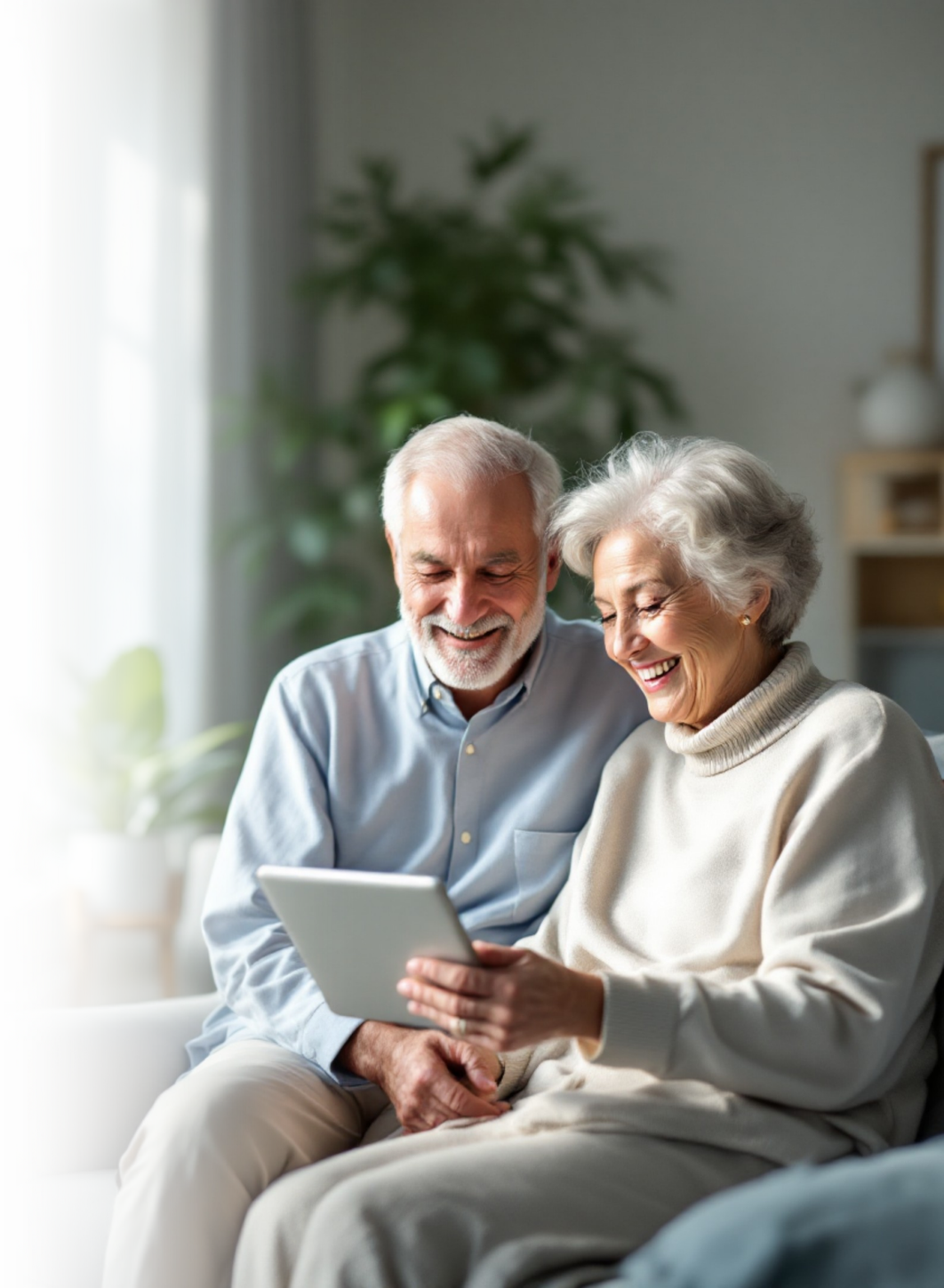
CSNP
CYBERSECURITY NON-PROFIT

Social Media Safety for Seniors

A friendly guide to staying safe on Facebook and protecting your personal information online. Created especially for adults 65+ and their families.



CHAPTER 1

Getting Started with Facebook Safety

Facebook is the most popular social media platform for seniors, connecting you with family and friends. However, it's important to understand basic safety practices before diving in.

Why Facebook safety matters: Scammers specifically target older adults because they often have more savings and trust people easily. Learning these safety basics protects both your money and your personal information.

Don't worry—staying safe on Facebook is easier than you think! Follow our step-by-step guide to enjoy connecting with loved ones while keeping your information secure.

Quick Safety Tip

If something feels wrong or suspicious on Facebook, trust your instincts. It's always better to be cautious and ask a family member for help.

CHAPTER 2

Essential Privacy Settings You Need to Change

Facebook's default settings often share more than you'd like. Take 10 minutes to adjust these critical privacy controls and protect your personal information.

01

Access Privacy Settings

Click the down arrow in the top-right corner, then select "Settings & Privacy" and click "Privacy Shortcuts"

02

Control Who Sees Your Posts

Set "Who can see your future posts?" to "Friends" instead of "Public" to limit who views your content

03

Review Your Profile Visibility

Go to "Privacy Checkup" and limit who can see your email, phone number, and birthday to "Only Me" or "Friends"

04

Manage Friend Requests

Change "Who can send you friend requests?" to ensure you only receive requests from real people, not fake accounts

CHAPTER 3

Spotting Fake Profiles and Friend Request Scams

Scammers create fake profiles to trick people into sharing money or personal information. Learn the warning signs to protect yourself.

1

Check Their Friends List

Real people usually have 100+ friends with visible connections. Be suspicious of profiles with very few friends or friends you don't recognize.

2

Look at Their Photos

Fake profiles often have only 1-3 photos, or photos that look like models or stock images. Real people have varied, casual photos over time.

3

Review Profile Age

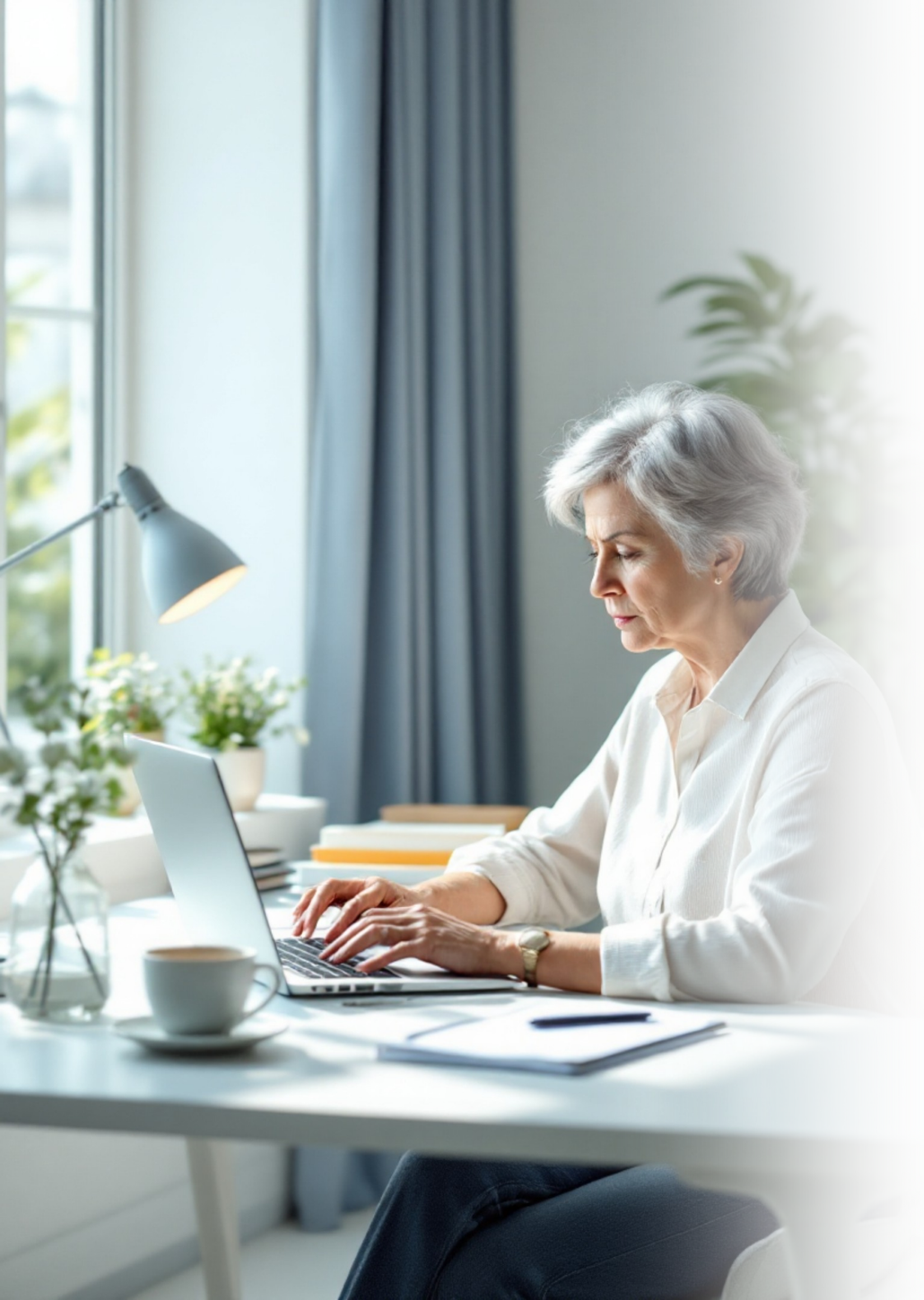
Check when they joined Facebook. New accounts (created in the last few weeks) requesting friendship are often scams.

4

Watch for Duplicate Requests

If someone who's already your friend sends another request, it's likely a scammer copying their profile. Contact your real friend to verify.

Golden Rule: If you don't personally know someone in real life, don't accept their friend request—even if you have mutual friends.



CHAPTER 4

What NOT to Share on Facebook

Financial Information

- Bank account or credit card numbers
- Social Security number
- Investment account details
- Tax information

Personal Security Details

- Your full birthdate (especially year)
- Home address or phone number
- Current location or travel plans
- Passwords or security questions

Family Safety Information

- Grandchildren's schools or locations
- Photos of grandkids without parents' permission
- Family members' personal details
- Home security system information

Remember: Once something is posted online, it can never be completely deleted. Scammers use personal details to steal identities or target you with scams.

CHAPTER 5

Common Facebook Marketplace Scams

Facebook Marketplace is convenient for buying and selling locally, but scammers use it to steal money. Stay alert for these common tricks.

Warning Signs of Scams

- **Too Good to Be True Prices:** Items priced far below market value are usually scams designed to steal your money or information.
- **Requests for Prepayment:** Legitimate sellers meet in person. Never send money, gift cards, or wire transfers before seeing the item.
- **Pressure to Act Fast:** Scammers create urgency ("Sale ends today!") to prevent you from thinking clearly.
- **Shipping Requests:** Marketplace is for local pickup. If they insist on shipping, it's likely a scam.

Safe Buying Tips

Meet in Public Places

Always meet at police station parking lots, busy coffee shops, or bank lobbies during daylight hours.

Bring Someone With You

Never meet alone. Bring a family member or friend for safety and a second opinion.

Use Cash Only

Pay with cash in person. Avoid checks, money orders, payment apps, or wire transfers for Marketplace transactions.

CHAPTER 6

How to Report Problems and Get Help

If you encounter suspicious activity, scams, or inappropriate content on Facebook, reporting it protects both you and others. Here's exactly what to do.

Find the Report Button

Click the three dots (•••) in the top-right corner of any post, profile, or message you want to report

Select "Report"

Choose the appropriate reason: scam, fake profile, harassment, or inappropriate content from the menu options

Follow the Prompts

Facebook will guide you through additional questions. Answer honestly and provide any relevant details

Block the Person

After reporting, block the account to prevent them from contacting you again or viewing your profile

Important: If someone asks for money claiming to be a family member in an emergency, call that family member directly before sending anything. This is a very common scam targeting seniors.

CHAPTER 7

Sharing Photos and Updates Safely with Family

Connecting with family is one of the best parts of Facebook! Follow these guidelines to share memories while protecting everyone's privacy and safety.

Ask Permission First

Before posting photos of grandchildren, always ask their parents for permission. Some families prefer to keep children's images private online for safety reasons.

Use Facebook's "Friends Only" Setting

When posting family photos or updates, select "Friends" from the audience selector. Never use "Public" for personal family content.

Create Private Family Groups

Consider creating a private Facebook group just for close family members. This keeps conversations, photos, and updates completely private and secure.

Avoid Oversharing Locations

Don't tag specific locations where grandchildren spend time regularly, such as schools, daycares, or sports practice fields. This information could be used by strangers.

QUICK REFERENCE

Your Facebook Safety Checklist

Keep this handy reference guide nearby whenever you use Facebook. Print it out or bookmark this page for easy access!

Daily Safety Habits

- Check that posts are set to "Friends" before sharing
- Review friend requests carefully before accepting
- Never click suspicious links in messages
- Log out when using shared computers
- Use a strong, unique password

Red Flags to Watch For

- Messages asking for money or gift cards
- Friend requests from people you don't know
- Posts or messages with urgent language
- Requests for personal or financial information
- Deals that seem too good to be true

When in Doubt...

Stop, breathe, and ask for help. Contact a trusted family member, friend, or call CSNP's helpline before taking action. Scammers rely on pressure—give yourself time to think.

Cybersecurity Non-Profit (CSNP)

Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

Business & Non-Profit Security

Protecting organizations of all sizes with comprehensive cybersecurity training and resources

Family Cybersecurity

Keeping families safe online with practical guidance for all ages and technical skill levels

Kids Safety

Teaching children how to navigate the digital world safely and responsibly

Senior Digital Safety

Empowering older adults to confidently use technology and protect themselves from scams

Women's Security

Addressing unique cybersecurity challenges and providing targeted safety resources

Parents & Educators

Equipping adults with tools to guide and protect young people in digital spaces

Everything we offer is completely free. Visit us at **csnp.org** or explore our resources at **csnp.org/resources**