**How the Elderly are Being Scammed – Part 1**

We’re all familiar with the world of scammers and hackers. There are so many methods used to try to steal from others that it can be difficult to keep up with warnings for our aging family members. It is important for younger generations to make sure that protective knowledge is gathered and shared with those who are vulnerable to these attacks. In this three-part blog, we will discuss the tricks of the scammers, tips to give the aging persons in your life, and how you can help protect your aging family members. By knowing tips and tricks, they can apply the information to any situation, so they can figure out if it is valid or not.

**Computer Support Trick**

These tricks usually come in one of two ways. The first is through a pop-up message on the computer saying that a virus was found, indicating the user should immediately call the phone number shown to get assistance with fixing the computer. The other method is a phone call claiming to be support from one of the major tech companies, saying they are calling to help with computer problems they can see happening. Neither of these are legitimate requests.

Once someone falls for this ploy, the person on the other end of the phone talks them through the steps to connect to the computer and support them. However, they are not going to support the user, they are instead going to use a trick to lock the computer so that access is completely blocked by the user. Then, they put another person on the phone and explain that the only way to gain access back to the computer is to pay the people on the phone. This is a ransom price. They threaten that if they do not receive payment then all files will be deleted from the computer.

**Ordering & Shipping Emails**

Emails that are made to look like they came from Amazon or other major retailers may show a very large purchase made which scares the recipient into thinking their account was used fraudulently. Or, they may receive an email saying that there was an issue with the payment or the shipping. There may also be emails that look like they come from UPS or FedEx saying that the shipment has an issue. These emails often have attachments included and the attachments are malware or viruses that run on the computer as soon as they are opened.

**The Grandparent Scheme**

One particularly nasty method is someone will call the elderly person claiming to be their grandchild and will say they are in trouble and don’t want mom or dad to know. They may claim to be in jail or stuck in another country. There are a multitude of tricks used to request financial assistance to get out of a jam.

**Medicare Scam**

This one may happen via phone or in person. In person, an elderly person may be attending a community event or other type of event where a company says they can investigate Medicare benefits if provided the member number. There are also phone callers that claim to be with Medicare and they say that they need to review benefits and they ask for the member number. In both cases, they use the member’s number to run a bill against their benefits. This uses up some of their benefit and they make money from Medicare for a service that was not truly offered to the member.

These are a few of the most prevalent scams occurring. In part 2, we will share methods to spot the scammers that can be shared with the aging individuals in your life. By working together, we can make sure that they are protected. There are too many real life cases where people have been scammed out of hundreds of thousands of dollars. Let’s work together to keep more aging persons safe!

**Keeping the Elderly Safe from Scams – Part 2**

In part one we reviewed several of the prominent scams happening to aging persons in today’s world. In this part we will share key tips to provide to those you love to help them deduce if they are being taken advantage of by a scam.

* **You Don’t Know the Person** – If a person is not someone known to them then it is okay to stop and verify who the person is. Any legitimate phone caller is not going to be offended if you say that you want to verify who they are. Even if it seems to be a distraught grandchild who doesn’t want their parents to know, it really isn’t in the best interests of the child to hide this type of thing so checking with the parents is a good idea.
* **Large Companies Do Not Randomly Call You** – Tech companies, shopping companies, and most shipping companies do not call you on the phone. You may receive an automated message from a shipping company about the day and time that your shipment will arrive, but they don’t call asking to help you. Microsoft (Windows) and Apple do not have a way to see that your computer is having an issue, so they won’t call you directly to help you.
* **Guard Your Personal Information** – If someone calls you, do not give out any personal information. Always insist that you will hang up and call the company directly. Do not use the number they give you. Look up the phone number for the doctor’s office, Medicare, or the bank to call them directly and interact. When someone asks you for your birthdate to confirm your identity and you didn’t call them, don’t give it to them. Same with private information such as mother’s maiden name, social security, driver’s license, or Medicare numbers.
* **Legitimate People Don’t Get Offended** – If you ask questions or require proof, a legitimate representative does not get impatient or agitated with you. They understand and usually appreciate that you are not just giving them your private information.
* **Do Not Buy Gift Cards** – People continue to fall for this demand repeatedly. There is nothing that can happen that requires you to go to the store to buy gift cards to pay the person on the phone.
* **Do Not Do Anything on Your Computer When Asked by Someone on the Phone** – Just don’t do it! Don’t go to a screen or type in something they tell you to do. Only allow trusted family members access your computer over the phone and only when you have called them. If they called you, call them back so you know that it is truly the person you believe it to be.

By reminding your loved one of these specific concerns, they can use the information to apply to situations that arise. The scammers are attempting different methods and adjusting their attacks on a regular basis. Being able to apply these known methods will help critical thinking about whether to participate.

**Actions Family Members Can Take to Protect Their Aging Family Members – Part 3**

With aging comes changes in cognition which means that even with the best warnings there may come the time when intervention needs to occur from family members. Here are some options to help protect those who can no longer protect themselves.

* **Block Scam Calls** – This is easier said than done but there are several methods to put in place. Begin by putting their phone numbers in the National Do Not Call Registry. Utilize software options like Nomorobo (<https://www.nomorobo.com/>) to block most calls. There is a system called teleCalm (<https://www.telecalmprotects.com/>) that allows you to block and manage numbers coming through their phone.
* **Protect Their Computers** – There are many ways to protect the computer, including anti-virus and anti-malware software. It is important to make sure that both types of software are installed on the computer. Most scammers who try to connect to a computer start with having the user start their Run Command to start the connection software. This can be disabled to slow the scammer down, here is a video to see how to remove this feature from Windows 10 - <https://www.youtube.com/watch?v=YK5epATpooA>. Most scammers will often hang up if the user says they have an Apple computer; however, protections should be put in place. This article from AARP discusses the Apple options for protection - <https://www.aarp.org/money/scams-fraud/info-07-2011/mac-computer-attack-scam-alert.html>.
* **Secure Their Bank Accounts and Money Access** – Depending on your loved ones cognitive level and your legal access to help manage finances, there are tools available to help protect their money from falling prey to scammers. True Link (<https://www.truelinkfinancial.com/>) offers a refillable credit card that can be provided for their use. With a refillable card you can control the amount available to them and this card even has a feature that will decline online and phone payments.

Looking out for your aging family members to prevent them from falling prey to scammers is a constant battle but one that protects them and keeps them safe. Scams are constantly evolving. If you are concerned about an older adult who may be falling prey to a scam, please reach out to us and we will be happy to review the situation and provide guidance on how to best safeguard them.