CSNP
CYBERSECURITY NON-PROFIT

# Scam Recognition Guide

A practical guide to protecting yourself from common scams. Cybersecurity Non-Profit (CSNP) is here to help you stay safe and informed.

OVERVIEW

# Understanding Today's Scams

Scammers use many tricks to steal money and personal information. They may contact you by phone, email, text, or even appear on your computer screen. The good news: once you know what to look for, you can protect yourself.

**$3.4B**

### Lost to scams

Americans lost billions to scams in 2023

**68%**

### Senior targets

Seniors are targeted more than other age groups

**95%**

### Prevention works

Scams can be prevented with awareness

PHONE SCAMS

# Recognizing Phone Scams

Phone scammers create urgency and pressure. They may claim to be from your bank, the IRS, Social Security, or even a family member in trouble. Remember: legitimate organizations will never demand immediate payment or threaten you.

### Robocalls

Automated messages claiming your account has problems or you owe money. Hang up immediately—your real bank will send a letter.

### Caller ID Spoofing

The number looks real, but scammers can fake any caller ID. Even if it shows a government agency, verify before sharing information.

### High-Pressure Tactics

Demands for immediate action or payment. Real organizations give you time to think and verify. Never feel rushed.

EMAIL SCAMS

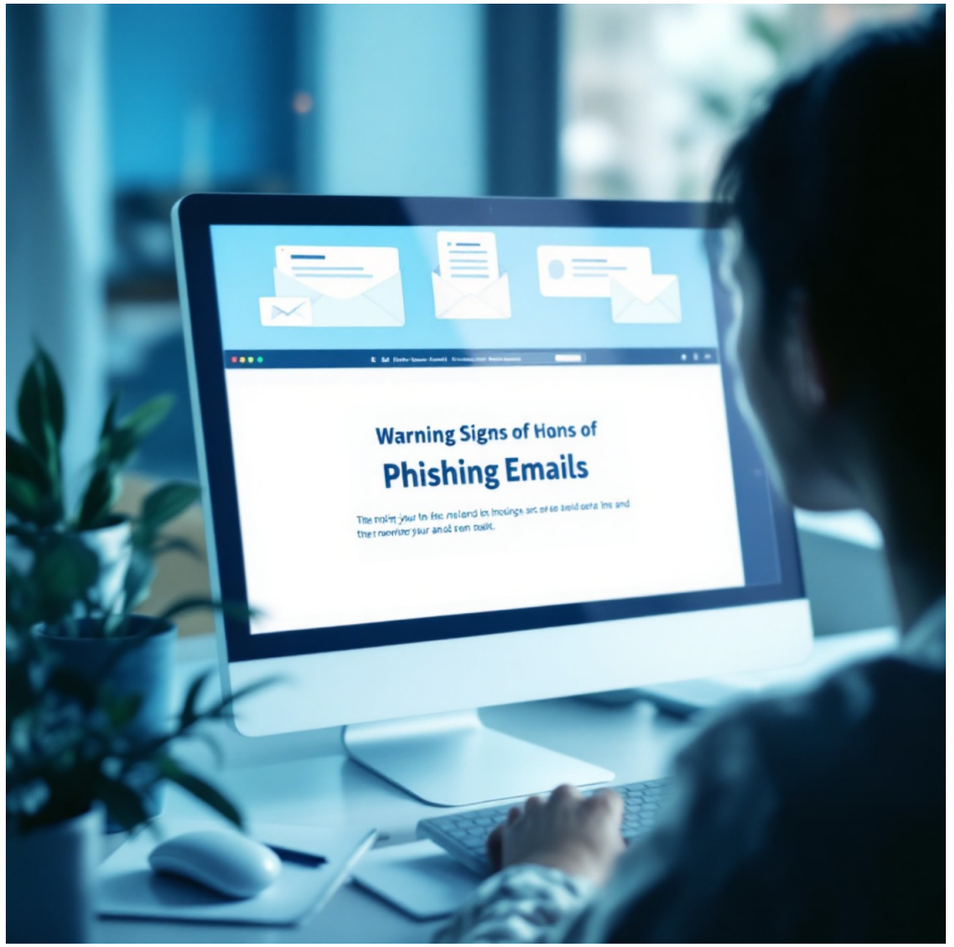
# Spotting Email Scams

Scam emails often look official but contain small mistakes. They ask you to click links, download attachments, or provide personal information. Before clicking anything, look carefully at the sender's address and message content.

## Common Email Scams

- Fake package delivery notices
- Account suspension warnings
- Requests to verify personal information
- Too-good-to-be-true offers
- Messages with urgent language

Never click links in unexpected emails. Go directly to the company's official website instead.



TECH SUPPORT

# Tech Support Scams

## Pop-Up Warnings

Scary messages appear saying your computer has a virus. These are fake. Real security software doesn't work this way. Close the browser window.

## Cold Calls

Someone calls claiming to be from Microsoft or Apple, saying they detected a problem. Companies never call you about computer issues. Hang up.

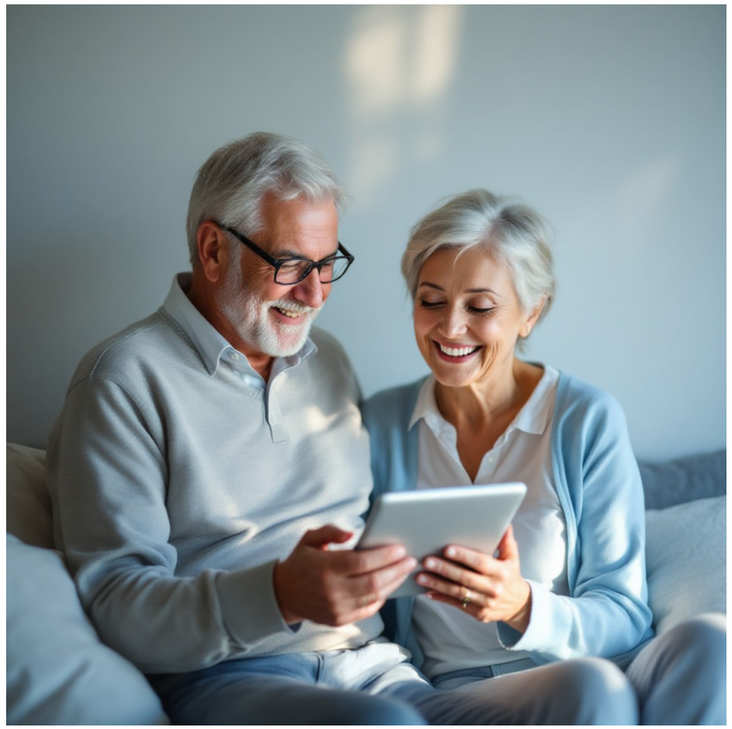
## Remote Access Requests

Scammers ask to remotely control your computer "to fix it." Never give anyone remote access unless you initiated contact with a trusted company.

ROMANCE & LOTTERY

# Romance and Prize Scams

## Romance Scams



Scammers create fake profiles on dating sites or social media. They build trust over weeks or months, then ask for money for emergencies, travel, or medical bills. Real relationships don't start with requests for money.

- Avoid anyone who quickly declares love
- Never send money to someone you haven't met
- Be wary of excuses for not video chatting

## Lottery and Prize Scams


You're told you won a prize or lottery you never entered. To claim it, they say you must pay fees, taxes, or processing costs upfront. Legitimate prizes never require payment.

- You can't win contests you didn't enter
- Real prizes don't require upfront payment
- Pressure to act fast is a red flag

IMPERSONATION

# Government Impersonation Scams

Scammers pretend to be from trusted government agencies to steal your money or personal information. They use official-sounding language and create fear to pressure you into acting quickly.

## IRS Scams

Threats of arrest for unpaid taxes. The real IRS always contacts you by mail first, never by phone demanding immediate payment via gift cards or wire transfer.

## Social Security Scams

Claims your Social Security number is suspended or compromised. Social Security will never call threatening to suspend your benefits or asking for personal information.

## Medicare Scams

Offers for free medical equipment or prescription cards. Medicare representatives don't make unsolicited calls offering products or asking for your Medicare number.

FAMILY EMERGENCY

# Grandparent Scams

This scam preys on your love for family. A caller pretends to be your grandchild in trouble—arrested, in an accident, or stranded abroad. They beg you not to tell their parents and need money urgently wired or sent via gift cards.

## How It Works

The caller may have basic information from social media. They create urgency and secrecy, claiming they need bail money, hospital payments, or travel funds immediately.

## Protect Yourself

Always verify. Hang up and call your grandchild directly on their known number. Ask questions only the real person would know. Tell other family members about the call.

## Remember

Real emergencies can be verified. No legitimate situation requires secrecy from family or payment via untraceable methods like gift cards or wire transfers.

WARNING SIGNS

# Red Flags Checklist

Learn to recognize these common warning signs that indicate a potential scam. Trust your instincts—if something feels wrong, it probably is.

1

## Urgency and Pressure

Demands for immediate action or payment. Legitimate organizations give you time to think and make informed decisions.

2

## Unusual Payment Methods

Requests for gift cards, wire transfers, cryptocurrency, or cash. Real businesses and government agencies don't ask for these.

3

## Threats or Fear Tactics

Warnings of arrest, account closure, or other consequences. This is designed to make you panic and act without thinking.

4

## Requests for Personal Information

Asking for Social Security numbers, bank details, or passwords. Never share sensitive information with unsolicited contacts.

5

## Too Good to Be True

Promises of large prizes, amazing deals, or guaranteed returns. If it sounds too good to be true, it almost always is.

6

## Poor Grammar or Spelling

Professional organizations proofread their communications. Mistakes often indicate a scam attempt from overseas.

TAKE ACTION

# What to Do If You're Contacted

01

## Stay Calm

Don't let pressure or fear drive your decisions. Take a deep breath. It's okay to hang up or close the message.

02

## Don't Engage

Don't click links, download attachments, or provide any information. Don't call back numbers they provide.

03

## Verify Independently

Look up the official contact information yourself. Call the company or agency directly using a number you find on their official website.

04

## Talk to Someone

Discuss it with a trusted family member or friend before taking any action. A second opinion helps you think clearly.

05

## Report It

Report scams to help protect others. Your report can prevent someone else from becoming a victim.

Remember: It's always better to be cautious than to act in haste. Legitimate organizations will understand if you need time to verify.

RESOURCES

# Reporting and Getting Help

If you've been contacted by a scammer or believe you're a victim, report it immediately. These resources are here to help you.

## Where to Report

- **Federal Trade Commission (FTC)**

  ReportFraud.ftc.gov or call 1-877-382-4357. Report scams and identity theft.

- **FBI Internet Crime Complaint Center**

  ic3.gov for online and internet scams. They track and investigate cybercrime.

- **Local Police**

  Contact your local police department if you've lost money or shared personal information.

- **Your Bank**

  Call immediately if you shared account information or sent money. They can help protect your accounts.

## Additional Support

**AARP Fraud Watch Network:** 1-877-908-3360 for support and resources

**Elder Justice Hotline:** 1-833-372-8311 for elder abuse concerns

**Social Security Fraud Hotline:** 1-800-269-0271

**Medicare Fraud Hotline:** 1-800-447-8477

Don't be embarrassed. Scammers are professionals at manipulation. Reporting helps law enforcement track and stop them.

# Cybersecurity Non-Profit (CSNP)

Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

## Our Programs—All Free

### Business & Non-Profit Security

### Family Cybersecurity

### Kids Safety

### Senior Digital Safety

### Women's Security

### Parents & Educators

---

**Visit us online:** csnp.org

**Free resources:** csnp.org/resources

Together, we can build a safer digital world for everyone. Stay informed, stay protected, and never hesitate to ask for help.