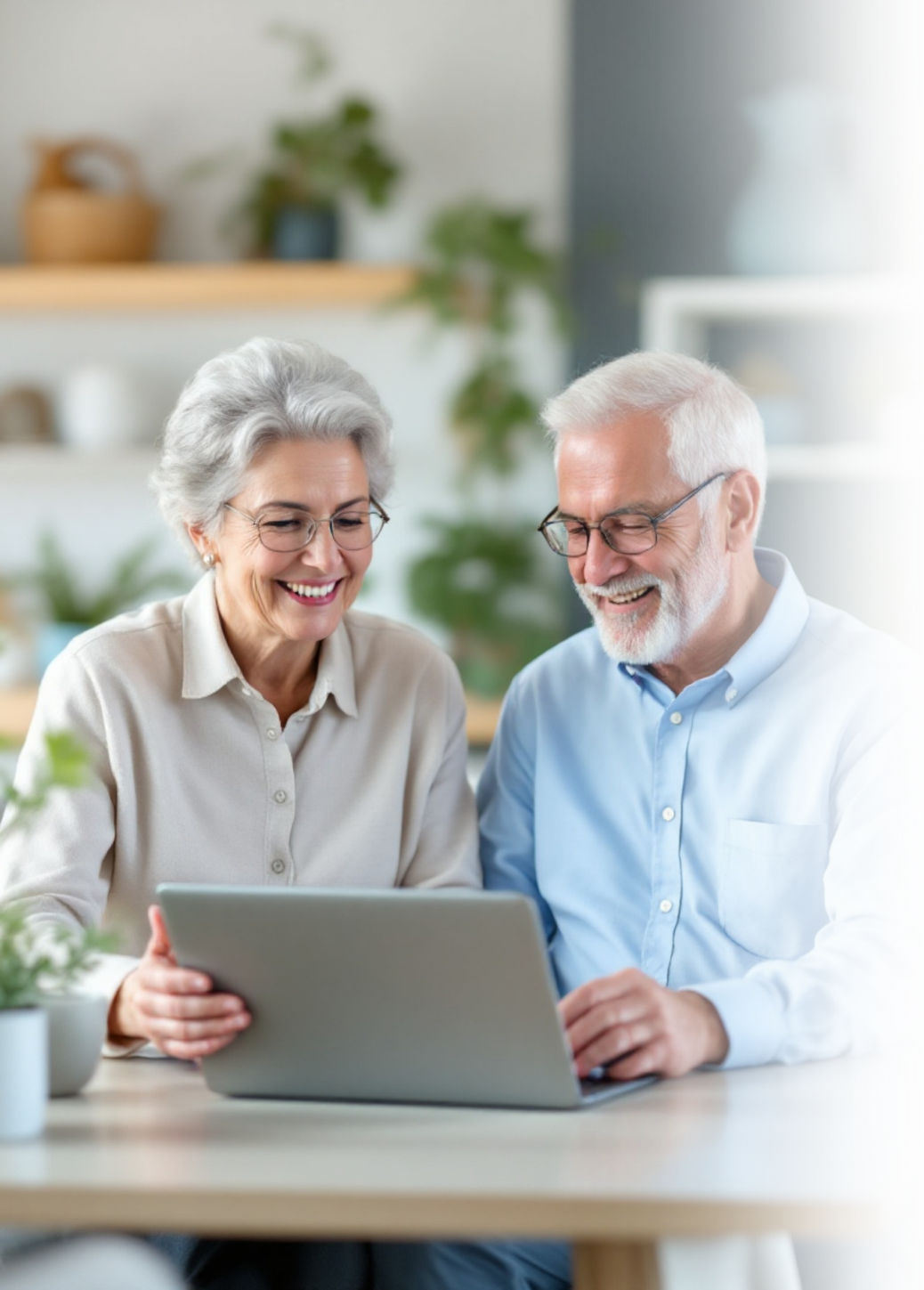


CSNP
CYBERSECURITY NON-PROFIT

Safe Online Shopping Guide for Seniors

A step-by-step guide to help you shop online with confidence and security. Shopping from home can be convenient and safe when you know what to look for.

CYBERSECURITY NON-PROFIT

Recognizing Safe Websites

Look for the Padlock

Check for a padlock icon next to the website address at the top of your browser. This means the site is secure.

HTTPS in the Address

The website address should start with "https://" not just "http://". The "s" stands for secure.

Check the Web Address

Make sure the website name is spelled correctly. Scammers create fake sites with similar names.

Before entering any personal information, take a moment to verify these three important security signs. Trust your instincts—if something feels wrong, it probably is.

Creating Secure Accounts

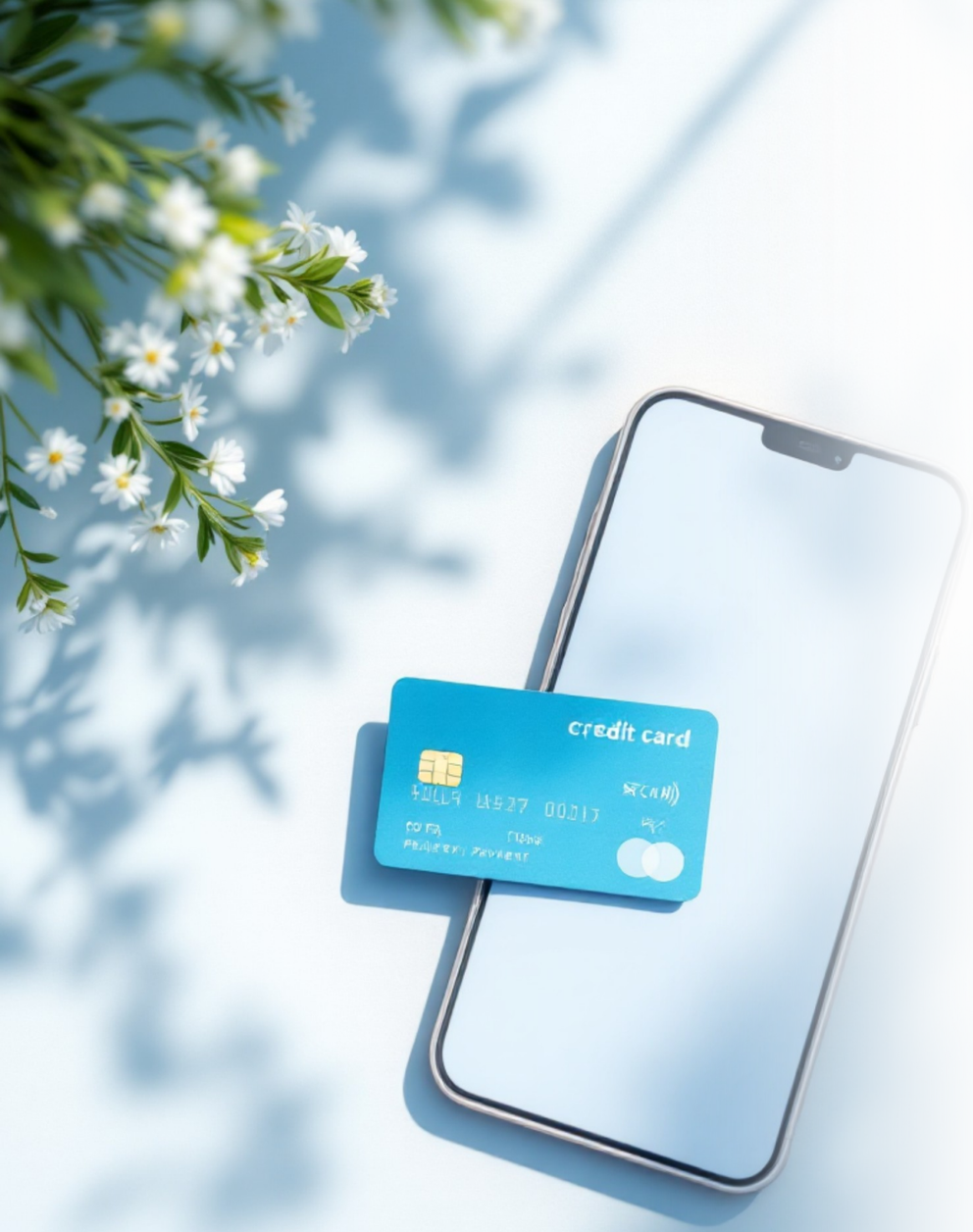
Strong Passwords

- Use at least 12 characters
- Mix letters, numbers, and symbols
- Avoid birthdays or pet names
- Use a different password for each site
- Consider a password manager

Account Safety Tips

- Never share your password with anyone
- Turn on two-factor authentication when available
- Use your real email address for account recovery
- Review account activity regularly
- Log out after shopping

Write down passwords in a notebook kept in a safe place at home. This is safer than reusing simple passwords you can remember.



Safe Payment Methods

01

Credit Cards Are Safest

Credit cards offer the best fraud protection. If something goes wrong, you can dispute the charge.

02

Avoid Debit Cards Online

Debit cards are connected directly to your bank account. If stolen, thieves can drain your account immediately.

03

Use Trusted Payment Services

PayPal, Apple Pay, and Google Pay add extra security layers between you and the seller.

04

Never Wire Money or Send Gift Cards

Legitimate businesses never ask for payment via wire transfer, gift cards, or cryptocurrency.

Spotting Fake Online Stores

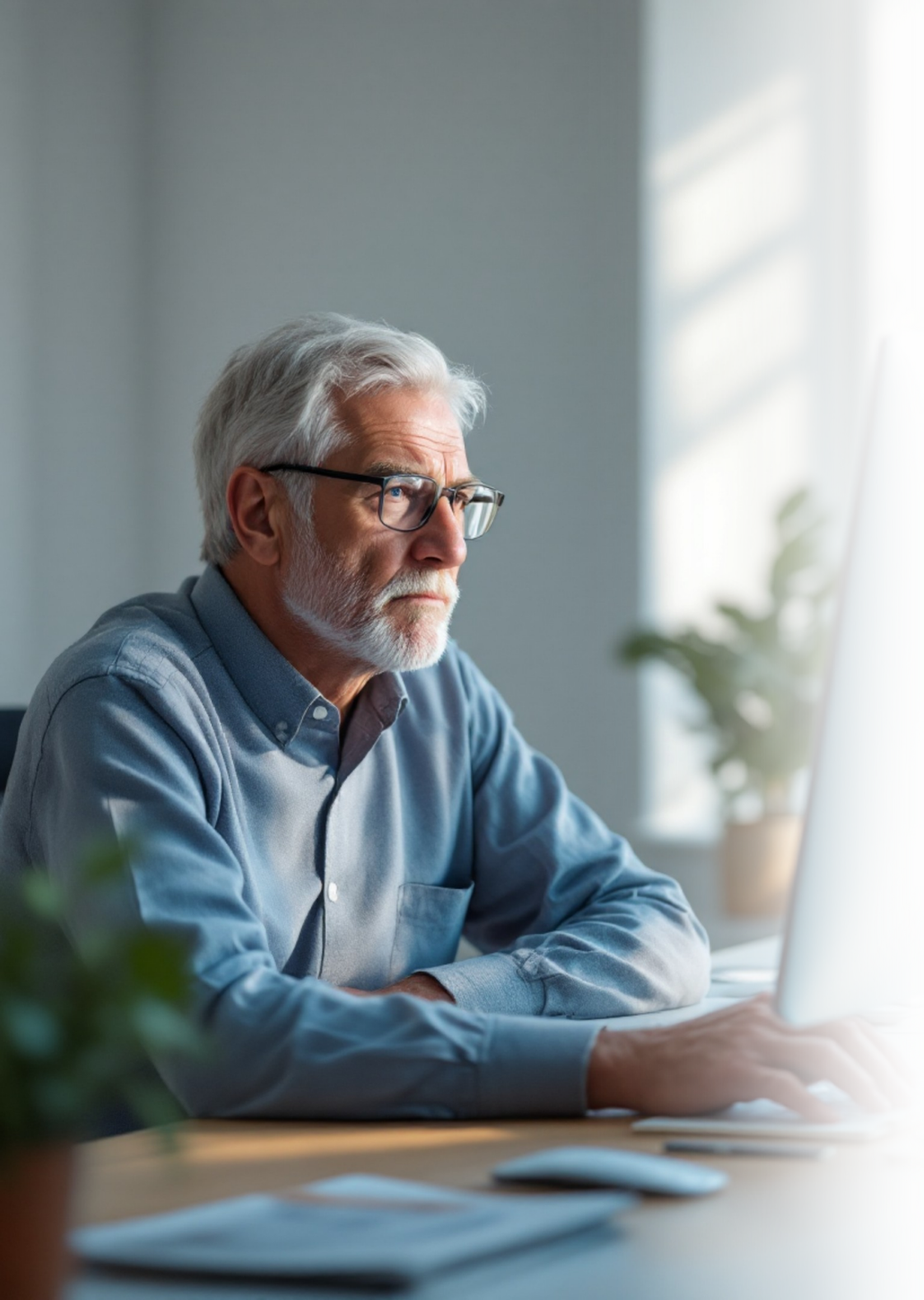
Warning Signs of Fake Stores

- Prices that seem impossibly low
- Poor spelling and grammar
- No phone number or physical address
- Only accepts wire transfers or gift cards
- Pressure to "act now" or "limited time"

Signs of Legitimate Stores

- Clear contact information and customer service
- Professional website design
- Detailed return and refund policies
- Customer reviews from multiple sources
- Secure payment options

When in doubt, search for the store name plus "reviews" or "scam" to see what others are saying. Stick with well-known retailers when possible.



If It Sounds Too Good to Be True, It Probably Is

Beware of Unbelievable Discounts

A brand new laptop for $100? Designer handbags for $20? These extreme discounts are almost always scams or counterfeit products.

Watch Out for Fake Ads

Scammers create fake advertisements on social media and search engines. Just because you see an ad doesn't mean it's legitimate.

Research Before You Buy

Take time to compare prices on several trusted websites. Check independent review sites before purchasing from unfamiliar stores.

Protecting Your Credit Card Information

- **Never save card details on websites**

  Enter your card information each time you shop for maximum security.

- **Check your statements weekly**

  Review charges regularly to catch unauthorized purchases quickly.

- **Set up fraud alerts**

  Most banks will text or email you about suspicious activity.

- **Shop on your home network**

  Avoid making purchases on public WiFi at cafes or libraries.

Keep your card company's phone number handy. Report suspicious charges immediately—most banks have 24/7 fraud lines.

Avoiding Delivery and Package Scams

1

Verify Tracking Information

Only click tracking links from the retailer's official website or app. Scam emails contain fake tracking links.

2

Beware of Fake Delivery Texts

Legitimate delivery services don't ask for payment or personal information via text message.

3

Don't Click Links in Unexpected Emails

If you get a delivery notice for something you didn't order, go directly to the carrier's website instead of clicking the link.

4

Verify Before Opening

Check that packages are addressed to you before opening. Brush-scams send items to create fake reviews.

Your Safe Shopping Checklist

1

Before Shopping

- Verify the website is secure (padlock and https)
- Research the store and read reviews
- Compare prices across trusted websites

2

During Checkout

- Use a credit card, not a debit card
- Review the total cost including shipping
- Save or print your order confirmation

3

After Purchase

- Check your credit card statement
- Track your package on the official website
- Keep all receipts and order numbers

4

Returns and Refunds

- Read the return policy before buying
- Keep original packaging until you're satisfied
- Document any issues with photos
- Contact customer service through official channels

Cybersecurity Non-Profit (CSNP)

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

Our Free Programs for Everyone

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

All our educational resources, workshops, and support are completely free. Visit us at **csnp.org** or explore our resource library at **csnp.org/resources** to continue learning about staying safe online.

FREE RESOURCES | COMMUNITY SUPPORT | EXPERT EDUCATION