Trust Hijacked:
Cybercriminals Masquerading as Health Insurers and Fraud Investigators

Office of Information Technology
Division of Information Security
AUGUST 2025

Many healthcare scams target older Americans, especially retirees. Due to their weak or no IT skills, older Americans are an easy target group for cyber scammers. It is easy to find lists of names of older adults, who, as an aging group, are significant users of medical services and tend to respond to offers for discounted medical care, pharmaceuticals, and other fraudulent healthcare offers. Cybercriminals who focus on exploiting healthcare weaknesses through health insurance and dare to pose as fraud investigators are well aware of the vulnerabilities of senior citizens.

The Problem

The U.S. population age 65 and over qualifies for Medicare, a program that provides health care coverage to more than 68 million older American adults who need help with rising medical costs. As it is widespread medical coverage, many seniors depend on Medicare for their healthcare needs; hence, the program is a prime tool for fraud.

In Medicare scams, scammers pose as Medicare representatives, trying to convince older adults to share their personal information, such as Medicare or Social Security numbers, to commit identity theft and submit fake Medicare claims in the beneficiary's name to obtain healthcare services, supplies, or prescription drugs.

Trust Abused

So far, one of the more successful healthcare frauds is criminals posing as legitimate health insurers and fraud investigators. They send emails and text messages to patients and healthcare providers, disguising them as legitimate communications from trusted healthcare authorities. The messages try to pressure victims into disclosing protected health information, medical records, personal financial details, or providing reimbursements for alleged service overpayments or non-covered services.

How the Scam Works

These schemes typically start with a phone call, email, text message, or even an in-person visit from someone claiming to represent a well-known insurance provider, government health agency, or an official fraud investigation unit. Criminals often:

- Use official-sounding titles like "Medicare Fraud Investigator" or "Compliance Officer"
- Spoof caller IDs and email domains to make the contact appear legitimate
- Reference real healthcare companies or agencies to gain credibility
- Pressure victims by claiming there's an urgent problem, such as suspected fraudulent charges on their account

The goal is to get the victim to share personal identifying information (PII)—like Social Security numbers, Medicare/insurance numbers, or banking details—or to pay for unnecessary services, fake premiums, or “fraud protection” plans.

How to Protect Yourself from a Healthcare Scam

Be informed and take several preventive measures to avoid this type of healthcare scam. Here are a few tips:

- Be cautious of unsolicited messages, emails, texts, and calls that request personal information
- Never click on links that are included in suspicious and/or unsolicited emails
- Use strong passwords and enable Multi-Factor Authentication for all accounts
- Keep operating system software updated and use antivirus software on all devices
- Always contact your health insurance provider directly to verify the legitimacy of any messages before sharing personal or health care information

Report It

If you believe you have been a victim of a similar fraudulent activity, please report the incident to the FBI’s Internet Crime Complaint Center at www.ic3.gov. Be sure to submit as much information as possible about the individual or company, including name, phone number, mailing or physical address, and email address

Conclusion

We encourage you not to shy away from confronting and reporting scammers if this type of fraud happens to you or your loved one. Cybercriminals count on your silence. In addition to the IC3 Center, be sure to reach out to other relevant authorities, such as the Office of the Comptroller of the Currency, Elder Care, and you can also submit a Hotline Complaint to the HHS Office of Inspector General and the FBI’s Healthcare Fraud.

Stay healthcare safe!

For questions or further information, please contact the IHS Office of Information Technology, Division of Information Security, at cybersecurity@ihs.gov.