Connecting Generations
Cyber-Seniors™

How to Spot Government Imposter Scams

Government Imposter Scams involve fraudsters pretending to be government representatives to steal money or personal information. These scams occur through various communication channels such as phone calls, emails, and text messages. This guide will help you identify, prevent, and respond to such scams.

Common Government Imposter Scams

1. **IRS/CRA Scams** – Fraudsters claim you owe back taxes or have committed financial crimes, demanding payment via transfers, gift cards, or cryptocurrency.
2. **Social Security/Insurance Scams** – Scammers claim illegal activity under your SIN/SSN or request payment for fake benefits.
3. **Medicare/Medicaid/Healthcare Scams** – Involve fake offers, pressure to switch plans, fraudulent card renewal notices, or coverage threats.
4. **Law Enforcement Scams** – Fake threats about missed jury duty, illegal packages, or fines. Some target specific communities, like Asian individuals, by pretending to be foreign law enforcement.

How Scammers Contact You

- **Phone Calls:** Unsolicited calls, robocalls, spoofed numbers, and aggressive threats.
- **Emails:** Look out for inconsistencies, spelling errors, suspicious attachments, and incorrect logos.
- **Text Messages:** Unexpected texts with shortened or suspicious links, poor grammar, and unverified numbers.

Warning Signs of a Scam

- Unsolicited government communication
- Requests for sensitive personal or financial information
- Urgent threats of arrest, deportation, or fines

- Payment requests via unconventional methods (gift cards, wire transfers, crypto)
- Suspicious links or attachments

How to Handle Scam Communications

- Text Messages: Delete, mark as spam, and block the sender.
- Phone Calls: Do not engage, hang up immediately, and block the number.
- Emails: Mark as spam and block the sender.
- Verify Legitimacy: Contact the government agency through official channels, log into your online accounts securely, and search for scam reports online.

Proactive Protection Steps

- Use security software, VPNs, and password managers.
- Avoid oversharing personal information online.
- Adjust privacy settings on social media and accounts.
- Properly dispose of sensitive documents.
- Register for Do Not Call lists (USA: donotcall.gov, Canada: lnnte-dncl.gc.ca).

Reporting Scams

- U.S.: Report fraud to the Federal Trade Commission (FTC) at reportfraud.ftc.gov or call 1-877-FTC-HELP.
- Canada: Report to the Anti-Fraud Centre at antifraudcentre-centreantifraude.ca or call 1-888-495-8501.
- Contact local law enforcement.

If You Have Been a Victim

- Stop any payments to scammers.
- Freeze your credit and alert your financial institution.
- Change passwords for compromised accounts.
- Document all communications and fraud details for reporting.

Need More Help?

For more information, contact Cyber-Seniors at **844-217-3057** or visit **www.cyberseniors.org**.

*This lesson guide was made possible by a **CIRA Net Good Grant**. Learn more at **cira.ca**.*