THRIVING SENIOR

Helping seniors live better, one tip at a time

Digital Safety Checklist

The security steps that actually protect your accounts

☐ Create a unique password for every account

Download a free password manager such as Bitwarden, or use the built-in password manager on your iPhone or Android phone. Let it generate a new, random password for each site you use. Store them all in the manager so you never have to remember them individually. Update any account where you currently reuse a password you use elsewhere.

☐ Enable two-factor authentication on your email

Log into your email account — Gmail, Yahoo, Outlook, or whichever you use — and navigate to Security settings. Find 'Two-Step Verification' or 'Two-Factor Authentication' and turn it on. Choose text message as your verification method. From this point forward, logging in will require both your password and a code sent to your phone.

☐ Enable two-factor authentication on your bank accounts

Log into each bank, credit union, and investment account you hold. Go to Security or Account Settings and look for a two-factor or two-step verification option. If you cannot find it, call the number on the back of your debit or credit card and ask a representative to help you enable it and set up login alerts.

☐ Create and secure your ssa.gov account

Go directly to ssa.gov and click 'Sign In' or 'Create an Account.' You will need your Social Security number, a valid email address, and some personal information to verify your identity. Once inside, enable two-factor authentication immediately. This prevents criminals from creating an account in your name and redirecting your benefit payments.

☐ Freeze your credit at all three bureaus

Visit each bureau's website individually: equifax.com, experian.com, and transunion.com. Create an account at each and select 'Credit Freeze' or 'Security Freeze.' This is free and prevents any new credit from being opened in your name without your explicit approval. Keep your PIN or account credentials for each bureau in a safe place so you can lift the freeze when needed.

☐ Review your free annual credit reports

Go to annualcreditreport.com — the only federally authorized source for free credit reports — and request all three reports. Look for accounts you do not recognize, inquiries you did not initiate, or addresses you have never lived at. Dispute any errors directly with the bureau that is reporting them. Set a reminder to do this again in twelve months.

☐ Review and tighten your Facebook privacy settings

Log into Facebook and go to Settings, then Privacy. Change 'Who can see your future posts' to Friends only. Change 'Who can send you friend requests' to Friends of Friends. Under Profile and Tagging, restrict who can see your friends list and who can look you up. Scammers mine public Facebook profiles to personalize phishing attacks and answer security questions on your accounts.

☐ Learn to identify phishing emails before clicking

Before clicking any link in an email, look at the sender's full email address — not just the display name. A real email from your bank will come from a domain like yourbank.com, not yourbank-support.net or a string of random characters. Hover over any link to see where it actually leads. If an email creates urgency or asks for your password, Social Security number, or payment information, do not click anything — go directly to the organization's website by typing the address yourself.

☐ Register your number on the Do Not Call registry

Go to donotcall.gov or call 877-382-4357 to register your home and mobile phone numbers with the FTC's National Do Not Call Registry. Registration is free and permanent. While it will not stop illegal scam calls, it does reduce legitimate telemarketing and makes it easier to identify calls that come through anyway as likely scams. Report unwanted calls at the same website.

☐ Turn on 'Silence Unknown Callers' on your smartphone

On an iPhone, go to Settings, then Phone, and enable 'Silence Unknown Callers.' On most Android phones, open the Phone app, go to Settings, and find 'Block Numbers' or 'Spam Protection' to enable call screening. Calls from numbers not in your contacts will go directly to voicemail. Legitimate callers will leave a message; scammers typically will not.

☐ Set up account alerts on your bank and credit cards

Log into each of your financial accounts and look for Alerts or Notifications in the settings. Enable alerts for every transaction, every login, and any change to your account information. These notifications arrive by text or email in real time. If you receive an alert for a transaction you did not make, call the number on the back of your card immediately.

☐ Update your devices and apps regularly

On your smartphone, go to Settings and find Software Update or System Update. Install any available updates immediately. On your computer, make sure automatic updates are turned on for your operating system and your web browser. Also open your app store once a month and update all installed apps. Security patches in these updates close vulnerabilities that criminals actively exploit.

☐ Know how to report fraud if it happens to you

Save these contacts now so you are not searching under stress later. Report scams and identity theft to the FTC at ftc.gov or 877-382-4357. Report internet crimes at ic3.gov. Contact the FCC about scam calls at 888-225-5322. For Social Security-related fraud, call the SSA at 1-800-772-1213. For Medicare fraud, call 1-800-MEDICARE. Acting quickly — within the first 24 to 48 hours — dramatically improves the chance of recovering lost funds.

What to Do Next

Once you have worked through every item on this list, share it with a family member or friend you trust — protecting one person in your circle often protects the whole group. Return to this checklist every six months to make sure your passwords are still unique, your credit is still frozen, and your contact information on financial accounts is current. Digital safety is not a one-time task; it is a rhythm, and the steps above make that rhythm manageable.

Print this page. Work through one box at a time. Every box you check is one more layer of protection.