

## My Cyber Safety Action Plan

Name: \_\_\_\_\_ Date: \_\_\_\_\_

Choose 1–3 actions you will do in the next month. Even one action makes you harder to scam.

### 1. My Everyday Safety Habits

- **Trusted Numbers & Websites List:** I will make a small list of trusted phone numbers and websites (bank, doctor, pharmacy, government) and use only those when I need to call or log in.
- **My Personal Safety Rule:** I will choose one clear rule, write it down, and keep it by my phone or computer.  
Example rules:
  - “I let unknown numbers go to voicemail.”
  - “I never click links in messages about money or prizes.”
  - “I don’t share codes or passwords with anyone who contacts me.”
- **Let Unknown Numbers Go to Voicemail:** I will stop answering unknown numbers and let them go to voicemail first.
- **Sticky Note Reminder:** I will put a small note near my phone/computer that says: “If it’s about money or panic → HANG UP & VERIFY.”

### 2. Protecting My Money & Accounts

- **Turn On Bank Alerts:** I will ask my bank to turn on alerts (text/email) for large withdrawals, new payees, or unusual activity.
- **Check My Statements Monthly:** Once a month, I will check my bank/credit card statements for any transactions I don’t recognize.
- **Update One Device:** This week, I will check that automatic updates are on my phone or computer and run any waiting updates.
- **Stronger Login Protection:** I will improve security on one important account (bank or email) by using a stronger/different password or turning on two-step verification (codes when I log in).

### 3. Handling Messages, Calls, and Texts

- **Practice My “No” Script:** I will practice one safety sentence out loud at least three times this week so it’s ready if I get a scam call.  
Example:  
“I don’t give information on calls I didn’t start. I’ll hang up now.”
- **Check the Real Sender:** For the next month, I will look at the actual sender address or phone number before opening messages about money, prizes, or accounts. I will look at other small clues that emails may be phishing.

- **Create a “Scam” Email Folder:** When I spot a suspicious email, I will move it to a folder called “Scams” and not click anything in it.
- **Learn to Block/Report Spam Texts:** I will learn how to block or report spam texts on my phone and use it on the next suspicious message I receive.

#### 4. Staying Informed

- **Save Important Help Numbers:** I will save key numbers in my phone or address book (for example: my bank, fraud line, non-emergency police).
- **Monthly 10-Minute Safety Check-In:** Once a month, I will spend 10 minutes on my cyber safety: check statements, delete obvious scam messages, review my notes or handouts from this session.

#### My Top 1–3 Actions

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_