Peggy”

Peggy’s e-mail has been hacked.



Now, this bogus e-mail wants me to click on the link to view some “Pictures”.

*That’s not going to happen!!!*

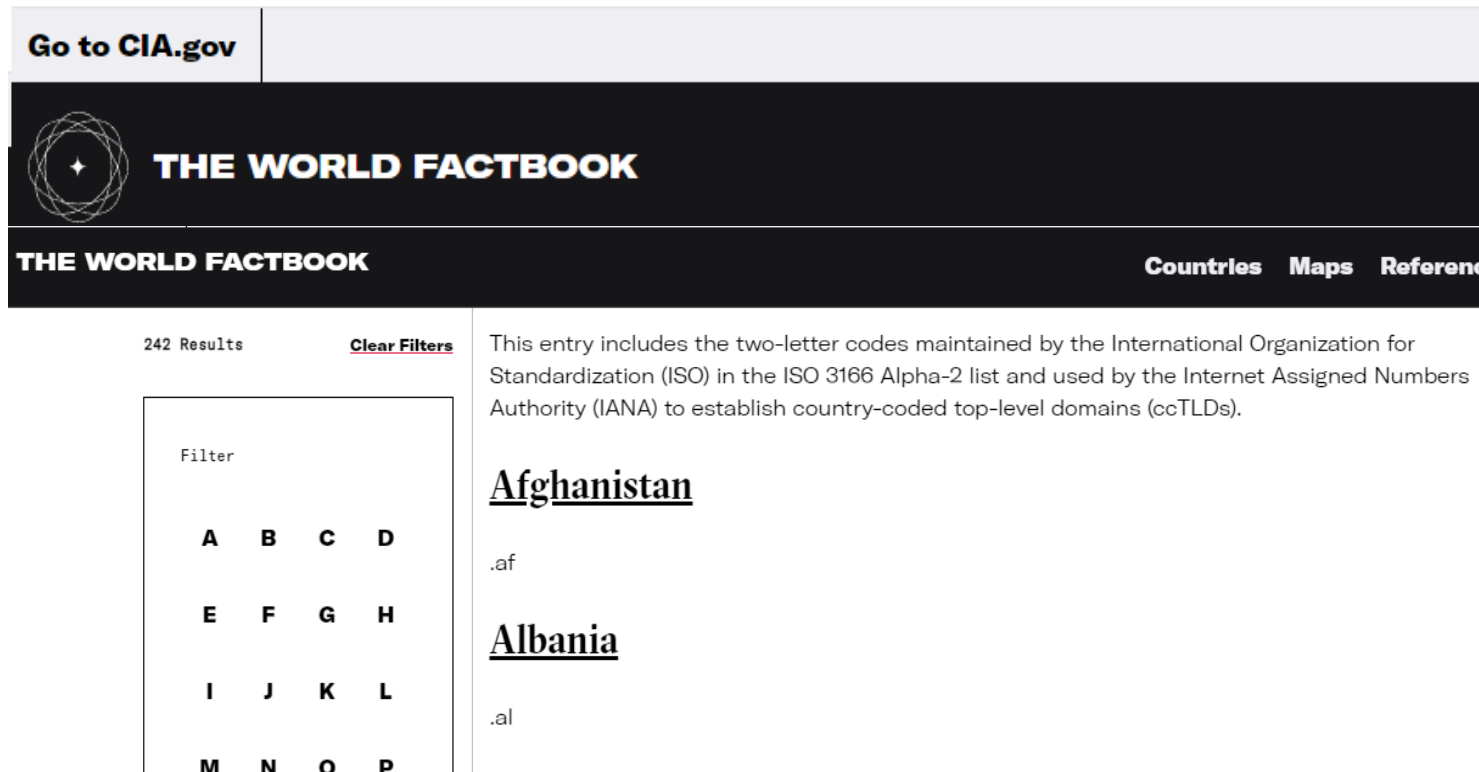
I have these e-mails go automatically to my “Spam” folder, for deletion.

# How to Find Country Codes

There are Several Searchable Websites that Will Show the Country Codes.

Here is one of these:

Go to CIA.gov



The screenshot shows the CIA World Factbook interface. At the top, there is a navigation bar with "Go to CIA.gov" and "THE WORLD FACTBOOK" logo. Below the logo, there are links for "Countries", "Maps", and "Reference". The main content area shows search results for "Country Codes". On the left, there is a filter menu with letters A through P. The main text area displays the entry for "Afghanistan" with the code ".af" and "Albania" with the code ".al". A descriptive paragraph explains that these codes are maintained by the International Organization for Standardization (ISO) and used by the Internet Assigned Numbers Authority (IANA) to establish country-coded top-level domains (ccTLDs).

242 Results [Clear Filters](#)

Filter

A B C D

E F G H

I J K L

M N O P

This entry includes the two-letter codes maintained by the International Organization for Standardization (ISO) in the ISO 3166 Alpha-2 list and used by the Internet Assigned Numbers Authority (IANA) to establish country-coded top-level domains (ccTLDs).

[Afghanistan](#)

.af

[Albania](#)

.al

**F Y I dot extension indicators:**

▪ **.com**

Commercial (for-profit) websites

▪ **.net**

Network-related domains

▪ **.org**

Non-profit organizations

▪ **.edu**

Educational institutions in the US

▪ **.gov**

US government entities

▪ **.mil**

US military use

yahoo!mail

Advanced



Compose



Restore to Inbox

Move

Delete

Not Spam

**LOOK!**  
**I HAVE AN IMPORTANT E-MAIL FROM AMAZON !**  
**OH, NO! MY AMAZON ACCOUNT IS LOCKED!**  
*(Yes, this really did come into my e-mail.)*

Last week

Spam



update@info-amz.com



Account Locked. ID : MTMGQM-RGYIFPX Billing Information Issues

Account Locked. ID : MTMGQM-RGYIFPX

update@info-amz.com <aeklfvzbzuhdwiof-zenym-zzxmdewfsnntiuq@ovk7xmlfdnbsya1.buzz>



NOT  
AMAZON  
ICON !

This e-mail was  
NOT sent by  
AMAZON!  
Look at the full  
name of the  
sender!

Billing Information Issues

Hello @yahoo.com,

We placed a temporary hold on your account due to a billing issue. Due to a problem with your card , we have been unable to charge your bill.

To unlocked your account, you can click button below and proceed with identity verification to prove that it is your account.

Account Verify

To resolve this issue, please verify with the billing name, address, and the telephone number registered to your payment method If you have recently moved, you may need to updates this information with the card issuer seperately.

We appreciate your patience with our security measures.

Thank you for your concern.

Sincerely,  
Amazon

Services. Inc. is a subsidiary of Amazon.com. Inc. Amazon.com is a registered trademark of Amazon.com, Inc. This message was produced and distributed by Amazon Services Inc. 410 Terry Ave. North. Seattle. WA 98109-5210

# The REAL AMAZON e-mail.....

The screenshot shows a Yahoo! Mail interface. At the top, there is a navigation bar with links for HOME, MAIL, NEWS, FINANCE, SPORTS, ENTERTAINMENT, LIFE, SEARCH, SHOPPING, YAHOO PLUS, and MORE... Below this is the 'yahoo!mail' logo and a search bar with an 'Advanced' dropdown and a search icon. On the left side, there is a 'Compose' button. The main area displays an email from Amazon.com with the subject 'Act now: Grubhub+ free for two years'. The email header shows 'Amazon.com <store-news@amazon.com>' and the date 'Sat, Jun 17 at 1:20 PM'. A contact card is overlaid on the email content, featuring the Amazon logo, the text 'Amazon', the website 'www.amazon.com', the phone number '(206) 266-2992', and social media icons for email, Facebook, Twitter, and LinkedIn. Below the contact card, it says '+ Add to contacts'. At the bottom of the card, it reads 'Auto generated card visible only to you'. Below the email content, there is a copyright notice '© Amazon.com' and a disclaimer: 'Product prices and availability are subject to change. Ref: 646720740.' and a link to 'Privacy Policy'.



Compose

← Back

Archive

Move

Delete

Spam

Get Your New Surge Mastercard Right Here Right Now!

Yahoo/SPAM P...



Surge Mastercard <sara@mybunwarmer.com> [Unsubscribe](#)



Sun, Jul 2 at 11:36 PM



This message contains blocked images. [Show images](#) or [Always show images](#)



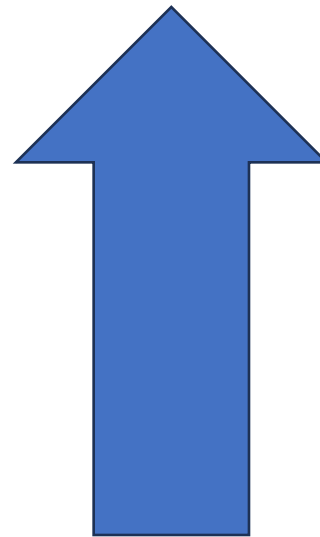
GIVE YOUR CREDIT  
A SURGE!



- Get Your New Surge Mastercard Right Here Right Now!



• **Surge Mastercard** <sara@mybunwarmer.com> [Unsubscribe](#)



WHY DON'T YOU WANT TO CLICK  
ON THIS "BOGUS" E-MAIL'S  
UNSUBSCRIBE BUTTON?

# Possible E-mail Option

---

- If you currently have an e-mail where all your friends, family, and businesses connect with you, you may want to **create an e-mail just for your friends and family to correspond with you.** (Keep the **old** for **business**, and add **new** for **family/friends**)
- **Your bank, investment firm, and doctor(s) can also be part of this new e-mail.**
- **Those that you do online business with – keep in your current “old” e-mail.**
- **When a company or new business contact asks for your e-mail – give them the one that you use just for business.**
- **Not sure of a “new” acquaintance – you may want to give them the business e-mail for starters.** When you feel that **you can trust him/her**, then **you can choose to give them your family/friends e-mail address.**

# PHONE SCAM ALERTS - the GOOD, the BAD, the UGLY

---

## THE GOOD

- Call Identified as a Large Bank
- Caller Stated Someone Had Made a \$4k Charge to Her Credit Card and They Flagged It as Potential Fraud.
- Asked Her to Identify Her Card's Expiration Date so They Could Deny the Charge.
- Caller Said They Were Trying to Save Her Money from a Fraudulent Charge.

**She Refused.**

- Asked if She was Born in a Certain Year - **They Had the Year Correct.**

**She Didn't Confirm.**

- They Continued to Pressure Her.

**She Hung Up.**

**She Immediately Called the Telephone Number for the Bank Listed on Her Credit Card (Very Similar Number as the One from the Scammer).**

**Asked for the Fraud Department.**

**Bank Person told Her the Call was Phishing and She had No Charges Pending.**

### IMPORTANT TO NOTE:

**All of the Info About Us is Available to a Scammer on the Internet (State, Year Of Birth, Telephone Number, Etc).**

# PHONE SCAM ALERTS - the GOOD, the BAD, the UGLY

---

## THE BAD

*L-L Scammed - Prior To Living At Sunnyside, About 6 – 7 Years Ago.*

- Received a Call Identified as **Best Buy**
- Caller Stated They Were **from Direct TV** – Had a Great Deal to Save Us Money
- They Knew – **Within \$2 – How Much My Bill Was** (How? Our Service was Not Basic, but Upgrade)
- They Said They were **Affiliated with Best Buy** (Stated That's Why Call Id'd on Phone as Such.)
- Told Them (*Several Times*) I Think **It's a Scam.**
- They Insisted That **They Would get Fired – Not a Scam!**
- Got Hubby to Listen to “Deal”. **We Both Were Taken In!**
- After Several Minutes – **I Gave Credit Card Info.**
- Then, Hung Up and **Told Myself, “I’ve Been Scammed”.**
- Called Credit Card Company to **Deactivate the Card IMMEDIATELY.**
- Called **Direct TV** – They Said They Would **Never Call Customer About Deal.**

# PHONE SCAM ALERTS - the GOOD, the BAD, the UGLY

---

## THE UGLY

### TALE OF WOE #1 . . .

- The Caller Told the Victim to Call the Number on Her Credit Card to Verify.

**She Did**

- What She Did Not Know Was That --- They Had Rerouted That Number.

**Now She Was Certain All Was Legit**

- **Lost It All.**

# PHONE SCAM ALERTS - the GOOD, the BAD, the UGLY

---

## THE REALLY UGLY TALE OF WOE #2 . . .

### **A Former White House Scientist Was Scammed**

- **She had a Script from the Man Promising to Save the Retirement Account She Built Over Decades as a Scientist**
- **He Told Her to Transfer More Than \$600,000**
- **If Anyone Asked If She was Put Up To It, She Was to Reply: “No, Absolutely Not”!**
- **The Government She Served for More than Four Decades is Compounding Her Pain:  
The IRS told Her that She Had to Pay Hefty Taxes on the Stolen Money,  
Which the Federal Government Considers Income.**

# OTHER SCAM ALERTS !

---

- **Grandma**, I'm on vacation in Canada and was in **a car accident**.

Please **wire me \$3,000** to pay for medical expenses.

---

- I'm on **vacation in London** and **was mugged**.

I can't pay my hotel bill and they're going to **send me to jail !**

~~Please **wire me \$2,500 NOW!** I'll pay you back when I get home.~~

- **NOW .... A NEW THREAT !**

**SO, WHAT COMES NEXT ???**

**AI**

**(Artificial Intelligence)**



**..... What's Your Response ???**

**On the back of the handout, you will see this:**

## **Scamming Seniors**

Note: The web link below will take you to the website where you can click on any scam listings to see more detailed information about a particular scam.  
Scroll down the page until you see the title “**FRAUD RESOURCE CENTER**”.

**Web link: AARP website:** <https://www.aarp.org/money/scams-fraud.html>

**How can seniors be scammed – here’s some of the ways**  
*(all these website topics are clickable links for more info):*

**When you review this website from your computer, you will then be able to click on the link under the FRAUD RESOURCE CENTER” and scroll to ...**

Scam, Fraud Alerts - Protect You

aarp.org/money/scams-fraud/

MENU **AARP** Join Renew Help Member Benefits AARP Rewards Register | Login

## FRAUD RESOURCE CENTER

Learn how to spot and avoid the common scams listed below

<a href="#">Apartment Rental Scams</a>	<a href="#">Gift Card Scams</a>	<a href="#">Nigerian Scams</a>	<a href="#">Social Security Scams</a>
<a href="#">Business Email Compromise</a>	<a href="#">Government Grant Scams</a>	<a href="#">Obituary Scams</a>	<a href="#">Spear-Phishing</a>
<a href="#">Car Warranty Scams</a>	<a href="#">Grandparent Scam</a>	<a href="#">Online Banking Scams</a>	<a href="#">Student Loan Scams</a>
<a href="#">Caregiver Fraud</a>	<a href="#">Greeting Card Scams</a>	<a href="#">Online Pharmacy Scams</a>	<a href="#">Survey Scams</a>
<a href="#">Celebrity Impostor Scams</a>	<a href="#">Health Fraud</a>	<a href="#">Online Shopping Scams</a>	<a href="#">Sweepstakes and Lottery Scams</a>

**This link will supply more information about Grandparent Scams, but don't overlook the other links that are also helpful !**

# Another Tip: HTTP vs HTTPS

---

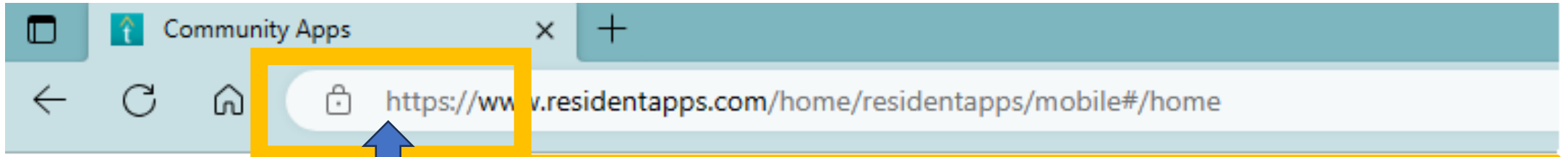
## What is HTTP?

- When you connect to a website that starts with HTTP, your browser looks up the website, and assumes it's connected to the correct web server.
- Data is sent over the connection in clear text.
- An eavesdropper on a Wi-Fi network, your internet service provider, or government intelligence agencies can see the web pages you're visiting and the data you're transferring back and forth.

**I don't usually worry about this UNLESS.....I'm placing an online order or entering personal data**

## What is HTTPS?

- **HTTPS is much more secure than HTTP.**
- **When you connect to an HTTPS-secured server---secure sites like your bank's will automatically redirect you to HTTPS.**
- **Your web browser checks the website's security certificate and verifies it was issued by a legitimate certificate authority.**



Sometimes the letters "HTTPS" will not be shown, but you will see a picture of a CLOSED little lock which signifies "HTTPS".



Alerts



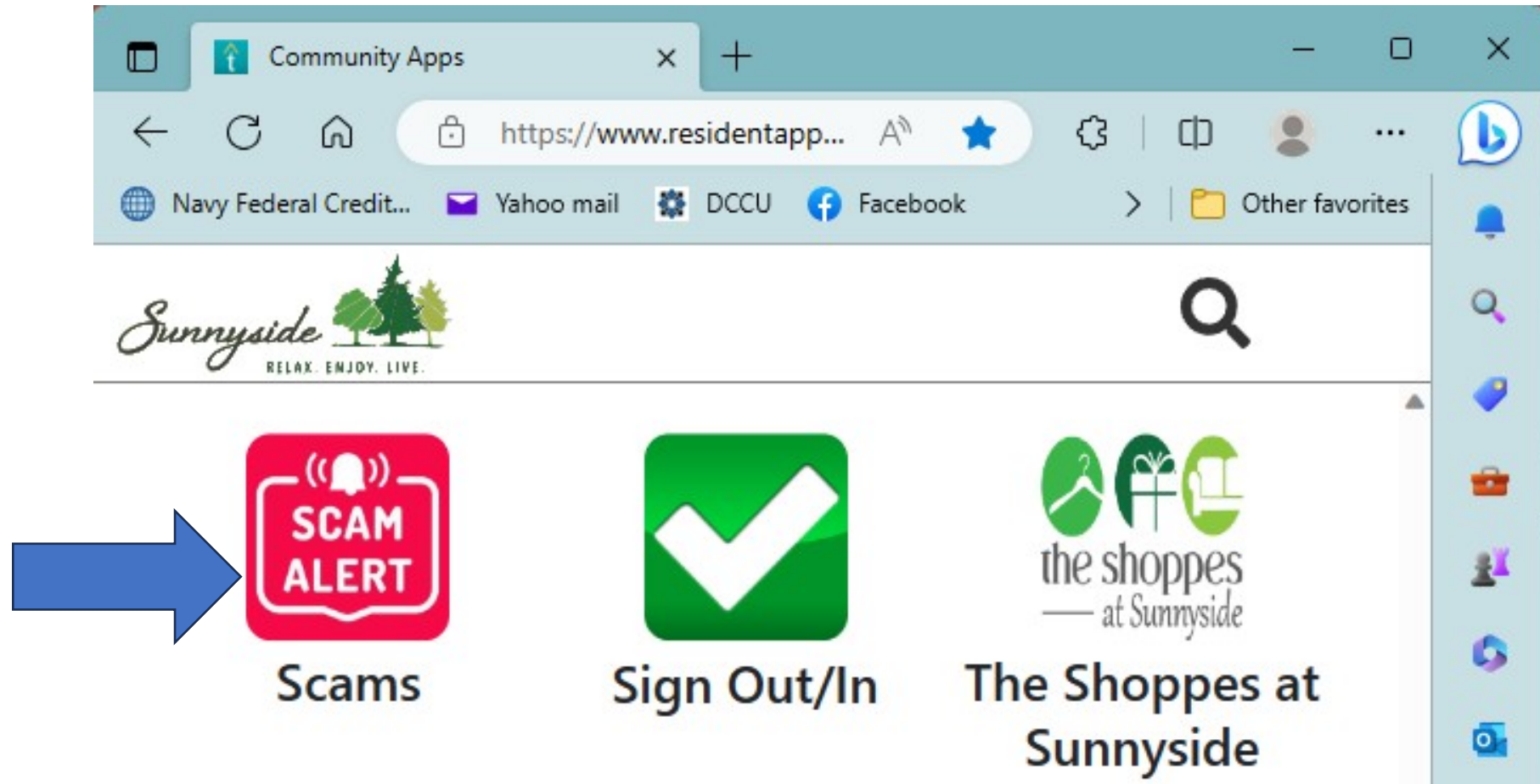
Campus Notices



Channel 970

# SCAM Resources @ Sunnyside

<https://www.residentapps.com/home/residentapps/mobile#/home>



# SCAM Resources @ Sunnyside

<https://www.residentapps.com/home/residentapps/mobile#/module/scams>

Community Apps x Community Apps x Community Apps +

← ↻ 🏠 <https://www.residentapps.com/home/residentapps/mobile#/module/scams> 🔍 ☆ ⚙️ | 📄

🌐 Navy Federal Credit... ✉️ Yahoo mail ⚙️ DCCU 📘 Facebook 🏦 Edward Jones 📄 Sunnyside Times Lite 📱 Community Apps 📍 Google Maps 🟣 Wageworks

← Back Scams

Scams 🔍

[Expand All \(65\)](#)

SCAMS Update Feb 2023

Scam information 2023

▼ **Scam Alerts**

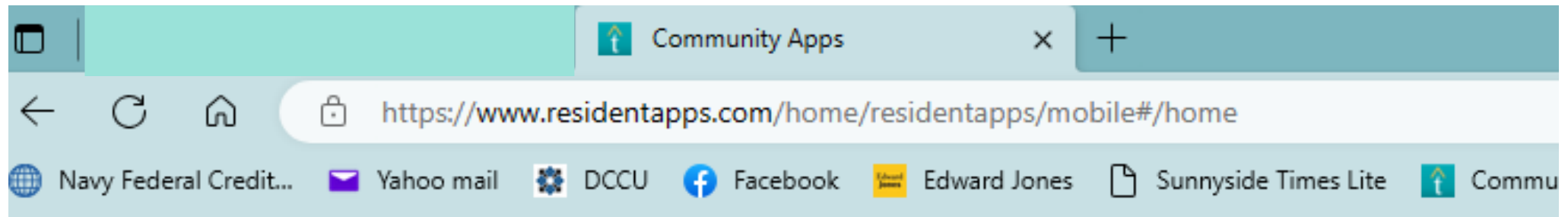
▼ **Stay informed**

Select an item from the list to view its details.

If you are ever concerned about being SCAMMED,  
**DO NOT HESTITATE** to **Contact**  
**Highlands Front Desk**  
**540-568-8200** for further assistance

---

If you need any help with any type of electronic device that you own,  
Go to “Community Apps” and scroll down to Technical Assistance  
to contact the Geek Squad here at Sunnyside.



Technical  
Assistance



## A new warning on the latest scam.....

[Woman sounds alarm on sophisticated wire transfer fraud - Good Morning America](#) 3.47 Mins.

## Other Scam Awareness Videos:

[Recognizing online scams: A tragi-comedy in 4 acts - CBS News](#) 4.24 Mins.

[Online scams: 3 rules to prevent being conned - CBS News](#) 4.11 Mins.