DON'T BE A NAIL!

Sniff Before You Scan

If it smells off, it probably is. Avoid scanning QR codes or clicking links from suspicious sources.
Call trusted numbers—not the one in a shady message.

Pause Like a Possum

Urgency is a scammer's favorite tool.
Take a breath. Read carefully. Think critically.
Scammers want you to rush.

Stop, Think, Verify the Tale

Before you click, stop and evaluate. If a message seems urgent, flashy, or too good to be true, it probably is. Look for signs of phishing—spelling errors, odd requests, emotional manipulation.

Check the Sender, Check the URL

Scammers often disguise links and emails. Hover over links before clicking and inspect email addresses carefully. Use known websites or apps instead of clicking unknown links.

Keep Your Codes Secret, Use MFA

Never share verification codes. Ever.
Use Multi-Factor Authentication (MFA) to protect your accounts—it's your safety rail.

Resources:

- cisa.gov/shields-up
- cyberhouserock.info
- cisa.gov/topics/cybersecurity-best-practices