CSNP
CYBERSECURITY NON-PROFIT

Email Safety Handbook

A friendly guide to staying safe and secure with email

FOR SENIORS 65+

CSNP

CHAPTER 1

Email Basics: A Quick Refresher

What Is Email?

Email is like sending a letter through your computer or phone. You write a message, add someone's email address, and click send. It arrives in seconds!

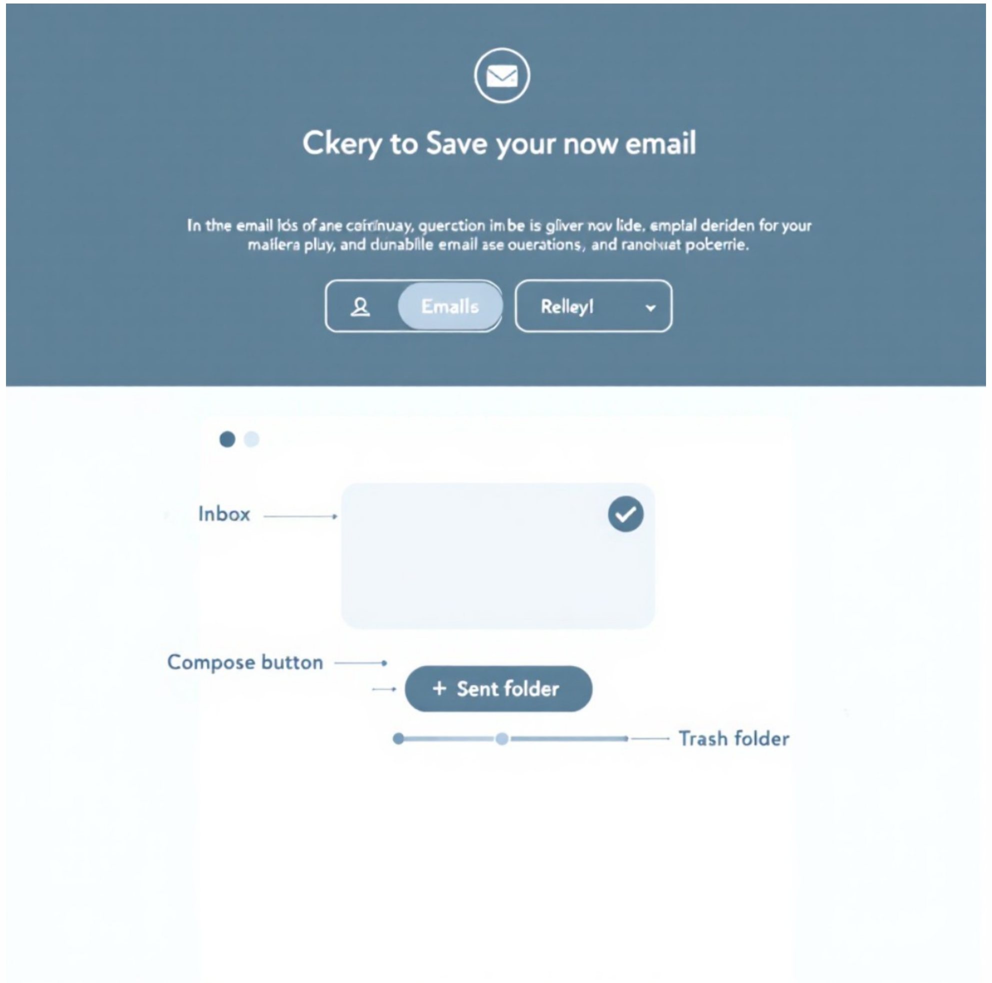
Key Parts of an Email

To: The person receiving your message

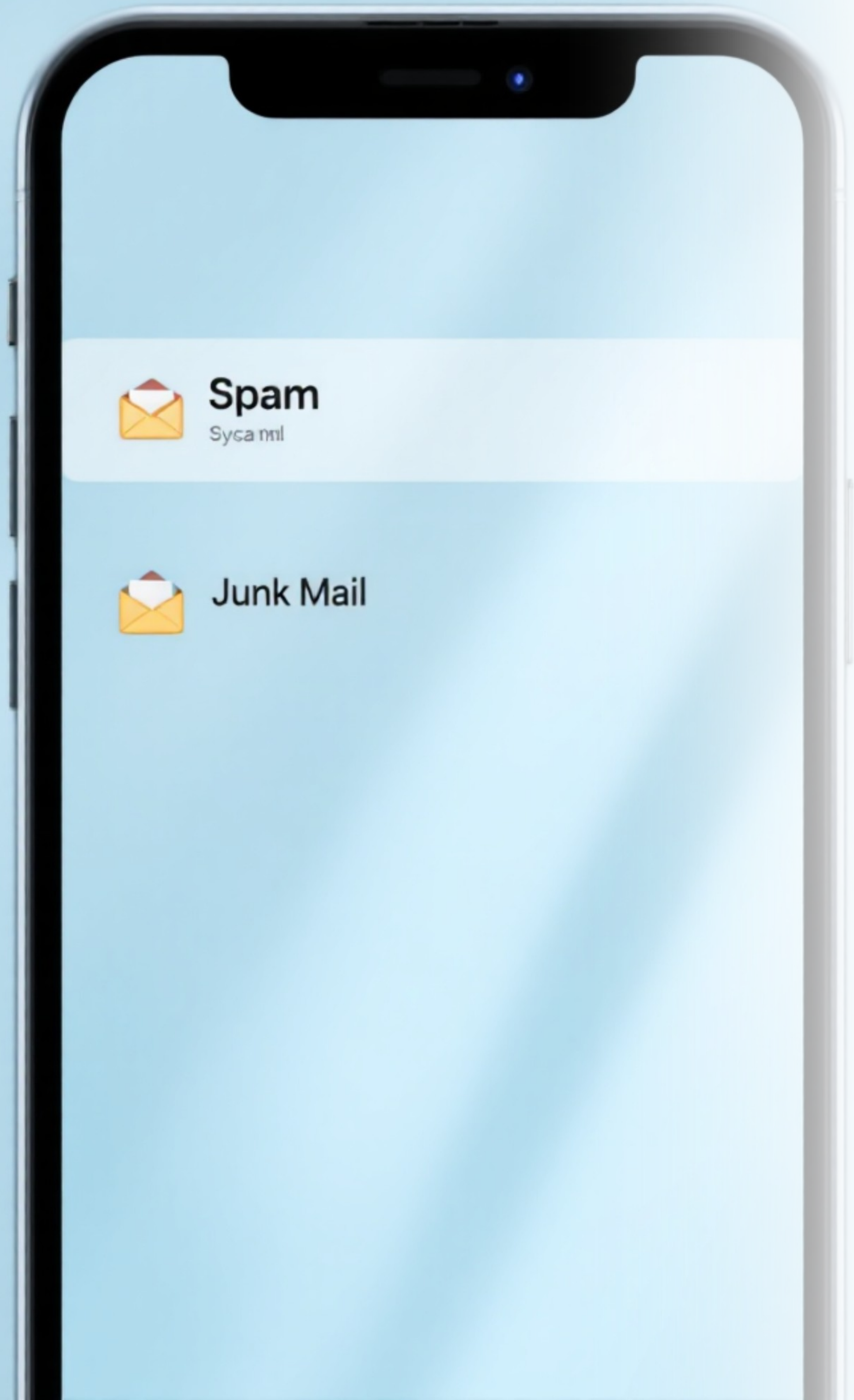
Subject: A brief description of your message

Body: Your actual message

Attachments: Files you can send along


Ckery to Save your now email
In the email lós of ane coirinuay, querction im be is gliver nov lide, emplal deriden for your mallera pluy, and dunabille email ase ouerations, and ranolwat poberrie.
Emalls
Relleyl
Inbox
Compose button
+ Sent folder
Trash folder

Remember: Take your time when reading and sending emails. There's no rush, and it's always okay to ask for help from a trusted family member or friend.



CHAPTER 2

Recognizing Spam and Junk Email

Spam emails are unwanted messages that clutter your inbox. Learning to spot them helps keep your email organized and safe.

What Spam Looks Like

- Messages from unknown senders
- Offers that seem too good to be true
- Requests for personal information
- Poor grammar or strange wording

What to Do

- Don't open emails from strangers
- Use your email's spam filter
- Delete suspicious messages immediately
- Never reply to spam emails

Stay Protected

- Mark spam emails as "junk"
- Don't share your email address publicly
- Use a separate email for online shopping
- Trust your instincts—if something feels wrong, it probably is

CHAPTER 3

Phishing Emails: The Dangerous Imposters

Phishing emails pretend to be from trusted companies or people to steal your personal information. They're like con artists in your inbox.

Warning Signs

- Urgent requests for passwords or account details
- Threats that your account will be closed
- Emails claiming you've won a prize
- Messages from "banks" you don't use
- Strange email addresses that don't match the company

How to Stay Safe

- Never click links in unexpected emails
- Call the company directly using a known number
- Check the sender's email address carefully
- Don't download attachments from strangers
- Remember: Real companies never ask for passwords by email

Golden Rule: When in doubt, don't click! If an email seems suspicious, delete it. Your bank, doctor, or other trusted organizations will never ask for sensitive information through email.

CHAPTER 4

Safe Links vs. Dangerous Links

Before You Click

Links in emails can take you to helpful websites or dangerous ones designed to steal your information. Here's how to tell the difference.

01

Hover Over the Link

Place your mouse over the link without clicking. The real web address will appear at the bottom of your screen.

02

Check the Address

Look for "https://" at the start and a lock symbol. Avoid links with misspellings or strange characters.

03

Type It Yourself

If you're unsure, open your browser and type the company's website address yourself instead of clicking the link.

Red Flags to Watch For

- Links that look like random letters and numbers
- Web addresses that are slightly misspelled (like "Amaz0n" instead of "Amazon")
- Links promising free gifts or prizes
- Shortened links (like bit.ly) from unknown senders

CHAPTER 5

Attachment Safety: What to Open and What to Avoid

Email attachments are files sent along with messages. While some are perfectly safe, others can contain viruses or harmful software.

1

Safe Attachments

- Files from people you know and trust
- Photos from family and friends (JPG, PNG)
- Documents you're expecting (PDF, DOC)
- Attachments you specifically asked for

2

Proceed with Caution

- Unexpected attachments, even from known senders
- Files with unusual names or extensions (.exe, .zip)
- Attachments that ask you to "enable macros"
- Files from contests or prizes you didn't enter

3

Best Practices

- Keep your antivirus software updated
- Scan attachments before opening them
- When in doubt, ask the sender if they sent it
- Delete suspicious attachments immediately

CHAPTER 6

Protecting Your Email Address

Your email address is like your home address—you want to be careful about who you share it with. Protecting it helps reduce spam and keeps you safer online.

1

Be Selective

Only share your email with trusted people and legitimate businesses. Think twice before signing up for newsletters or online accounts.

2

Create a Secondary Email

Consider having two email addresses—one for personal contacts and one for shopping or subscriptions.

3

Avoid Public Posting

Never post your email address on social media or public websites where scammers can easily find it.

4

Check Privacy Settings

Review who can see your email address in social media and other online accounts. Set it to private when possible.

Pro Tip: If a website or service seems untrustworthy, don't hesitate to walk away. You can always ask a family member or friend to help evaluate if a site is legitimate.

CHAPTER 7

Reporting Suspicious Emails

When you receive a suspicious email, reporting it helps protect not just you, but others too. Here's how to take action safely and effectively.

Use Your Email's Report Button

Most email providers (Gmail, Yahoo, Outlook) have a "Report Spam" or "Report Phishing" button. Click it to flag the message and help improve filtering.

Delete After Reporting

Once you've reported the email, delete it from your inbox and empty your trash folder to remove it completely.

Forward to Authorities

You can forward phishing emails to the Federal Trade Commission at spam@uce.gov or report them to the Anti-Phishing Working Group at reportphishing@apwg.org.

Tell the Impersonated Company

If the email pretends to be from a real company, contact them directly to let them know about the scam.

CHAPTER 8

Email Security Settings: Your Safety Toolkit

Taking a few minutes to adjust your email security settings can make a big difference in protecting your account and personal information.

Strong Passwords

Create a unique password with at least 12 characters, mixing letters, numbers, and symbols. Never use the same password for multiple accounts.

Two-Factor Authentication

Enable two-factor authentication (2FA) so you need both your password and a code sent to your phone to log in. This adds an extra layer of protection.

Spam Filters

Turn on your email's spam filtering feature to automatically catch suspicious messages before they reach your inbox.

Additional Security Tips

- Log out of your email when using shared or public computers
- Review account activity regularly for any unfamiliar sign-ins
- Keep your email software and apps updated
- Be cautious when accessing email on public Wi-Fi networks

About CSNP: Your Partner in Digital Safety

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

Our Free Programs for Everyone

- Business & Non-Profit Security
- Family Cybersecurity
- Kids Safety Online
- Senior Digital Safety
- Women's Security
- Parents & Educators

Visit us online: csnp.org

Access free resources: csnp.org/resources

Everything we offer is completely free. Our mission is to ensure everyone, regardless of age or technical experience, has access to the tools and knowledge needed to stay safe online.