CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Did You Know?

Criminals may pose as Medicare or health insurers to get your personal information over the internet. It is not always easy to distinguish an important email about your benefits from an online scam. Learn what to look for:

- Even if the email looks legitimate, watch out for email addresses that do not end in .com, .gov or .org or that do not match the address on a company's website.
- Beware of emails with misspellings or grammatical errors.
- Scam emails may say there is a problem with your account or ask for updated information to continue your Medicare coverage. The email asks you to click a link to enter information.

To discuss benefits, coverage or claims payment concerns, contact Customer Service at: 1-800-843-9536

To report suspected Medicare Part C or D fraud, call: 1-877-7SAFERX (1-877-772-3379)

Do Your Part

Once scammers steal your personal or Medicare information, they can harm you financially and may disrupt your Medicare benefits. Follow these online safety tips to avoid becoming a victim:

- Delete or ignore suspicious emails.
- Do not click links or download attachments in suspicious emails. To visit your insurer or Medicare's websites, type your plan's website address or CMS.gov into the browser address bar.
- Do not provide personal or financial information an email asks for. Health insurers and Medicare never ask for your username, password, Social Security Number, Medicare number or banking information by email.
- Update your anti-virus software regularly, and set up filters for junk or spam email.
- When in doubt, call your insurance provider using the number on the back of your card or 1-800-MEDICARE.

For questions about Medicare or for more information, call:
1-800-MEDICARE (1-800-633-4227)
www.cms.gov