

SCAMS REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING DECEMBER 13, 2021

Submitted by Arnold H. Shifrin

Cell Phone Call Forwarding Scam

You receive a call on your cell phone informing you of the death or serious illness of a distant relative. You're asked to call another number for further details and to preface the number with the code *72. If you follow the caller's instructions, the *72 code automatically forwards all calls from your number to the scammer's phone. The scammer then gives your number to relatives and friends, and they can call him via your phone from anywhere in the world. You are billed for those calls.

You won't realize that you're a victim of this scam until you receive the bill from your phone carrier with the higher than usual charges. You'll likely sense that something is wrong throughout the month because incoming calls on your phone suddenly stopped.

How to avoid being a victim: Never enter *72 or any other code when making a call to a number you don't recognize. To disable call forwarding, dial *73 from the device you wish to disable. [NOTE: you should confirm the respective call forwarding and disabling codes with your telephone carrier as some carriers may have different codes.]

[Source: consumeraffairs.com. This is not a government agency]

United States Retirement Protection Task Force (USRPTF) Scam

An area resident received a call from someone claiming to be from the United States Retirement Protection Task Force in Washington, D.C. about a possible breach of her retirement fund account. The resident was instructed to go to the agency's website, www.usrptf.com, and enter the 8-digit PIN she was given to confirm her identity. She was told she could also call 1-202-808-0934, the agency's Washington, D.C. telephone number.

If you receive such a call or email, immediately hang up or delete the message. Do not click on any links or attachments in the message. This is a "phishing" scam. If you go to the site and enter the PIN as instructed, scammers will try to induce you to reveal your personal information when discussing the "breach," placing you at risk for identity theft.

How you can tell this is a scam.

- There is no legitimate federal agency named The United States Retirement Protection Task Force. To confirm this, you should note the website's URL address. It ends in ".com" instead of ".gov."
- If you do an internet search of 1240 Martin St, Washington, DC 20005, which is the agency's address listed on the website, you'll find that the address exists in Winston Salem, NC, not in the nation's capital.

[Source: Glen Ellyn Senior Center]

Northwestern Medicine Data Breach Scam

The following was posted on NextDoor, a social networking platform, by a Carol Stream, IL resident:

"I just received a call from someone claiming to be with Northwestern Medicine. They left a message with a reference number to call them back. I called back and intentionally gave them the wrong reference number, yet somehow my account came up with a \$300 balance. Don't give these people any information. If you're concerned about your account, call the official number that's listed on your Northwestern Medicine Bill, or on their website."

[Source: nextdoor.com]