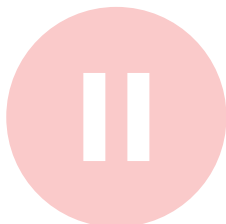


# PAUSE LIKE A POSSUM



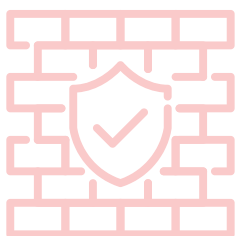
## Don't Click

If a message or link seems “off” or comes from an unknown sender, don't click it. Fake shipping notices and mystery texts are classic phishing tactics.



## Pause

Scammers often create urgency—“Act now!” or “Your account's been hacked!” Take a moment. Breathe. Real organizations don't rush you.



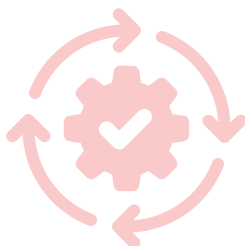
## Verify

If something seems important—like a bank alert or delivery issue—check the source yourself. Go directly to the app or official website rather than following a link in the message.



## Keep it Close

Never give out passwords, verification codes, or personal details via text or email—especially if you didn't initiate the conversation.



## Use Tools

Install antivirus software, keep your devices updated, and use multi-factor authentication. That way, even if you slip, your digital “burrow” stays protected.

## Resources:

- [cisa.gov/shields-up](https://cisa.gov/shields-up)
- [cyberhouserock.info](https://cyberhouserock.info)
- [cisa.gov/topics/cybersecurity-best-practices](https://cisa.gov/topics/cybersecurity-best-practices)

