Protect Your Data During Open Benefits Enrollment

During the annual Open Benefits Enrollment Period, scammers exploit the opportunity to extract personal data via calls, emails, and mail. The Federal Trade Commission warns against sharing personal information in response to unexpected contacts, emphasizing that Medicare doesn't engage in unsolicited sales. They caution against clicking links or responding to suspicious messages, advising vigilance, and seeking help from your organization's Human Resources department. It's crucial to avoid sharing personal data and verify communication sources independently to prevent falling victim to fraudulent related schemes. To stay safe, use official sites like MEDICARE.GOV or HEALTHCARE.GOV for plan changes and seek guidance from the NC Department of Insurance's hotline (855-408-1212) for insurance queries.

The CRITICAL**START**® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. For future updates the CTI team will post updates via Cyber Operations Risk & Response™ Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://consumer.ftc.gov/consumer-alerts/2023/10/how-avoid-medicare-open-enrollment-scams#:~:text=They%20might%20look%20or%20seem,if%20you%20get%20those%20messages
2. https://www.cbs17.com/news/investigators/open-enrollment-scams-spiking-as-time-approaches-to-choose-2024-health-care-plan/
3. https://www.kiplinger.com/retirement/medicare/how-to-avoid-medicare-open-enrollment-scams