AgeHelper.com
Friendly Technology Help for Seniors
Austin, TX • (737) 667-7007

Safety Guidelines for Seniors

Table of Contents

1. Digital and Phone Security

Devices & Accounts

- **SIM Card PIN:** Be sure to set up a PIN on your SIM card. If your phone is lost or stolen and someone swaps your SIM card into another device, a SIM PIN prevents scammers from accessing your bank accounts or resetting your passwords via text messages.
- **Port-Out Protection / Number Lock:** Contact your mobile carrier and enable protection against unauthorized number transfers (commonly called "Port-Out Protection" or "Number Lock").
- **Screen Lock Passcode:** Set up a passcode or password to unlock your screen if you haven't already.
- **Voicemail PIN:** Secure your voicemail with a custom PIN. Never leave it set to your carrier’s default PIN.

- **Strong, Unique Passwords:** Use long, unique passwords for every website. Use at least 15 characters if a password is your single factor of protection, or at least 12 characters (preferably 14+) when combined with multi-factor authentication. Never use your name, birthdate, phone number, or simple words. Avoid keeping passwords in plain sight or reusing the same password across multiple sites. Using a password manager is highly recommended.
- **Multi-Factor Authentication (MFA / 2FA):** Turn on two-factor or multi-factor authentication to log into your accounts. Passkeys, authenticator apps, or hardware security keys are preferred. SMS text codes are acceptable—they are much better than having no MFA at all, though they are less secure against certain types of attacks.
- **Apple ID & Google Account Passwords:** Never share your primary account passwords with anyone under any circumstances. Giving someone access to your main Apple ID or Google Account grants them full control over all your connected devices and personal data.
- **Automatic Updates:** Enable automatic software updates for your phone, computer, and applications. An outdated system is an easy target for hackers because it contains unpatched security bugs. Always ensure updates come strictly from official sources.
- **Emergency Contacts / Medical ID:** Set up your device so that an emergency contact (a family member or friend) can be viewed even from a locked screen (if supported by your phone). Also configure emergency contacts for easy access right from your phone's screen.
- **Location Sharing & Trackers:** Turn on location sharing in Google Maps or Apple's *Find My* app with trusted relatives or friends. You can also place an Apple AirTag or Samsung SmartTag in a purse or bag so you or your loved ones can locate it during an emergency. *Note:* An AirTag or SmartTag is not a substitute for a cell phone or a dedicated GPS tracker. In an emergency, a cell phone with active location sharing is significantly more reliable.

Phone Calls & Phone Communication

- **Don't Trust Caller ID (Caller ID Spoofing):** Phone numbers and caller names displayed on your screen can be easily faked. Never trust what appears on your Caller ID. Hang up and call back using a trusted phone number you already know, rather than redialing the incoming caller.
- **Never Share SMS Verification Codes:** One-time passcodes sent via text message are keys to your money. If someone claiming to be from your "bank" calls asking for a code, hang up immediately. Call your bank back directly using the official customer service number printed on the back of your debit or credit card.
- **Hang Up Immediately on Requests for Personal Data:** Never share your Social Security Number (SSN), card details, CVV (3-digit security code), PIN, or passwords during an unsolicited call. If a legitimate organization actually needs to verify your identity, look up their official phone number independently and call them back yourself.
- **Enable Spam Filtering and Block Unknown Callers:** Turn on built-in spam call filtering or features like "Silence Unknown Callers".

Protection Against Remote Access Software

- **Strict Ban on Remote Access Apps (AnyDesk, TeamViewer, RustDesk):** If anyone calls asking you to install an application "for security," "to cancel a transaction," or "for technical support"—**hang up immediately**. These programs grant scammers full control of your phone or computer screen, allowing them to transfer your money directly.
- **CRITICAL WARNING:** Real representatives from **Microsoft, Apple, your bank, or law enforcement / police will NEVER call you** asking to install remote access software (such as AnyDesk, TeamViewer, or RustDesk).

Phishing, Suspicious Links, and Fake Invoices

- **Do Not Click ANY Links in Texts or Messaging Apps:** Avoid clicking on links received via SMS/text or messaging apps—even if sent by someone you know, as their account may have been hacked. Call the sender directly on a known phone number to confirm whether they actually sent it.

- **Fake Email Receipts & Renewal Invoices:** Scammers frequently send emails pretending to be from Norton, McAfee, Amazon, or other companies, claiming you have been charged $400+ for an automatic subscription renewal. **Do not call the phone number listed inside the email!** This is a scare tactic designed to create panic. Always verify your actual account balance directly through your official banking app, or by calling the official phone number on the back of your bank card or official website.

2. Financial Protection and Specific Scams

- **SSN Protection & Credit Freeze:** Protect your Social Security Number (SSN) and never share it unless strictly necessary. If you suspect a data breach or identity theft, place a security freeze on your credit reports with all three major credit bureaus (Equifax, Experian, and TransUnion).
- **Set Up a Free Credit Freeze / Security Freeze:** Proactively freeze your credit reports with Equifax, Experian, and TransUnion. By law, placing and lifting a credit freeze is 100% free! Keep in mind that a credit freeze prevents scammers from opening *new* credit accounts in your name, but it does not protect your *existing* bank or credit card accounts—you still need to monitor transactions on those regularly.
- **Monitor Transactions Regularly:** Check your banking and credit card activity frequently using your official bank mobile apps or online banking statements.
- **Red-Flag Payment Methods:** Never pay an unexpected caller using gift cards, cryptocurrency, wire transfers, or peer-to-peer payment apps (such as Zelle, Venmo, or Cash App) based on their instructions. Demand for these specific payment methods is an immediate red flag that requires stopping and verifying.
- **Romance Scams:** If someone you recently met online asks for money, bank transfers, or gift cards, cut off all communication immediately.
- **The "Red Flag" Urgency Rule:** Phrases like *"URGENT," "RIGHT NOW,"* or *"BEFORE IT'S TOO LATE"* are your primary warning sign to stop immediately. Scammers deliberately create artificial panic.

- **Dedicated Credit Card for Online Purchases:** Use a separate credit card with a low credit limit for online shopping. Never use a debit card or an account holding your primary life savings for online purchases. If you notice a suspicious transaction, contact your card issuer immediately to dispute the charge.
- **Bank Limits & Transaction Alerts:** Ask your bank to set daily withdrawal and transfer limits on your accounts. Turn on instant transaction notifications via your bank’s app or text messages (SMS) to your phone.
- **Never Send Money for "Account Verification":** Never transfer money or buy gift cards to "verify your account" or "test system security." Legitimate financial institutions will never ask you to do this.
- **Avoid Calling Phone Numbers in Google Search Ads:** Never call a bank's customer service number displayed inside the "Sponsored" (advertisement) block at the top of Google search results—scammers buy these ads. Scroll down past the ad section to find the bank's official website. Always double-check the web address (URL) to ensure the bank’s name is spelled correctly with no extra, unusual, or altered characters.

3. Staying Safe with Loved Ones: AI Threats and Safe Words

- **Scheduled Check-In Calls:** Agree on set, regular times for phone calls with family members or friends. Establishing a routine helps your loved ones quickly notice if you haven't checked in due to a sudden illness, a fall, a home emergency, or another serious issue.
- **AI Voice Cloning & Family Emergency Scams ("Grandchild in Trouble"):** Scammers now use Artificial Intelligence (AI) to clone the voices of adult children and grandchildren with frightening accuracy, and can even generate realistic photos and videos. If someone claiming to be your "son," "daughter," or "grandchild" calls from an unfamiliar number crying and desperately begging for money—**do not trust the photo, video, voice, or Caller ID!** End the call immediately without explanation, and call your relative back directly at the trusted phone number you have saved for them.

- **Family Code Word / Safe Word:** Establish a secret family code word or phrase with your loved ones. If a caller claiming to be a "relative" cannot provide the code word, hang up immediately and call them back on their regular phone number. Keep in mind that a safe word should not be your only line of defense—always independently call your relative at their known number whenever money is requested.
- **The "Pause and Verify" Rule:** Take a long pause and hit the "brakes." Always discuss any "urgent" message, request for money, or financial emergency with a trusted friend or family member before taking any action or transferring funds.

4. Physical Home Security and Injury Prevention

Home Access and Doors

- **Locks and Door Reinforcement:** Use modern high-security deadbolts and cylinders equipped with key-duplication protection (restricted keyways) and protective collar plates/reinforcement hardware. Many standard grade-3 locks can be picked or bumped in seconds. High-security cylinders feature complex key profiles, side pins, pick/bump resistance, and drill-resistant construction. However, a lock cylinder alone is not enough: ensure your entire door assembly, door frame, lock mounting, and heavy-duty strike plate (secured with 3-inch screws into the wall stud) are thoroughly reinforced.
- **Track Key Access:** Maintain strict control over who has made copies of your house keys or has access to spare keys to your home.
- **High-Security Lock Features:** Quality modern deadbolts and cylinders should provide certified protection against lock picking, lock bumping, drilling, and physical manipulation. Look for locks engineered with hardened steel inserts, reinforced solid-metal housings, and drill-resistant pins.
- **Video Surveillance & Doorbells:** Install security cameras and a video doorbell (such as Ring, Nest, or Arlo). Never open the door to strangers—check who is outside using your smartphone camera feed, a peephole, or

a door security chain/latch. Ensure video footage is not just recorded onto a local memory card, but also automatically backed up to secure cloud storage.

- **Unexpected Utility Workers & Inspectors:** Never let an unannounced utility worker, meter reader, or contractor into your home based solely on what they say. Keep the door closed and locked, and call the utility company yourself using the official phone number printed on your monthly bill or official website.
- **Door-to-Door Visitors and Salespeople:** Never discuss your personal finances, living situation, daily routine, or savings with strangers, no matter how kind or helpful they appear. Do not trust a visitor simply because they wear a uniform, look professional, or know your name. Independently verify their identity through the company or organization they claim to represent before letting them near your home.

Fall Prevention and Home Safety ("Hazard-Free Home")

- **Remove or Secure Loose Rugs:** Remove unanchored area rugs and throw rugs, or secure them with non-slip backing or double-sided rug tape—loose rugs are a primary trip and fall hazard.
- **Keep Walkways Clear:** Clear electrical cords, charging cables, clutter, and obstacles from hallways, doorways, and main walkways throughout your home.
- **Nighttime Motion Lighting:** Install motion-sensor nightlights in hallways, stairwells, and along the path from your bedroom to the bathroom to ensure safe movement in the dark.
- **Keep a Physical Paper Contact List:** Maintain a printed paper list of essential phone numbers—including family members, your bank, insurance providers, and key organizations—and store it in a safe place at home. Do not rely solely on your mobile phone in an emergency.
- **Secure Sensitive Documents & Shred Personal Info:** Store your Social Security card, Medicare card, passport, banking papers, and other sensitive documents in a safe, locked location. Always shred mail and documents containing personal information or account details before

putting them in the trash or recycling.

Emergency Information Sheet on the Refrigerator (For First Responders)

- **Emergency Info Display:** Print a single sheet in large, bold, easy-to-read text and attach it to your refrigerator with a magnet (where paramedics and First Responders are trained to look first):
    - Phone numbers for close family members and emergency contacts.
    - Phone number for your Primary Care Physician (PCP).
    - A list of key chronic medical conditions and known allergies.
    - A complete list of current medications and exact dosages.
    - Additional phone numbers for medical specialists or preferred local hospitals.
- **Maintain Medical Privacy:** Avoid posting sensitive medical diagnoses, full health histories, or unnecessary personal details out in plain sight unless critical for emergency care.

5. Social Media and Online Privacy

- **Friend Requests from Strangers:** Do not accept friend requests or connections from people you do not know personally on Facebook or other social media platforms.
- **Facebook: Check Who Can See Your Posts:** Before publishing a post, manually verify your audience settings to ensure **Friends** is selected instead of **Public**. Always double-check your privacy settings for Facebook **Stories** as well, so your personal photos, location, and daily updates are not visible to the general public.
- **Avoid Accidental Public Sharing:** It is very common to accidentally share a sensitive photograph or private message publicly on your main feed instead of sending it privately through a direct message (such as Facebook Messenger).
- **Fake Accounts and Impersonation (Cloned Profiles):** Scammers frequently create duplicate accounts using a real friend's or relative's

profile picture and recent posts. If a "friend" or "family member" sends you a message asking for money or urgent help—especially if their tone or wording seems unusual—verify their identity with a direct phone call or video call.

Refrigerator Cheat-Sheet (12 Core Safety Rules)

1. **Passwords:** Use long, unique passwords + a Password Manager + Multi-Factor Authentication (MFA / 2FA).
2. **Phone Security:** Set a SIM PIN, block unknown callers, and enable official automatic software updates.
3. **Suspicious Calls:** If a call feels strange or urgent, hang up immediately and call back independently using a trusted number!
4. **Links & Attachments:** Never click links in unexpected text messages, and never open suspicious email attachments.
5. **SMS Passcodes:** Never share verification codes sent to your phone with anyone—ever!
6. **Bank Calls:** Legitimate banks will never call asking you to transfer money or reveal security codes.
7. **Remote Access:** Never install remote control software (such as AnyDesk or TeamViewer) at a caller's request.
8. **Personal Info:** Keep your Social Security Number (SSN), card CVV, and Apple/Google passwords strictly private.
9. **Family Safe Word:** Always ask for your secret family code word if a "relative" calls asking for money or emergency assistance.
10. **Gift Cards:** Police, government agencies, and banks NEVER demand payment or fees via gift cards.
11. **Door Safety:** Always check your security camera feed or peephole. Real utility workers do not drop by unannounced.
12. **When in Doubt:** Take a pause, hang up the phone, and call a trusted family member or friend to double-check.