INDOAMERICAN IASGH
SENIORS OF GREATER HOUSTON

Scams & Identity Theft – Quick Guide

Typical Targets

- Seen as trusting
- Financially stable
- Less tech-savvy

Common Scams

- **Phone:** IRS, Medicare, "grandchild in jail".
- **Email:** Bank alerts, prize winnings, suspicious attachments.
- **Door-to-door:** Fake contractors, charities.

Spotting Fraud

- Urgent or threatening tone.
- Spelling mistakes or odd grammar.
- Strange links or attachments.
- www.haveibeenpwned.com
- **Rule: Don't click, don't reply, verify first.**

Credit & Banking

- Use trusted ATMs; shield your PIN.
- Shop only on secure sites (https:// + padlock 🔒 in the address bar).
- Set up bank alerts for unusual activity.

Protecting Your Info

- Guard SSN, bank info, passwords.
- Shred old documents.
- Use strong passwords.
- Don't carry all IDs/cards at once.

Stay Safe Online

- Keep devices updated.
- Avoid pop-ups and fake alerts.
- Use antivirus protection.

Investment Red Flags

- "Guaranteed returns" = scam.
- Pressure to act fast.
- Check sellers with FINRA or SEC.

If Identity Theft Happens

- Call your bank/credit card company.
- Place fraud alert or freeze credit.
- Report at IdentityTheft.gov.
- File a police report.

Reporting Scams

- Houston Police Department.
- Texas Attorney General – Consumer Protection.
- FTC: ftc.gov/complaint.
- AARP: 1-877-908-3360
  https://www.aarp.org/forms/scam-map-form-page/

✓ Quick Checklist

☑ I hang up on suspicious calls.

☑ I never click unknown links.

☑ I shred old documents.

☑ I monitor my SSN/bank accounts.

☑ I know where to report fraud.