Medicare Card Scam

Congress enacted legislation in 2015 that requires the Centers for Medicare and Medicaid Services (CMS) to remove Social Security numbers from all Medicare cards. CMS will start implementing this change in April 2018. New beneficiaries will be the first to get the modernized cards, and then new cards will be issued to existing beneficiaries. This change is intended to help prevent fraud and protect people's identity. Scammers, however, are taking advantage of the situation. They're calling Medicare beneficiaries claiming to be from CMS and are telling potential victims that a fee is required in order to receive the new card. Victims are also told they need to confirm their Medicare number in order to receive the new card, thereby risking identity theft if they comply. Be aware that CMS does not charge beneficiaries a fee for the new card. Nor would the agency ever call a beneficiary to verify a Medicare number because that information is already in the CMS database. *(courtesy of AARP Fraud Watch Network)*

Cell Phone Scam

When a lady's purse containing her cell phone, credit cards, wallet, etc. was stolen, she called her husband from a pay phone to tell him what happened. Her husband told her, "I received your text message asking for our ATM PIN, and I sent you a reply a little while ago." When the victim told her husband she did not text him, they immediately rushed down to the bank. When they arrived at the bank, the staff informed them that all the money in their account had been withdrawn.

How the scam works:
The victim had disclosed how to contact her husband by entering his name as "Hubby" in her cell phone contact list. The thief sent a text to "Hubby" to obtain the ATM PIN and was then able to withdraw money from the victims' account.

How to avoid being a victim:
- Do not disclose the relationship between you and the people in your contact list. Avoid using names such as "Home," "Honey," "Hubby," "Sweetheart," "Mom," or "Dad."
- If you receive a text message requesting that you provide personal information (e.g., a PIN), you should first confirm that the request is legitimate by telephoning the person who sent you the text.
- If a friend or relative sends you a text asking you to meet them somewhere, you should first telephone the individual to confirm that the message is legitimate. If you can't confirm the legitimacy of the message, be very cautious about meeting "family members" and "friends" who text you to meet them. Such meetings could result in your being physically harmed or robbed.