Bringing Generations Together

PAK PIONEERS COMMUNITY ORGANIZATION OF CANADA

Internet Safety & Scam Awareness

A step-by-step guide for staying safe online, written especially for you, with clear language and real-life examples.

BEGINNER FRIENDLY

PRACTICAL & REALISTIC

What You Will Learn Today

By the end of this lesson, you will be able to recognize common scams, protect your personal information, and know exactly what to do if something feels wrong online.

01

Recognize Scams

Spot fake emails, texts, and phone calls before they fool you.

02

Protect Yourself

Use strong passwords and visit only safe websites.

03

Take Action

Know exactly what to do if you think you've been scammed.

04

Practice & Review

Test your knowledge with real examples at the end.

The Most Common Scams Targeting Seniors

Scammers specifically target older adults because they are often polite, trusting, and less familiar with online tricks. Here are the most common types you need to know:

Phishing Emails

Fake emails pretending to be from your bank, Medicare, or Amazon — designed to steal your password or credit card number.

Scam Phone Calls

A caller pretends to be from the IRS, Social Security, or tech support. They pressure you to act fast and pay immediately.

Fake Text Messages

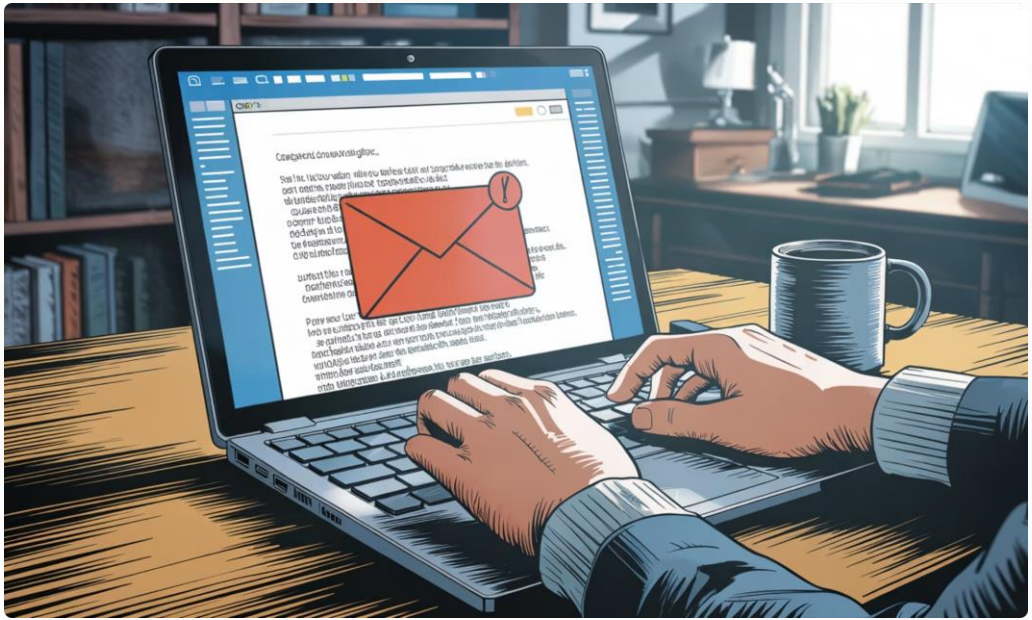
A text says your package is delayed or your account is locked — with a link that steals your information when clicked.

Social Media Scams

Fake friends, fake giveaways, and romance scammers who build your trust over time before asking for money.

How to Spot a Phishing Email

Phishing (say it like "fishing") means a scammer is "fishing" for your personal information by pretending to be someone you trust — like your bank or Medicare.



🚩 Red Flags to Look For

- **Urgent language:** "Your account will be closed TODAY!"
- **Strange sender address:** support@amaz0n-help.net (not a real Amazon address)
- **Spelling mistakes:** Real companies rarely make typos
- **They ask for your password or Social Security number** — real companies NEVER do this by email
- **Suspicious links:** Don't click — hover over the link to see where it really goes

🛑 STOP: Your real bank will NEVER email you asking for your password or full account number. If in doubt, call your bank directly using the number on the back of your card.

Real Example: Safe vs. Scam Email

Let's look at two emails side by side. One is real. One is a scam. Can you spot the difference?

✅ Real Email (Safe)

From: support@chase.com

Subject: Your monthly statement is ready

"Hello Maria, your April statement is now available. Log in at chase.com to view it. We will never ask for your password."

- Correct email address ending in @chase.com
- No urgent threats
- No request for personal info
- Directs you to the official website

🚨 Scam Email (Fake)

From: alert@chase-secure-login.net

Subject: URGENT: Your account has been SUSPENDED

"Dear Customer, your account is locked!! Click here NOW to verify your password or your account will be deleted forever."

- Fake email address — not chase.com
- Uses scary, urgent language
- Asks you to click a suspicious link
- Multiple exclamation marks and ALL CAPS

✅ Rule to remember: When in doubt, do NOT click. Call your bank directly using the phone number on your card or statement.

Scam Phone Calls & Fake Texts

Common Scam Call Scripts

Scammers are trained actors. They sound very official. Here is what they often say:

⚠ ⚠ Helpful Tip: It is always okay to hang up. You do not owe a stranger on the phone your time or your information. Hang up, then call a trusted family member.

"This is the IRS. You owe back taxes."

The IRS always contacts you by mail first — never calls out of the blue demanding immediate payment.

"Your Social Security number has been suspended."

Social Security numbers cannot be "suspended." This is always a scam.

"Your computer has a virus. Let me fix it remotely."

Microsoft and Apple will NEVER call you uninvited about your computer. Hang up immediately.

Creating Strong Passwords

A **password** is like a lock on your front door. A weak password is like using a screen door — easy to push through. A strong password keeps criminals out.

❌ Weak Passwords

- password123
- yourname1950
- 123456
- YourPetName

✅ Strong Passwords

- At least 12 characters long
- Mix of letters, numbers & symbols
- Example: Sunshine$River!2024
- Different for each website

Easy Way to Create a Strong Password

Think of a sentence you will remember, then use the first letter of each word plus some numbers and symbols.

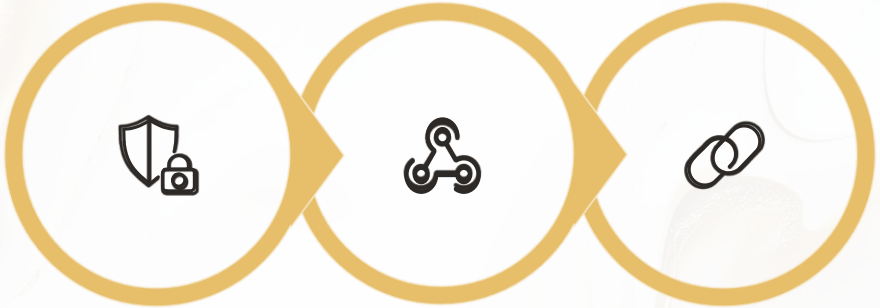
Example sentence: "My dog Biscuit loves walks in the park!"

Password: MdBLw!tp2024

💡 Helpful Tip: Write your passwords in a small notebook kept in a safe place at home — not stored on your phone or computer. Never share passwords with anyone who calls or emails you.

How to Recognize a Safe Website

Before entering any personal information — like your name, address, or credit card — always check that the website is safe. Here is what to look for:



Padlock **HTTPS** **Exact URL**

These three quick checks take only a few seconds and can protect you from fake websites designed to steal your information. If any of these signs are missing, leave the website immediately.

🛑 Never enter your bank account number, Social Security number, or credit card information on a website that is missing the padlock or starts with http:// instead of https://.

Social Media & Banking Scams

Social Media Scams

- A "friend" you don't know well sends you a message asking for gift cards or money for an emergency
- Fake Facebook contests: "You've won! Click here to claim your prize!"
- Romance scams: Someone spends weeks building a friendship, then asks for money for a plane ticket or medical bill

Banking Scams

- A caller says your account was hacked and asks you to move money to a "safe account" — this is always a scam
- Fake bank websites that look identical to the real one
- Emails asking you to "confirm" your debit card number

Gift Card Scams

- Any person or organization asking you to pay using iTunes, Google Play, or Amazon gift cards is running a scam — always
- No government agency, utility company, or legitimate business accepts gift cards as payment

What To Do If You've Been Scammed

First: You are not alone, and it is not your fault. Millions of people are targeted every year. The important thing is to act quickly.

1

Step 1: Stop All Contact

Hang up, stop replying to messages, and do not send any more money or information.

2

Step 2: Call Your Bank

Call the number on the back of your debit or credit card immediately. Ask them to freeze your account if needed.

3

Step 3: Tell Someone You Trust

Call a family member, friend, or trusted neighbor. Do not handle it alone.

4

Step 4: Report It

Report to the FTC at **ReportFraud.ftc.gov** or call **1-877-382-4357**. Your report helps protect others.

✅ Remember: Reporting a scam is a brave and helpful act. It protects your neighbors and community from the same criminals.