

Fraud Watch Overview

Identification and protection

Agenda

- Warning signs of fraud and vulnerabilities
- Protecting yourself from:
 - Medicare Scams and Cyber Crime
- Identify resources to report and resolve consumer problems



Overview

Scams targeting seniors are all over the news!

Here are a few headlines:

- Organized Crime Gangs Earn Big Bucks in Shift to Fraud
- Recidivist Fraudster Convicted of \$10 Million COVID-19 Loan Fraud
- Falling for Fraud Might be Early Sign of Alzheimers
- Consumers Lost **\$56 billion** in Identity Fraud Last Year (2021)



Warning Signs

Why are scammers able to steal from us

- They play on our emotions!

- Fear
- Excitement
- Desire for romance

- Examples:

- “Your Social Security account has been frozen”
- “Your computer has a dangerous virus”
- “You have won a million dollars”
- “I never thought I could love someone like I love you”



Red flags



Guaranteed returns



If it sounds too good to be true...

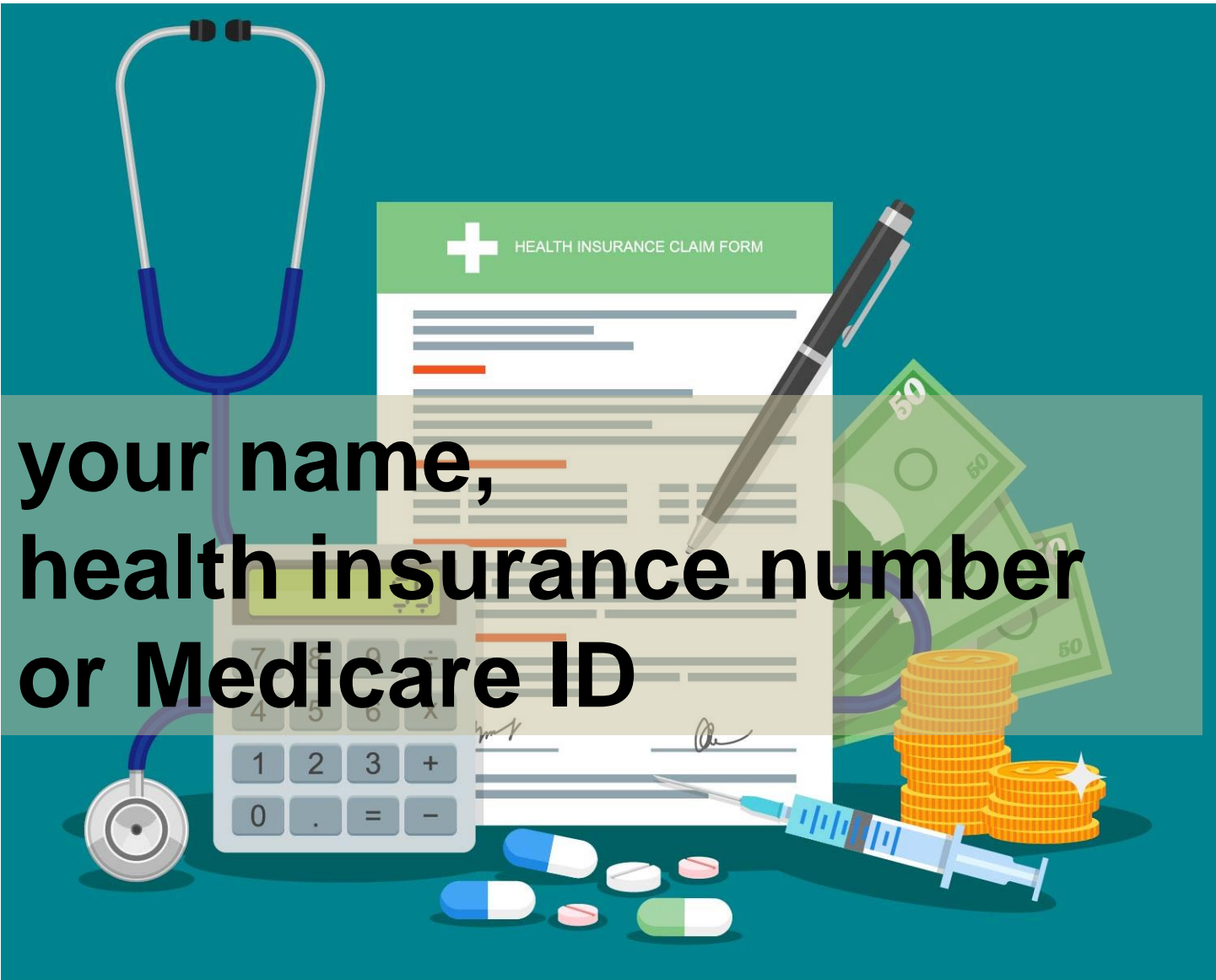


Pressure to send money right away



“Everyone is buying it...”

Medical identity theft

An illustration on a teal background depicting medical identity theft. It features a blue stethoscope on the left, a grey calculator in the center, a 'HEALTH INSURANCE CLAIM FORM' with a white cross icon and a pen resting on it, a syringe on the right, and stacks of gold coins and green 50 Euro banknotes. In the foreground, there are several pills: a blue and white capsule, a white round pill, a pink round pill, and a green and white capsule.

**your name,
health insurance number
or Medicare ID**

MEDICARE SCAMS



WHAT
YOU
NEED
TO
KNOW

Only your health care provider can prescribe Medicare-covered equipment or tests – if a stranger offers you something “free” from Medicare, *it is a scam.*

Cyber Crime

- A computer/smartphone/electronic device is object of or used as tool of a crime
- Most common crime types reported by victims
 - non-payment/non-delivery
 - phishing scams
- Most common crime types in terms of dollar loss
 - e-mail compromise
 - investment scams



Online Risk Factors

Regularly Change Passwords

1. Create strong, easy to remember password/passphrase
 - Has 12 Characters, Minimum
 - Use easy to remember phrases



2. Use a Password Manager
 - Only requires remembering single password
 - Can automatically generate complex password
 - *Example: Last Pass*

Consider adding 2-factor authentication

- Cell Phone authentication code

Avoid Phishing Scams



- Don't click on the **link!**
- Don't open **files** from strangers
- If a message sounds too good to be true, it probably is
- Check **actual** email address
- Strange message from a friend? Be wary

Prevention

- **Be wary of unsolicited offers**
 - Via email or phone call
- **Ask questions!**
 - Be proactive
- **Research before you invest**
 - Sleep on it



Protecting yourself from Fraud



- **DON'T answer your phone**
- **DON'T click on links in email or text**
- **DO freeze your credit report or put on security alert**
- **Do change your passwords regularly**
- **DO review your accounts regularly – Medicare statement, bank, credit cards, retirement accounts**

You can protect yourself!

www.aarp.org/fraudwatchnetwork



TECH SCAMS

Inside the mind of a tech support scammer

Learn how it works

1 of 6



AARP®

Fraud Watch Network

Get Watchdog Alerts

Get Watchdog Alerts

Sign-up for free Watchdog Alerts to stay up on con artists' latest tricks

Resources and Help



Nov 2022



ADDITIONAL INFORMATION

Get access to information about how to protect yourself and your family

Quiz: Catch Me If You Can

Who to Contact (PDF)



Fraud Watch Network

aarp.org/fraudwatchnetwork

**If you or someone you know has been
a victim of fraud, contact:**

877-908-3360