

CAUTION CAUTION CAUTION

If you are on your computer and suddenly see the **“Warning” pic** shown below
(or similar warning) on your screen,
DO NOT call the number listed in the warning.

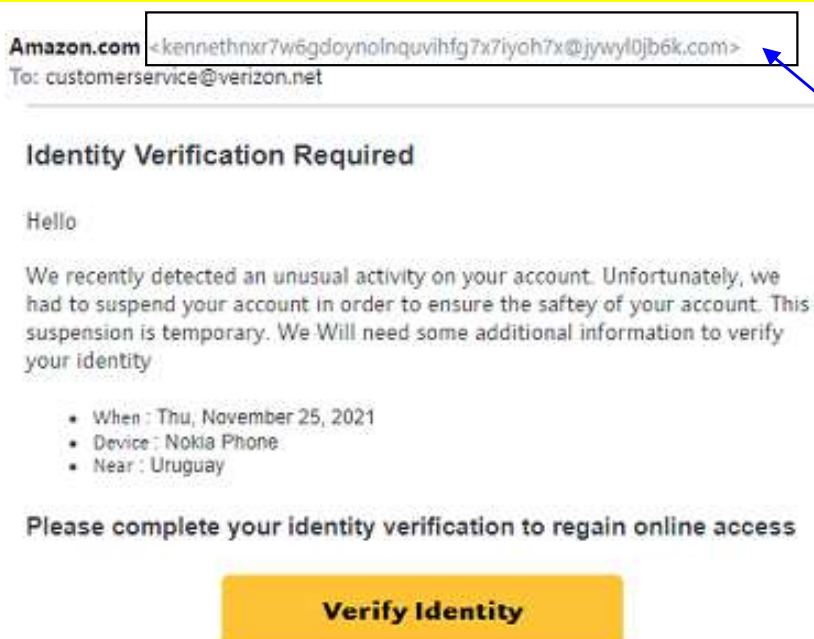
Instead: Immediately contact the Highlands Front Desk
540-568-8200 for further assistance,
or if you feel comfortable doing a forced shutdown.



Nearly half of tech support scams begin with an alert on the victim's computer screen.

Please keep this handout near your computer for future reference.

CAUTION E-mail SCAM.....



See anything wrong with this e-mail?

Check the long address listed after
“Amazon.com”
- this is a **bogus e-mail**.

Almost all e-mails from
companies/financial institutions wanting
you to **“Verify” or “Update”**
your Account info or Identity are
SCAMS!

**Be careful when clicking on a link
from an e-mail.**

**Want to know more about protecting
your e-mail, go here:**

<https://www.youtube.com/watch?v=hF1bIT1ym4g>

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/>

How can seniors be scammed – here’s some of the ways

(all these website topics are clickable links for more info):

Business Email Compromise	Identity Theft	Ransomware
Car Warranty Scams	Impostor Scams	Reverse Mortgage Scams
Caregiver Fraud	Investment Fraud	Robocalls
Celebrity Impostor Scams	IRS Impostor Scam	Secret Shopper Scams
Census Scams	Jury Duty Scams	Small Business Scams
Charity Scams	Lottery Scams	Smishing
Coronavirus Scams	Medical Equipment Scams	Social Media Scams
Credit Repair Scams	Medical Identity Theft	Social Security Scams
Cruise Scams	Medicare Fraud	Sweepstakes Scams
Cryptocurrency Fraud	Money Mule Scams	Tax ID Theft
Debt Collection Scams	Moving Scams	Tax Preparation Scams
Debt Relief Scams	Nigerian Scams	Tech Support Scams
Dietary Supplement Scams	Obituary Scams	Time-Share Resale Scam
Disaster Scams	Online Banking Scams	Travel Scams
DMV Scams	Online Pharmacy Scams	'Update Account' Scams
Email Extortion Scams	Online Shopping Scams	Utility Scams
Fake Check Scams	Package Scams	VA Pension Poaching
Free Trial Scams	Pet Scams	Vacation Scams
Funeral Scams	Phishing	Veterans Scams
Gift Card Scams	Phone Scams	Weight-Loss Scams
Grandparent Scam	Political Scams	Work-From-Home Scams
Health Insurance Scams	Public Wi-Fi Scams	
Holiday Scams		

Other Informative Links about Scamming....

FBI warns about tech support scam – YouTube: <https://www.youtube.com/watch?v=qrUotrIbB7I&t=5s>

Google Online Safety Roadshow – Basic Quick Tips: https://www.youtube.com/watch?v=BX3y_an89PQ

How to avoid 5 Common Scams: <https://www.youtube.com/watch?v=5zInI3Bzsl0>

How to avoid falling victim to an online financial: <https://www.youtube.com/watch?v=QXbF46RvY5k>

5 Common Phone Scams: <https://www.youtube.com/watch?v=5zInI3Bzsl0>

Additionally, the FBI provided a list of tips to avoid being scammed:

- Avoid installing apps or programs that allow strangers remote access to your computer.
- Never call the number in a pop-up window.
- If you see a scam-related pop-up screen, turn your computer off and **DO NOT RESTART**.
- Always be skeptical if someone tells you not to talk to your family about a money transfer.
- Always be skeptical if a "government agency" asks you to conduct business in Bitcoin.
- Always call companies, banks, or government agencies directly with numbers you have independently verified.
- Always contact the FBI at <https://www.ic3.gov> to make a report.