Fraud Awareness for Elderly People

**1. Understanding Online Fraud**

The internet is a useful tool, but it also comes with risks. Fraudsters try to trick people, especially older adults, into giving away their money or personal information. Understanding these scams can help you stay safe online.

**2. Common Online Scams Targeting Seniors**

Here are some of the most common scams that elderly people should watch out for:

A. Phishing Emails & Messages

What It Is: Fraudsters send emails or messages pretending to be from your bank, government agencies, or companies. These messages often ask for personal details or request you to click a link.

Why It’s Dangerous: Clicking a bad link can install harmful software or steal your login details.

How to Stay Safe:

Never click on links or download attachments from unknown emails.

Always check the sender’s email address—official organizations do not send emails from personal accounts like "@gmail.com."

If in doubt, call the company directly to verify.

(Include an image showing an example of a phishing email with warning signs highlighted.)

B. Lottery & Prize Scams

What It Is: Scammers send messages claiming you have won money, a car, or a prize but ask you to pay a fee to claim it.

Why It’s Dangerous: If you pay, you will likely never receive any prize, and scammers may continue to ask for more money.

How to Stay Safe:

If you didn’t enter a contest, you didn’t win anything.

Never send money or personal details to claim a "prize."

Report such messages to authorities.

(Include an image of a fake lottery email asking for money.)

C. Tech Support Scams

What It Is: Scammers call pretending to be from Microsoft, Apple, or your internet provider, saying your computer has a virus.

Why It’s Dangerous: They may ask you to install remote access software, which allows them to control your computer and steal information.

How to Stay Safe:

Companies do not call you about tech issues unless you ask for help.

Never allow strangers to access your computer remotely.

If you get such a call, hang up immediately.

(Include a video showing how a tech support scam works and how to respond.)

D. Romance & Friendship Scams

What It Is: Scammers create fake profiles on social media and dating sites to form relationships with seniors, then ask for money.

Why It’s Dangerous: They may claim they need financial help for medical emergencies or travel expenses.

How to Stay Safe:

Be cautious of people you meet online who quickly express love or ask for money.

Never send money or share bank details with someone you haven’t met in person.

Talk to family members before continuing an online relationship.

(Include an image of a fake dating profile with common scam signs highlighted.)

E. Investment & Pension Fraud

What It Is: Fraudsters may offer fake investment opportunities, promising high returns with little risk.

Why It’s Dangerous: You could lose your savings or retirement money.

How to Stay Safe:

Research investment opportunities thoroughly before investing.

Consult a trusted financial advisor before making any decisions.

Be skeptical of "guaranteed" profits—if it sounds too good to be true, it probably is.

(Include an infographic on safe investment tips.)

**3. How to Protect Yourself from Online Scams**

Use Strong Passwords: Create passwords with a mix of letters, numbers, and symbols. Avoid using your name or birthdate.

Enable Two-Factor Authentication (2FA): This adds an extra layer of security when logging into accounts.

Beware of Urgent Requests: Scammers try to create urgency—stay calm and verify the request.

Install Security Software: Keep your computer and phone updated with antivirus software.

Consult Family or Friends: If something seems suspicious, talk to someone you trust before taking action.

**4. What to Do If You Suspect Fraud**

Stop Communication Immediately – If you think someone is trying to scam you, do not reply to their messages or calls.

Report the Scam – Notify your bank, local authorities, or cybercrime portals.

Change Your Passwords – If you shared login details, update your passwords immediately.

Educate Yourself – Stay informed about new scams through trusted websites and news sources.

(Use an easy-to-read checklist summarizing these steps.)

**Remember!**

Online fraud is common, but by staying informed and being cautious, you can protect yourself. If something seems suspicious, always ask a trusted family member or friend before taking action.

(End with an image of a happy senior using technology safely!)