

CYBERSECURITY FOR OUR OLDER GENERATION

A review of the latest security threats and how you can avoid them



THIS MONTH'S TOPICS:

Protecting Our Elders
from Cybercrime - pg. 2

Medical Identity Theft /
The Family Codeword -
pg. 3

Scam of the Month - pg. 4

It's Never Too Late - pg. 5

Our elders have been shaping our path to maturity with their life lessons, words of wisdom and other guidance meant to educate us on right from wrong. It's time for us to return the favor for them!

Our older relatives like parents, grandparents, aunts and uncles may not have the same understanding of technology and the cybersecurity concerns we all face. And unfortunately, due to that lack of awareness, and a potentially larger nest egg, they become a prime target for scammers.

Without the proper resources and education, it can be hard for seniors to understand the security threats around them and how they can protect themselves. But the good news is, you can help! Provide some of the cybersecurity knowledge you've gained to help prepare them for the challenges they may face.

PROTECTING OUR ELDERS FROM CYBERCRIME

Believe it or not, our older generation is **not** the most victimized age group by scammers. That title belongs to the younger generation ages 20-29, according to recent studies. Although reported fraud may have been less for the older generation, the overall monetary loss from scams is typically much higher. Help these individuals like they've helped you by sharing cybersecurity tips and scams to watch out for.



Romance Scams - Many seniors turn to dating sites or apps to find companionship. Although many legitimate connections can be found, there are possibilities of catfishing with the attempts to swindle money or sensitive information from your older loved ones.

Tip! - If your older relative is looking for a connection, help guide them on safe platforms to use and how to avoid falling for a catfish.

Phone Scams - Typically the most common way seniors are targeted is through phone scams. Common tricks include technology support scams, fake trip or lottery scams, or pretending to be a grandchild or loved one in need of money for an emergency.

Tip! - Tell them to watch for threats, impersonations, and offers that seem too good to be true on any call they didn't originate.



Poor Password Controls - Seniors may not have as many accounts as we do, but most have at least one. Without strong password controls, any information within the account is vulnerable to exposure.

Tip! - Teach them about creating strong passwords and not to re-use those password on other accounts.

Consider purchasing them a password manager tool where they only need to remember 1 master password.



Online Shopping - Purchasing goods or services online can be a risk for anyone, especially those with less experience and knowledge about the dangers of online shopping.

Tip! - Inform your elders about risky websites and how to identify sites that are not secure.



Charity Scams - Scammers often pose as reps from charities asking for donations. Watch for unusual payment requests such as wire transfer, cash, cryptocurrency or gift cards.

Tip! - If they do wish to donate, use reputable charities and consider donating on the charity's webpage directly.



Yes, it may be hard to stop these scams and educate our loved ones at a late age, but here are some additional quick tips that can help keep them safe.



Perform a **dark web scan** to verify if their email address has been involved in a data breach.



Share some of these videos and newsletters for topics that they may relate to.



Keep your lessons **simple**; don't overwhelm them with complex technology lingo.



Be their resource; **let them know you can help** provide guidance and that they shouldn't rush into action.

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 one 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, it's 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 Armadillo. 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.



IT'S NEVER TOO LATE TO TRAIN ON CYBERSECURITY

Key Takeaways

Our older relatives can be prime targets for scammers. Help protect them by passing on some of your cybersecurity knowledge to help them avoid scams and protect their investments.



Help your loved ones understand the common scams and educate them on security tips to best prepare themselves.



Watch for Medical Identity Theft which could negatively affect you or your loved ones. Shred unnecessary documents, monitor reports and listen for phone scams.



Beware of grandparent scams by educating your loved ones of the warning signs. Use a family codeword to help everyone properly prepare to handle this threat.

A Cybersecurity Word Search for the Ages

- Charity
- Grandparent
- Romance
- Simple
- Codeword
- Giftcard

- Medical
- Scammer
- Vulnerable
- Protection
- Shred

V L I B Y P Z Z E G W E V J F D
 R P C R I T I Q I Y H R U H H K
 D G G Q O Z I F E Y D J L P Y J
 N N A R G F T R G Y I R N J P F
 Q H O T A C X H A S U S E Z E H
 J E V F A N B F S H X C R Q H I
 O T Y R F O D H M N C A A E P E
 M E D I C A L P O K U M B C H S
 S I M P L E E I A M W M L N O L
 V N D R Z I T T B R X E E A R Y
 I Q I K H C L M M C E R P M M N
 D R O W E D O C S T Y N S O I I
 U B O T Z Q Q S B H P K T R S L
 C B O U E G O I K J R D O P D W
 R R N X H M A W P T F E S N O H
 P D C A U V H Q K Y U M D W T J