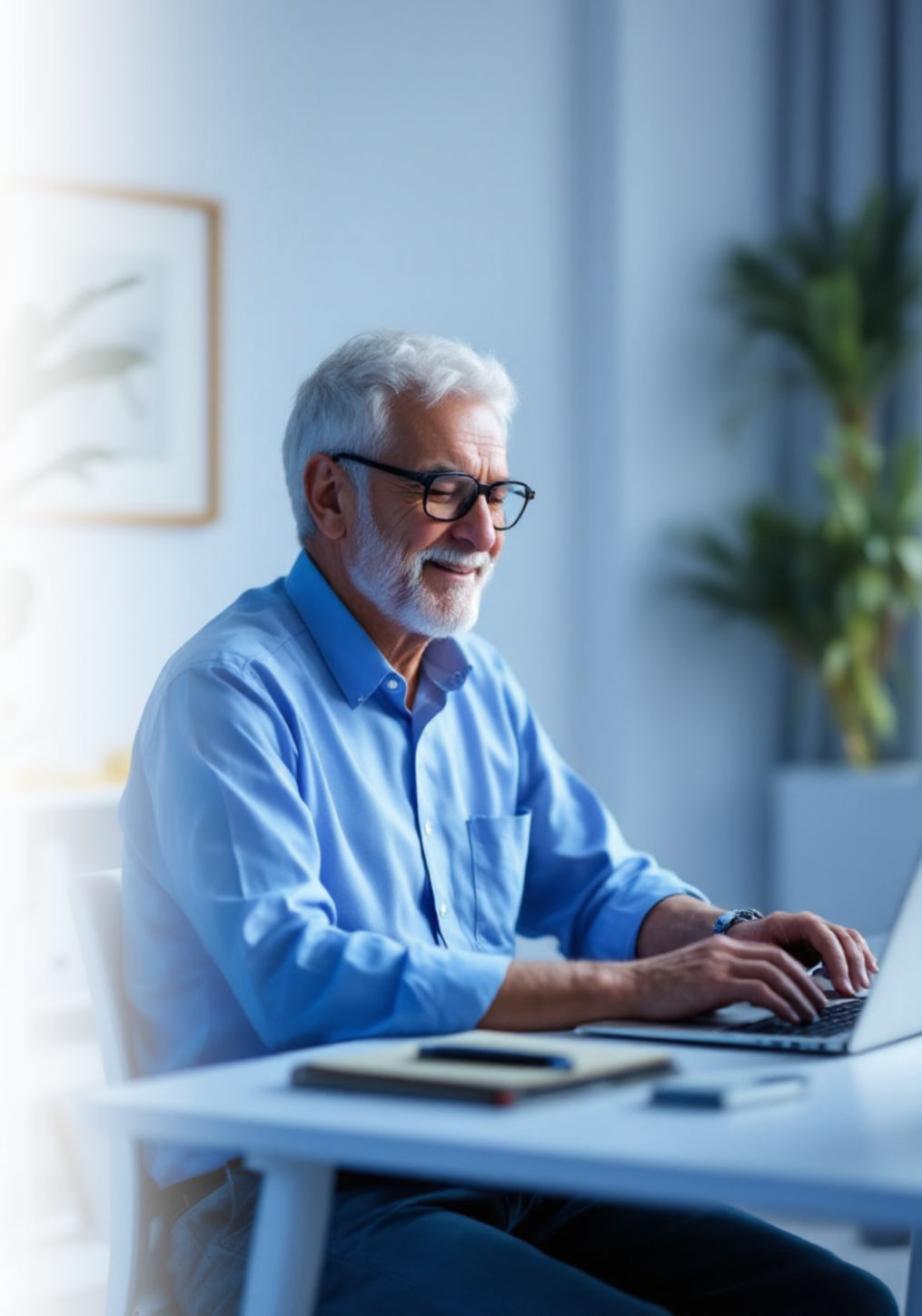
CSNP
CYBERSECURITY NON-PROFIT

Identity Theft Prevention Guide

A practical guide to protecting your personal information and staying safe online. Created specifically for seniors and their families.

SENIOR DIGITAL SAFETY



Understanding Identity Theft

What Is Identity Theft?

Identity theft occurs when someone steals your personal information—like your Social Security number, bank account details, or credit card numbers—and uses it without your permission. Thieves can open new accounts, make purchases, or even file tax returns in your name.

This crime affects millions of Americans each year, but you can protect yourself with the right knowledge and tools.

How Thieves Get Your Information

Phone Scams

Callers pretending to be from the IRS, Social Security, or your bank asking for personal details.

Phishing Emails

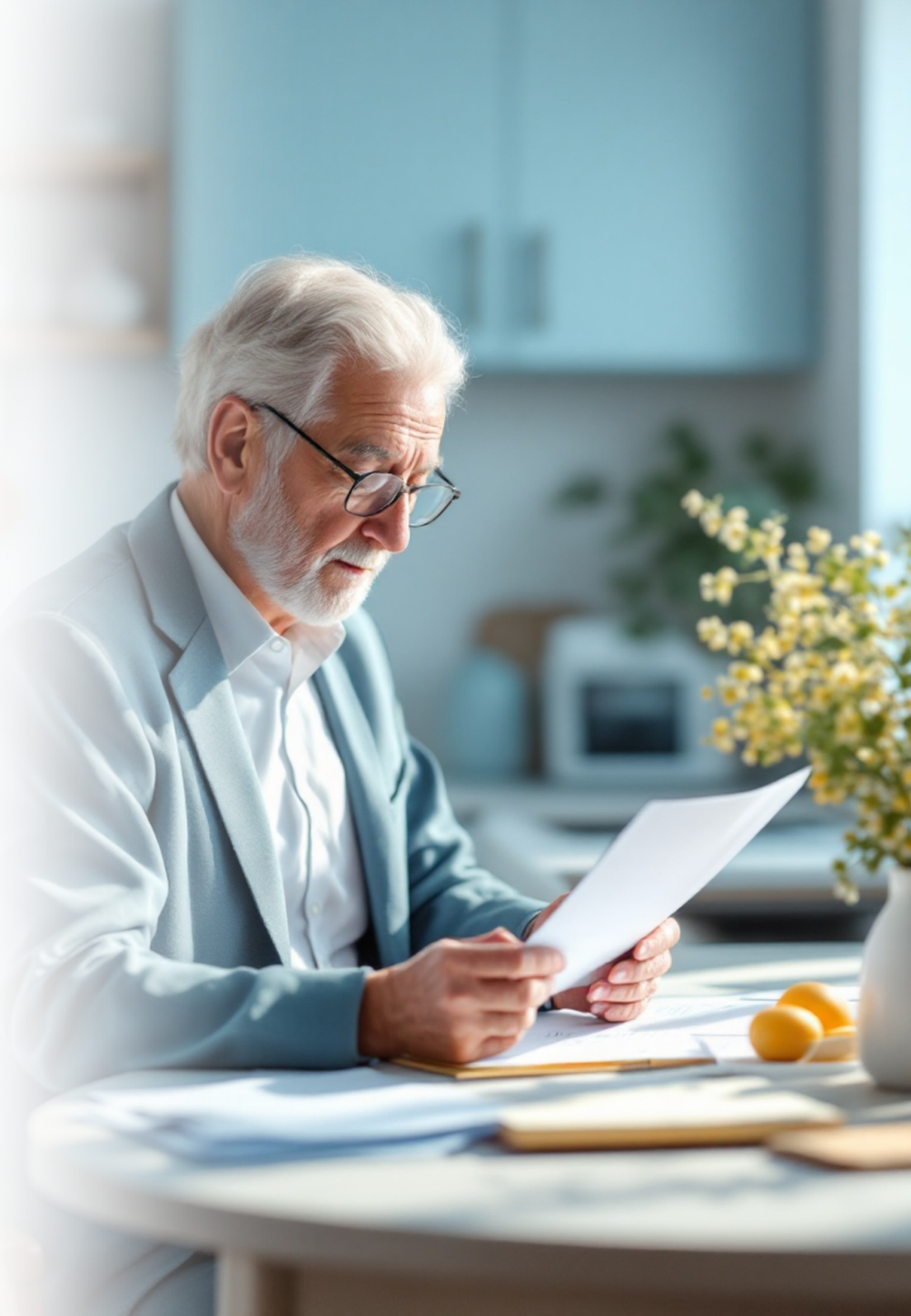
Fake emails that look official, asking you to click links or provide sensitive information.

Mail Theft

Stealing mail from your mailbox to get bank statements, credit card offers, or tax documents.

Dumpster Diving

Going through your trash to find documents with personal information.



Warning Signs to Watch For

Unexplained charges on your bank or credit card statements

Even small amounts can indicate someone is testing your account.

Bills or statements stop arriving in the mail

Thieves may have changed your mailing address to hide their activity.

Calls from debt collectors about accounts you didn't open

This is a clear sign someone has opened accounts in your name.

Your credit report shows accounts or inquiries you don't recognize

Regular monitoring helps catch this early.

You're denied credit unexpectedly

Identity theft can damage your credit score without your knowledge.

Protecting Your Personal Information

1

Never share personal information over the phone

Unless you initiated the call to a known, trusted number. Government agencies and banks will never call asking for passwords or Social Security numbers.

2

Create strong, unique passwords

Use a combination of letters, numbers, and symbols. Consider using a password manager to keep track of them safely.

3

Be cautious with email links

Don't click links in unexpected emails. Instead, go directly to the company's website by typing the address yourself.

4

Secure your mail

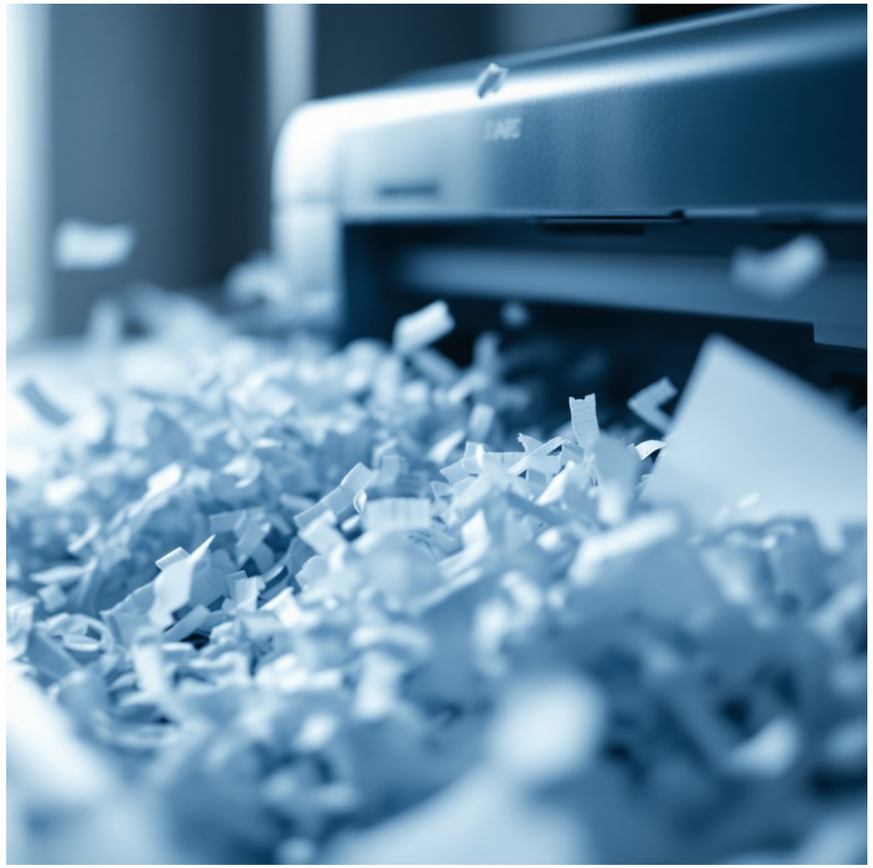
Collect mail promptly and use a locked mailbox. Consider a P.O. box for important documents.

5

Review statements regularly

Check your bank and credit card statements at least monthly for any suspicious activity.

Secure Document Disposal



Shred Before You Toss

Never throw away documents containing personal information without shredding them first. This includes:

- Credit card offers and applications
- Bank and investment statements
- Medical records and insurance forms
- Tax documents and pay stubs
- Expired credit or debit cards
- Any document with your Social Security number

Tip: Invest in a crosscut shredder for better security. They're affordable and easy to use at home.

Credit Monitoring & Freezes

01

Check your credit reports annually

Get free reports from all three bureaus at AnnualCreditReport.com. Review them carefully for errors or unfamiliar accounts.

02

Consider a credit freeze

A freeze prevents new accounts from being opened in your name. It's free and you can lift it temporarily when needed.

03

Set up fraud alerts

These require creditors to verify your identity before opening new accounts. Alerts last one year and are free to renew.

04

Monitor your accounts online

Many banks offer free alerts for transactions over a certain amount or unusual activity.

The three credit bureaus: Equifax (equifax.com), Experian (experian.com), and TransUnion (transunion.com). Contact all three to place a freeze.

If You're a Victim: Take Action Immediately

1

Contact your bank and credit card companies

Report fraudulent charges and request new cards with new account numbers.

2

Place a fraud alert on your credit reports

Contact one of the three credit bureaus—they're required to notify the other two.

3

File a report with the FTC

Visit IdentityTheft.gov to create a recovery plan and get step-by-step guidance.

4

File a police report

Bring your FTC report and any evidence of theft. You may need this for creditors.

5

Document everything

Keep records of all conversations, reports, and correspondence related to the theft.

Important Resources & Contacts

Federal Trade Commission (FTC)

Website: IdentityTheft.gov

Phone: 1-877-438-4338

Report identity theft and get a personalized recovery plan

Social Security Administration

Website: ssa.gov/fraud

Phone: 1-800-772-1213

Report Social Security number misuse

IRS Identity Theft Hotline

Phone: 1-800-908-4490

Report tax-related identity theft

AnnualCreditReport.com

Get free annual credit reports from all three bureaus—the only authorized source

Cybersecurity Non-Profit (CSNP)

Making cybersecurity knowledge accessible to everyone

We provide free education, community support, and practical resources to help you stay safe online.

Our Programs

- Business & Non-Profit Security
- Family Cybersecurity
- Kids Safety Online
- Senior Digital Safety
- Women's Security
- Parents & Educators Resources

Everything we offer is completely free.

Visit csnp.org

Browse Resources