



Scams are schemes or fraudulent activities designed to *trick people into giving away data* such as: personal information, money, or property.

Seniors may be targeted due to:

- high amount of savings
- unfamiliarity with modern technology
- trusting and polite

These attributes are what scammers aim to exploit!



Types of Scams
include:

- Phone Scams**, e.g. pretend to be government officials or tech support
- Online Scams**, e.g., fake emails or websites asking for personal info
- Romance Scams**, e.g., gain trust by building a relationship with you
- Grandparent Scams**, e.g., callers say your grandchild is in trouble and needs money
- Investment Scams**, e.g., fake investment opportunities that aren't legitimate

Tips to Recognize Scam

Sense of Urgency	Too good to be true	Personal Information Inquiries
Push for immediate action sent to a third party such as: ◦ money ◦ personal details on yourself or your family	May be alerted to receive a large sum of money out of a draw, contest or competition ◦ check it's size and sponsors	Sensitive information may be asked for: ◦ social insurance number ◦ bank details ◦ name and date of birth

It is never your fault if you ever get targeted for scam since they cast a wide net nor is it your issue for falling into one of their traps because they are designed that way.

So what can we do to prevent being a victim to scam?



Recent Types of Scams

What are some Scams that we may see now?

Spoofing

Caller ID	Email	Websites
• Call resembles a trusted number seeking out your personal information ◦ ex. bank or government agency	• Email address forgery into a legitimate contact prompting you to click on malicious links or leak information	• Fake websites resemble reputable one's, urging you to enter sensitive login credentials

SIM Swap Fraud / SIM Hijacking

Phone number is transferred to a new SIM card under their control, allowing for them to:

- **Bypass Two-Factor Authentication (2FA):** services and authentication codes often sent via SMS
- **Take-over Accounts:** Reset passwords and Gain access
- **Withdraw Funds:** Bypass bank security features to transfer money out

Deepfake Scams

AI used to create realistic fake videos or audio recordings, impersonating trusted individuals or celebrities



Quishing

Malicious links embedded within QR codes and redirected to fraudulent websites designed to steal personal information or install malware



Pig Butchering Scams

Build trust with victims over time, then convince them to invest in fake cryptocurrency



Rise in Scams

- increased commercialization of fraud tools and services
- advancements in AI allows for easy creation of highly personalized and convincing phishing emails and messages
 - overall, fraudulent schemes more sophisticated and harder to detect





"You can never be too careful"

Tips to Stay Safe

1. Keep your personal information private.
2. Don't share personal or financial details with unknown people.
3. Be cautious online.
4. Use strong passwords and be careful of unsolicited emails.
5. Verify before you trust.
6. Always double-check the identity of someone asking for money or personal info.
7. Stay updated.
8. Attend scam prevention workshops and follow news about current scam tactics.

Always stay attentive and aware of the intentions people might have!

Why we should be aware of scamming methods?

- **Scams targeting seniors are on the rise:** Increasing the chance of coming across one
- **Recognize warning signs as a precaution:** It teaches us ways to protect ourselves
- **Always verify and report:** Don't hesitate to voice out your concerns about anything you find suspicious

Let's all help **raise awareness** about scams by mentioning it to our peers, family and community. We should not be taken advantage of and let's stick together!