Your Financial Safety Checkup

Three steps to protect your finances and identity from fraud

A companion handout from the Senior Planet Lunch & Learn with Christina Riechers

Step 1: Freeze Your Credit

A credit freeze is the single most effective thing you can do to prevent identity theft. It locks your credit file at each bureau so that **no one — including you — can open new credit accounts** (credit cards, loans, store cards) until you temporarily lift the freeze. This is free, it doesn't affect your credit score, and your existing accounts keep working normally. You need to freeze at all three bureaus, because a lender might check any one of them.

- [ ] **Freeze credit at Equifax**

  equifax.com/personal/credit-report-services/credit-freeze/

  Create an account, then look for "Place a Security Freeze" or "Add a Freeze."

  Username / Password:

  _____

- [ ] **Freeze credit at Experian**

  experian.com/freeze/center.html

  Click "Add a Security Freeze" and follow the steps to create an account and verify your identity.

  Username / Password:

  _____

- [ ] **Freeze credit at TransUnion**

  transunion.com/credit-freeze

  Click "Add a Freeze." If the online questions are hard, you can call 1-888-909-8872 to freeze by phone.

  Username / Password:

> **Remember:** Write down your username and password for each bureau and keep them somewhere safe. You'll need them later if you want to temporarily lift a freeze — for example, if you're applying for a new credit card or loan.

Step 2: Add a Trusted Contact

A trusted contact is like an **emergency contact for your financial accounts**. If your bank or brokerage notices something concerning — like a large unexpected withdrawal or signs that someone may be taking advantage of you — they can reach out to this person to help protect you. **Your trusted contact cannot access your money, see your accounts, or make any transactions.** They can only be contacted by your institution, and only if something seems wrong. Good choices: an adult child, a sibling, a close friend, or your attorney.

- [ ] **Add a trusted contact to at least one financial account**

  Call your bank or brokerage and say: "I'd like to add a trusted contact to my account." You can also look in your account settings online — search for "Trusted Contact" or "Beneficiary & Contact." Start with your largest or most important account.

  Account / institution:

  Trusted contact name & phone:

Step 3: Device Security Check

Your phone and computer are how you access your bank accounts, email, and personal information. Keeping them up to date and blocking scam calls are two simple ways to **close the door on the most common digital threats**. Software updates fix security holes that hackers exploit, and spam filtering blocks the scam calls and texts that are the #1 way fraudsters target older adults.

- [ ] **Turn on automatic software updates**

  iPhone/iPad: Settings → General → Software Update → Automatic Updates → turn everything On

  Mac: System Settings → General → Software Update → click (i) next to Automatic Updates → turn On

  Windows: Settings → Windows Update → make sure automatic updates are on

- [ ] **Turn on spam call and text filtering**

  iPhone: Settings → Phone → Silence Unknown Callers → On. Also: Settings → Messages → Filter Unknown Senders → On

  Android: Phone app → menu (three dots) → Settings → Caller ID & spam → turn on Filter spam calls

  Your carrier: Call AT&T, Verizon, or T-Mobile and ask them to turn on free spam filtering for your line

> **Tip:** If you turn on "Silence Unknown Callers," calls from people not in your contacts go straight to voicemail. Real callers will leave a message — scammers usually won't.