Understanding Scams and Fraud

🛡️ Tech Support Scams (and how to stay safe)

Scammers sometimes pretend to be “tech support” to scare people into paying money or giving access to a phone or computer.

Common examples you might see

- A pop-up that says you have a virus and tells you to call a number.
- A phone call saying your device is infected.
- A text message saying you must click a link to “fix” your device.

Red flags (warning signs)

- They **rush you** or create panic.
- They say **only they** can fix the problem.
- They ask for **payment right away**.
- They ask you to install an app for “remote help”.
- They ask for passwords, bank details, or gift cards.

What to do instead (safe steps)

1. **Do not call the number** on a pop-up, text, or email.
2. **Do not click links** you were not expecting.
3. If you cannot close a pop-up:
    - Close your browser.
    - If needed, restart the device.
4. **Call someone you trust** or contact your usual support.

✅ Quick safety rules

- **Never pay with gift cards** for tech support.
- **Never share one-time codes** (codes sent by text or email).
- If it feels urgent or scary, **pause** and ask a trusted person.

If you think you were scammed

- Stop talking to the person.
- Take a screenshot if you can.
- Tell a family member or trusted friend.
- Contact your bank or card company if you shared payment info.

💡 How to spot a scam (email or phone)

If someone pressures you to act fast, send money, or share personal information, **stop and check first**. Real companies, banks, and government offices will not rush you or threaten you.

🧠 Is it real or is it a scam? (5 quick checks)

If you are not sure, look for these 5 clues.

1) **Emotional language**

- It tries to scare you or rush you.
- It says you must act “right now”.

2) **Sender’s contact info**

- The email address looks strange.
- The phone number is unfamiliar.
- The caller will not let you hang up and call back.

3) **Weird links or QR codes**

- It asks you to click a link, scan a QR code, or download something.
- If you did not expect it, do not click.

4) **Awkward language or typos**

- The writing feels unnatural.
- The message has odd grammar or spelling.

5) **Brand details that feel “off”**

- The logo, colors, or formatting looks slightly wrong.
- The message does not match what you usually receive from that company.

Example to watch for: `support@paypaI.com` (the “l” can be a capital “i”).

Common warning signs (expanded)

- **Urgency or fear** (“Act immediately”, “Your account will be closed today”).
- **Unusual payment requests** (gift cards, wire transfers, cryptocurrency, payment apps).

- **Requests for personal information** (Social Security number, Medicare number, bank details, passwords, one-time codes).
- **Strange email or phone behavior** (misspellings, weird addresses, refusing to let you hang up and call back).

Phone scam tricks

Scammers may pretend to be the IRS, Medicare, Social Security, your bank, a relative, or tech support.

What to do

1. Hang up.
2. Look up the official number yourself.
3. Call back directly.

Email scam tricks

Watch for messages that push you to click a link, open an attachment, or “verify” something.

Safe practice

- Do not click links in unexpected emails.
- Open your browser and type the company website yourself.

The “grandparent” emergency scam

If someone claims a family member is in trouble and asks for secrecy or immediate money:

- Call the family member directly.
- Call another relative to confirm.

If you are unsure

Pause and ask someone you trust.

- A family member or friend
- Your bank

- Local police non-emergency number

If you already sent money

Act quickly.

1. Call your bank or credit card company.
2. Report it at **reportfraud.ftc.gov**.
3. Tell family so they can watch for more attempts.

✅ Quick safety checklist

Before responding, ask:

- Did they rush me?
- Did they ask for secrecy?
- Did they ask for unusual payment?
- Did they ask for personal information?

If yes to any, it is very likely a scam.

A personal message from me

🌿 You are not “bad with tech”. Scammers are simply very good at creating stress and confusion.

If something feels urgent or scary, that is your signal to **pause**. You do not have to decide in the moment.

Here is the rule I want you to remember: **stop, breathe, and verify**.

It is always okay to hang up, close the pop-up, and call a trusted person.

You are allowed to take your time.

You have more control than you think, and with a few simple habits, you can stay safe.

— Molham