December 2019

'Care Share

NEW SCAM TO REPORT

This week we received a yet unsubstantiated claim that someone on Medicare received a call from "Medicare Insurance Company". The caller stated that every Medicare beneficiary is getting a new plastic chip-embedded card mailed to them and they just needed to verify their Medicare number.

Please remember that Medicare will never call and ask for personal information over the phone. If you instigate a call where you know who you are calling, such 1-800-MEDICARE, they will need your Medicare number and birthdate, among other things, in order to help you. However, they will not instigate a call where they ask for personal information.

If you receive a call asking you for personal information, whether it be from Medicare or any source, always err on the side of caution. If something is urgent it probably isn't legitimate. Gather more information and hang up. Never call the number back that was given, but rather look the number up independently either in a phone book or on the internet. If you're really suspicious and want to know if they are legitimate, or if you have given out personal information and it has to do with healthcare, please call your local Montana SMP at 1-800-551-3191.

Putting you in control...

Securing today and tomorrow

Wednesdays to Return to Full Public Service Hours; Agency to Hire 1,100 Direct Service Employees.

Starting on January 8, 2020, Social Security offices nationwide will be open to the public on Wednesday afternoons, Andrew Saul, Commissioner of Social Security, announced. This change restores Wednesday public service hours that were last in place in late 2012. "I don't want someone to come to our office at 2:30 on a Wednesday only to find our doors closed," Commissioner Saul said.

For more information, please visit https://www.ssa.gov/news/press/releases/.

SocialSecurity.gov

Montana SMP is a program coordinated by Missoula Aging Services and partnered with local Area Agencies on Aging. This project was supported by grant #90MPPG0052 from the U.S. Administration for Community Living, Department of Health and Human Services, Washington D.C., 20201. Points of view or opinions do not necessarily represent official ACL policy.

FRAUD TRENDS
Phishing Emails

Phishing emails and text messages may look like they're from a company you know or trust. They are used to "phish" for your information or trick you into giving out your passwords, account numbers, Social Security number, or Medicare number.

You must click the link

An email claims there's a problem or they noticed suspicious activity. You need to click the link to make a payment or confirm personal information.

Look-a-like

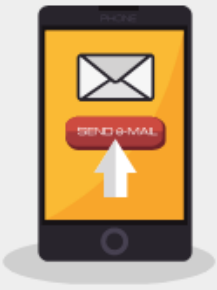
They may look like they're from a bank, social networking site, credit card company, or government entity. They may even use the logo of the company they are trying to look like.

Fake links

If the website asks you to click on a link, hover over the link so that the URL is revealed. If the ".gov" is followed by another period and then additional letters, you can't be certain that it leads to a legitimate website.

Sender's email address

Check the actual email address of the sender. If they are claiming to be from Medicare, their email address should not end in gmail.com.



If you see it, report it!

If you receive a phishing email, forward it to the Federal Trade Commission (FTC) at spam@uce.gov; if you give out personal information, go to IdentityTheft.gov; and if you give out your Medicare number, contact the SMP at info@smpresource.org.

https://www.fool.com/investing/2018/10/27/5-dangerous-social-security-scams.aspx
https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Supported by grant # 90MPRC0001 from ACL