Email Spam Safety Guide: Best practices for avoiding spam, blocking it, and staying safe.

Spam is annoying — but the bigger risk is **phishing** (emails that try to steal passwords, money, or personal info). These steps will cut down spam and help keep your account secure.

1) Know what "spam" vs "phishing" looks like

Spam usually:

- Tries to sell something, push ads, or get you to click.
- Comes from random senders you don't know.

Phishing/scams often:

- Pretend to be a bank, shipping company, "IT support," or even your email provider.
- Create urgency: "Account locked," "Payment failed," "Verify now."
- Ask you to click a link, open an attachment, or "confirm your password."

Rule: If an email asks for **passwords, codes, gift cards, wire transfers, crypto, or remote access** — it's a scam.

---

2) The #1 habit that stops most problems

Don't click links in unexpected emails.

If the email looks like it's from a company you use (bank, Amazon, PayPal, etc.):

- **Do not click the email link**
- Open your browser and go to the site **manually**, or use the official app.

---

3) What to do when you receive spam

Best actions (in order)

1. **Mark as Spam / Junk** in your email app
   This trains the filter and reduces future spam.
2. **Delete it**
3. **Do not reply**
   Replying confirms your address is active.
4. **Don't click "unsubscribe"** unless it's a sender you trust
   Real companies include legit unsubscribe links. Scammers sometimes use fake ones to confirm your address.

---

4) If you already clicked a link or opened an attachment

Don't panic — do this quickly:

1. If you entered your password: **change your email password immediately**
2. **Change passwords** anywhere you reused that same password (banking, shopping, social media)
3. Turn on **Two-Factor Authentication (2FA)** if available
4. Run a virus/malware scan on your device (Windows Security is fine; Mac can scan too)

***If you're unsure, contact our support team so we can help you assess what happened.**

---

5) Secure your email account (this matters)

Use a strong password

- Minimum **12–16 characters**
- Best is a **passphrase** (easy to remember, hard to guess):
  Example: River!Chair!Orange!48
- Never reuse the same password across sites

Enable Two-Factor Authentication (2FA), if your email app/provider supports it

This prevents most account takeovers even if a password is stolen.

---

6) Simple ways to reduce future spam

- Don't post your email address publicly (Facebook posts, marketplace listings, public websites)
- Activate a second "throwaway" email address for coupons, online forms, or sweepstakes
- Be careful with "free" offers, quizzes, and unknown sign-up forms
- Review what apps/websites have access to your email account and remove anything you don't recognize

---

7) Use your email app's built-in tools

Most email apps let you:

- **Block sender**
- **Create rules/filters** (example: send emails containing "crypto" or "investment" to Junk)
- **Safelist trusted senders** so important emails don't go to Junk

---

8) Red flags that should stop you immediately

Be suspicious if an email:

- Pressures you with urgency ("today only," "account will close")
- Has unexpected attachments (especially .zip, .exe, .html, macro-enabled Office files)
- Has spelling/grammar issues or weird formatting
- Uses a "from name" you recognize but the actual address looks wrong
- Asks you to buy gift cards, send money, or share codes

---

9) When to contact support

Reach out if:

- You're receiving **a sudden flood** of spam
- Your sent folder shows emails you didn't send
- Your password stops working unexpectedly
- Friends say they received strange emails "from you"
- You clicked something and you're not sure what it did