# Protect your Medicare number, your other info, and your money

By Bridget Small
June 6, 2022


Last year, the FTC got almost a million reports about impersonation scammers — fake government agents, pretend grandkids, bogus sweethearts, and others who took almost $2.3 billion from people across the country. So far this year, impersonation scams are still the most-reported fraud.

Scammers keep changing their stories to catch you off-guard. Some scams even ask you for your Medicare number. If anyone surprises you with a call, email, text, or message on social media and asks for money or personal information — no matter what story they tell — it's most likely a scam.

During Medicare Fraud Prevention Week this week, learn about protecting your number from health care fraud. Then, take steps to keep impersonators away from your money and valuable information:

**Reduce unwanted calls and email**

- Use call blocking technology or devices that stop unwanted calls — like scams calls and illegal robocalls — before they reach you.
- Use email spam filters to reduce phishing scam attempts, and set your computer software to update automatically.

**Keep information private**

Medicare won't call or text to ask you for money. Even if your Caller ID says it's Medicare, it could be faked. Don't share personal or financial information with anyone who calls, emails, or texts saying they are from a government agency.

- Don't click links or open attachments in email and text messages, even if they seem to come from Medicare or a company you know. They could be messages phishing for your account numbers, passwords, or other information.

**Protect your money**

- Refuse to pay anyone who demands payment by wire transfer, gift card, or cryptocurrency. Only scammers tell you to pay these ways. It's hard to track those payments, and almost impossible to get your money back.

If you suspect a scam, tell the FTC: ReportFraud.ftc.gov.