How to Spot a Scam Email in Under 10 Seconds

Your inbox should feel safe. Here's how to keep it that way.

Let's say you open your inbox and see something like this:

"Your account has been suspended — click here immediately!"
or
"You've won a $500 gift card!"

Before you click, take a breath.

Scam emails are everywhere these days, but the good news is: **you can spot most of them in under 10 seconds** once you know what to look for.

Let's walk through the simple signs.

---

1. Look at the sender's email address

Don't trust the name — check the actual email.

It might say:

From: "Apple Support"

But when you click or hover on it, the email is something like:

apple.support.1938zzx@gmail.com

If it's not from a real company domain (like @apple.com or @amazon.com), **it's a fake.**

---

2. Bad grammar or weird language

"You account have been suspended. Click now for regain access."

Yikes. **Real companies don't send emails like this.** If it sounds off, it probably is.

Trust your gut — if it reads like it was written by a robot or translated poorly, delete it.

Urgent threats or rewards

Scammers love to push you into action with messages like:

- "Your account will be closed in 24 hours!"
- "You've won something!"
- "We noticed suspicious activity — log in NOW!"

Urgency is a red flag.
Legit companies don't threaten you or pressure you like this in an email.

---

4. Strange links or attachments

Never click a link unless you're 100% sure it's safe.

Hover over the link (don't click!) and look at the bottom of your screen. If it goes somewhere strange like:

http://weirdsite.ru/verify-now — it's a scam.

If the email has a random attachment (like a .zip, .exe, or .pdf you weren't expecting), **do not open it**.

---

5. It's asking for personal info

Real companies will **never** ask for:

- Your password
- Your Social Security number
- Credit card info
- Login links inside the email

If they do — **it's a scam**.

Quick Checklist: 5-Second Scam Detector

Ask yourself:

- ✓ Do I recognize the sender's address?
- ✓ Does the email sound normal?
- ✓ Is it trying to scare or rush me?
- ✓ Does the link look weird?
- ✓ Is it asking for private info?

If you answer **yes** to any of those:
Delete the email. Do not click. Do not reply.

You're Smarter Than the Scammers

They're hoping you'll panic. But now?
You've got a cool head, a sharp eye, and a few simple tricks up your sleeve.

You're in control of your inbox again.