Protecting Our Seniors From Scams

A Phone Call with Devastating Consequences

Robert, a 73-year-old retiree, had spent 35 years working at the local manufacturing plant saving up for retirement and his family. All those years of hard work paid off as Robert now had enough in his checking, savings and retirement accounts to help ensure he and his wife can live out the rest of their days in comfort.

On a Monday morning Robert received an alarming call from someone claiming to be from his bank's fraud department. The caller informed Robert that his bank account had been hacked by cyber criminals, putting his savings and retirement at serious risk. Urgently, the caller instructed Robert that to protect his accounts he had to move his funds immediately into "secure" accounts maintained by the bank. The scammer provided new bank details over the phone, assuring him this was the only way to protect his money. Trusting and frightened, Robert complied, transferring all of his life savings to the new accounts.

Only days later, Robert discovered he had been deceived and his entire retirement was gone. The experience left Robert devastated, embarrassed and leaving his future uncertain.

Why Do Scammers Target Seniors?

Sadly, scammers frequently target older adults, believing them to be more trusting or less familiar with technology. In addition, seniors are often wealthy targets as they have accumulated large retirement and investment accounts, excellent credit, or other valuable assets that scammers are eager to exploit. Finally, older individuals may be less likely to report being scammed due to embarrassment, fear of losing independence, or simply not knowing who to contact. The fact that these scammers are absolutely devastating the lives of others means little to them.

Understanding the strategies scammers use is essential for protecting older adults. Phone scams are among the most prevalent, often involving callers pretending to represent government agencies, financial institutions, utility companies, or even family members in distress. Scammers create urgency or fear, pressuring seniors to act immediately without verifying information. For example, criminals may claim a utility bill is overdue and threaten to disconnect services unless immediate payment is made. Another common tactic is the grandparent scam, where criminals pretend to be a grandchild in urgent need of money for bail, medical treatment, or travel assistance.

These phone calls can be even more effective if scammers use Artificial Intelligence for voice cloning attacks.

Email phishing or text messages are another widespread method of targeting seniors. These deceptive messages may appear to come from legitimate sources such as banks, credit card companies, family members, or familiar businesses. They often contain alarming messages urging recipients to click links, download attachments, or provide personal details.

What Can We Do?

Despite being frequently targeted by criminals, seniors are subject to the same types of cyber threats as everyone else. Education about safe online practices, such as recognizing scams, safely managing passwords, and using trusted websites, can dramatically reduce their vulnerability. Encouraging open, regular conversations about these risks is a powerful preventive measure. Families should remind seniors that legitimate organizations will never demand immediate payments via gift cards, wire transfers, or cash deliveries. They should advise seniors never to share personal information such as tax ID numbers, bank account details, or credit card numbers unless they initiated the contact and trust the source entirely. Never grant remote access to, or control over your PC and mobile devices.

Our goal is to make security as simple as possible for them. Setting up call blockers can help seniors avoid unwanted or suspicious calls. Perhaps help them configure their phone so all phone calls, except from family, go straight to their voicemail. Another idea is to bookmark their most commonly used websites in their browser so they know they are accessing the correct sites. If Password Managers are confusing for them perhaps suggest a Password Notebook to write their passwords down in and store it in a secured location. Families can also periodically review financial statements and accounts with their elderly relatives to quickly identify and address suspicious activities. Most importantly, seniors should be reassured that being targeted by scammers is not their fault, nor something to feel ashamed about.

Guest Editor

Dean Parsons is CEO of ICS Defense Force, a SANS Principal Instructor, and a passionate defender of critical infrastructure. With over 20 years in cybersecurity, he conducts industrial incident response and writes 80s-inspired music with his band, Arcade Knights.

Resources

Romance Fueled Investment Scams: https://www.sans.org/newsletters/ouch/sweet-talk-empty-wallet-romance-fueled-investment-scams/
Lock Down Your Financial Accounts: https://www.sans.org/newsletters/ouch/dont-let-cybercriminals-swipe-your-savings-lock-down-your-financial-accounts/
Defend Against Voice Cloning Attacks: https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/