Phishing Email Safety Checklist

Before You Click or Reply - Check These Red Flags

Examine the Sender

- ▢ Look at the sender's email address carefully
- ▢ Verify it matches the official organization (e.g., @medicare.gov, not @medicare-update.com)
- ▢ Be suspicious of addresses using Gmail, Yahoo, or other personal email services for business
- ▢ Watch for random numbers or letters mixed into familiar company names

Read the Message Content

- ▢ Check if the email uses your actual name (not "Dear Customer" or "Account Holder")
- ▢ Look for urgent language like "IMMEDIATE ACTION REQUIRED" or "24 HOURS TO RESPOND"
- ▢ Notice excessive use of ALL CAPS or multiple exclamation points
- ▢ Be wary of threats about account closure or benefit suspension

Inspect Links and Attachments

- ▢ Hover over links without clicking to see where they really go
- ▢ Verify web addresses match the official organization's website
- ▢ Avoid clicking links that go to unfamiliar websites
- ▢ Never download unexpected attachments, especially .exe, .zip, or unknown file types

When You Receive a Suspicious Email

Immediate Actions

- ▢ Don't panic or feel pressured to act quickly
- ▢ Don't click any links or download any attachments
- ▢ Don't reply with personal information
- ▢ Take a screenshot or photo if you want to show someone later

Cyber Smart Seniors
Digital Guidance for Today's Seniors

Verification Steps

- ▢ Contact the organization directly using official phone numbers or websites
- ▢ Use contact information from your bills, cards, or trusted sources (not from the email)
- ▢ Log into your accounts through your usual method (bookmarks or typing the address)
- ▢ Ask a trusted family member or friend if you're unsure

Reporting and Cleanup

- ▢ Forward suspicious emails to spam@uce.gov (FTC)
- ▢ Delete the email from your inbox
- ▢ Delete the email from your trash/deleted items folder
- ▢ Mark similar emails as spam in your email program

If You Think You Made a Mistake

If You Clicked a Suspicious Link

- ▢ Close the website immediately
- ▢ Run a virus scan on your computer
- ▢ Change passwords for any accounts you think might be affected
- ▢ Monitor your bank and credit card statements closely
- ▢ Call your bank to report potential fraud

If You Shared Personal Information

- ▢ Contact your bank and credit card companies immediately
- ▢ Place a fraud alert on your credit reports
- ▢ File a complaint with the FTC at reportfraud.ftc.gov
- ▢ Change passwords for all important accounts
- ▢ Monitor all accounts for suspicious activity

Monthly Email Safety Review

Security Habits to Maintain

- ▢ Update your email software and antivirus programs
- ▢ Review and organize your email folders
- ▢ Clear out spam and junk mail folders
- ▢ Check that your trusted contacts list is current

Knowledge Updates

- ▢ Share what you've learned with friends and family
- ▢ Stay informed about new scam trends

Cyber Smart Seniors
Digital Guidance for Today's Seniors

Emergency Contact Information

Write your important phone numbers here:

Your Bank: _____

Credit Card Company: _____

Medicare: 1-800-MEDICARE (1-800-633-4227)

Social Security: 1-800-772-1213

FTC Fraud Hotline: 1-877-FTC-HELP

Trusted Family Member: _____

Quick Reminders

✓ When in doubt, don't click

✓ Verify through official channels

✓ Trust your instincts

✓ It's better to be safe than sorry

www.CyberSmartSeniors.com

Visit ***CyberSmartSeniors.com*** to access premium guides, personalized checklists, and expert podcasts for less than the cost of a cup of coffee each month!

Cyber Smart Seniors
Digital Guidance for Today's Seniors