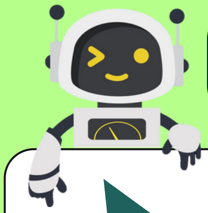

CHUCK THE SNEAKY CHAMELEON

Pause Before You Click

If you receive a link—especially from an unexpected or unusual message—don't click it right away. Hover over it to preview the URL, and check if it looks legitimate. When in doubt, go directly to the official website.

Verify the Sender

Scammers impersonate people you trust. Always double-check the sender's email or phone number. If something feels off—call or message the real person through a trusted channel.

Don't Panic

Scammers create urgency to make you act fast without thinking. Slow down. Real requests from real people can wait a moment while you verify.

Use MFA

Enable MFA (multi-factor authentication) on all your important accounts (email, banking, social media). Even if a scammer gets your password, MFA adds a second layer of protection.

Check First

Just because a message looks official or a name is familiar doesn't mean it's safe. Look for red flags like bad grammar, vague requests, and sketchy links. When in doubt, check through a separate channel.

Resources:

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