Medical Identity Theft

Medical identity theft is a major risk for anyone, but especially for our older relatives who are typically the primary target.

What is it? - Medical identity theft occurs when someone's personal information is stolen and used to claim benefits, get treatment or obtain prescriptions under their victim's name. Although our immediate speculation is to blame a scammer or cybercriminal, the culprit may be closer to home. **Friendly Fraud** is very common and is the term used when medical identity theft is conducted by a friend or family member, with or without consent.

Why is it so bad? - Medical Identity Theft can be far more damaging than traditional Identity Theft. Here are some examples of what can be negatively affected if Medical Identity Theft were to occur.

Your Health
If scammers pose as you or your loved one and obtain medical services, their medical issues become yours. This may affect how doctors provide treatment, may affect your prescriptions, or lead to a misdiagnosis.

Your Wallet
Unlike traditional Identity Theft, there are no protective laws in the United States that limit a consumer's Medical Identity Theft liability, putting you or your loved on on the hook for damages.

Your Financial Reputation
Victims of Medical Identity Theft face long term challenges such as a poor financial reputation, making it more difficult or expensive to take out loans or apply for credit cards.

Watch the Warning Signs & Take Precautions

Watch for unsolicited phone calls where the caller requests information related to your health plan.

Shred any outdated and unnecessary medical records and statements.

Monitor bank accounts, insurance statements and medical records for suspicious activity.

Remember! We all can be victims of Medical Identity Theft, but a primary target is our elders. Share some of your knowledge - *and this newsletter* - to help keep them safe!

THE FAMILY CODEWORD

A family codeword can help add confirmation to abnormal requests from scammers who pretend to be, or be with, your family member and may be requesting money or sensitive information. Here are some tips on creating a family codeword to help keep everyone safe.

It's not about length and complexity here, its about something **only your family** would ever know to say.

Keep it private - **Don't** announce this codeword to anyone outside your immediate family circle.

Try a **random** word or phrase like: Pineapple, Awesome Blossom or Aardvark. Make sure the entire family is aware of the selected word or phrase.

Avoid making it the answer to a question like, "what city or town do we live in?" or "what's our last name?"

Discuss **WHEN** to use the codeword and **WHAT to do** if the codeword is not successfully repeated. This could be calling the other family members directly or the police.

SCAM OF THE MONTH

Each month we highlight a REAL scam that was submitted to our security team. We highlight these real examples of tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

Mary is a recently widowed grandmother living at home alone but receives love and support from her close family. One day, Mary receives a phone call from an unknown number. The voice on the other line sounded a bit strange, but they say they are her grandson Bobby who got in trouble at their college and needed money or else they would be expelled. He pleaded with her to not tell his parents until he was able to get back and explain it to them himself. Mary loved Bobby and wanted to ensure he got a good education, so she agreed to help. Bobby told Mary she needed to go to her nearest convenience store and purchase gift cards then provide him with the numbers on the card. Mary completed this and called Bobby back on the new number he provided and transcribed the card numbers to him. Turns out the caller was not Mary's grandson Bobby, but a scammer.

Did you spot the red flags?

- The caller asked for Mary to purchase gift cards and send them the card information.
- The caller mentioned he did not want Mary to tell his parents.
- The caller gave Mary a new phone number to call when she got the gift cards, rather than calling Bobby directly.

Watch out for **Grandparent Scams**, which is what this event was. Scammers pose as a younger relative to prey on seniors with fake stories that need immediate attention. Talk to your older relatives about the real possibilities of these types of scams and a plan they should follow if they do occur. Consider setting up and using a family codeword.

Tell the entire family to avoid oversharing on social media sites. Many of these details are used by scammers in their attacks to trick our older relatives. With valid information such as where the grandchild goes to school, a trip they may be taking, or other details, the scam can be much more believable. All family members should accept friend requests wisely and keep accounts private.

Never purchase gift cards and provide the card information for an unsolicited call. It will **ALWAYS** be a scam. Other obscure payment methods to avoid include wire transfers or social payment platforms. For in-person variations of these scams, which do occur, avoid providing cash or checks to the individual requesting the payment.