CSNP

CYBERSECURITY NON-PROFIT

Medication & Banking Safety Online

A practical guide to staying safe when managing your health and finances online. Created by the Cybersecurity Non-Profit (CSNP) to help you navigate the digital world with confidence.

CHAPTER 1

Safe Online Pharmacies: What to Look For

Verify Credentials

Look for VIPPS certification (Verified Internet Pharmacy Practice Sites). Check the pharmacy is licensed in your state. A legitimate pharmacy will always require a valid prescription from your doctor.

Contact Information

The website must display a physical U.S. address and phone number. Be cautious of pharmacies that only provide email contact or no contact information at all.

Pricing Red Flags

Beware of prices that seem too good to be true. Extremely low prices often indicate counterfeit or expired medications. Compare prices across several trusted pharmacies.

CHAPTER 1

Recognizing Prescription & Medicare Scams

Common Prescription Scams

- Unsolicited calls offering discount medications
- Emails promoting "miracle" drugs or treatments
- Websites selling prescription drugs without requiring a prescription
- Requests for payment via gift cards or wire transfer

Medicare Scam Warning Signs

- Calls claiming your Medicare card is expired or suspended
- Offers of "free" medical equipment or testing
- Requests for your Medicare number over the phone
- Pressure to make immediate decisions

Remember: Medicare will never call you asking for personal information or payment details. If in doubt, hang up and call Medicare directly at 1-800-MEDICARE.

CHAPTER 2

Online Banking Safety Essentials

01

Use Strong Passwords

Create passwords with at least 12 characters, mixing letters, numbers, and symbols. Never reuse passwords across different accounts. Consider using a password manager to keep track.

02

Enable Two-Factor Authentication

Add an extra layer of security by requiring a code sent to your phone. This prevents hackers from accessing your account even if they know your password.

03

Monitor Your Accounts Regularly

Check your bank statements weekly for unauthorized transactions. Set up account alerts to notify you of large withdrawals or unusual activity.

04

Use Secure Connections

Only access your bank account from your home Wi-Fi or cellular data. Avoid public Wi-Fi networks at coffee shops, libraries, or airports for banking.

CHAPTER 2

Bank App Security: Protecting Your Mobile Banking

Download Official Apps Only

Always download banking apps directly from your bank's official website or from the Apple App Store or Google Play Store. Verify the app developer is your actual bank before installing.

Lock Your Device

Use a PIN, password, fingerprint, or face recognition to lock your phone. Enable automatic locking after a few minutes of inactivity to prevent unauthorized access.

Keep Apps Updated

Install updates promptly when your bank releases them. Updates often include important security fixes that protect against new threats and vulnerabilities.

CHAPTER 2

Recognizing Banking Scams

Phishing Emails & Texts

Banks never ask for passwords, PINs, or account numbers via email or text. Be suspicious of urgent messages claiming your account is locked or compromised. Always contact your bank directly using the number on your card.

Imposter Calls

Scammers may claim to be from your bank's fraud department. They often create urgency, saying your account is at risk. Never give out personal information over the phone. Hang up and call your bank's official number.

Tech Support Scams

Fraudsters pretend to be tech support, claiming your computer has a virus affecting your bank account. They may ask for remote access to your computer. Real tech support never contacts you unsolicited.

Your Safety Checklist

Medication Safety

- ✓ Verify pharmacy is VIPPS certified
- ✓ Check for U.S. license and address
- ✓ Require valid prescription
- ✓ Compare prices across trusted sites
- ✓ Never share Medicare number unsolicited

Banking Safety

- ✓ Use strong, unique passwords
- ✓ Enable two-factor authentication
- ✓ Monitor accounts weekly
- ✓ Avoid public Wi-Fi for banking
- ✓ Keep apps and devices updated
- ✓ Never share account details via phone/email

Print this checklist and keep it near your computer as a quick reference. Share it with family members who help manage your accounts.

About the Cybersecurity Non-Profit (CSNP)

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

Our Programs

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

Everything we offer is completely free. Visit us at **csnp.org** or explore our resources at **csnp.org/resources** to learn more about staying safe online.