



SOCIAL ENGINEERING TACTICS, TECHNIQUES AND DEFENSES



Presented by: Lily Lee, Splunk

SOCIAL ENGINEERING DEFINITION

so·cial en·gi·neer·ing
/ ,sōSH(ə)l ,enjə'niriNG/

the use of **deception** to **manipulate** individuals into divulging **confidential or personal information** that may be used for **fraudulent purposes** .

FAST FACTS: WHY IT MATTERS



Social engineering attacks are rising and the leading cyber attack vector.



No one is immune to social engineering attacks because they target human emotions, not intelligence.



Successful social engineering attacks can lead to data breaches, financial losses, reputational damage, and more.



Individuals aged 18 to 35 are more susceptible to phishing than other age groups.^[1]

[1] Get Cyber Safe, National Cybersecurity Alliance, & CybSafe. (2024). Oh, Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2024-2025 (p. 43).

SOCIAL ENGINEERING MYTHS

SOCIAL ENGINEERING MYTHS



“Social engineering only involves phishing.”

COMMON SOCIAL ENGINEERING METHODS

Technology-based

Phishing (email, SMS, website, Wi-Fi or “evil twin”, spear phishing, whaling, watering hole, angler, QR code)

Typo squatting / URL hijacking

Deepfakes

Baiting

Pretexting

Pop-up applications

Pharming

Scareware

Human-based

Vishing (voice phishing)

Impersonation (CEO fraud, supply chain compromise)

Physical breaches (piggybacking, tailgating)

Shoulder surfing

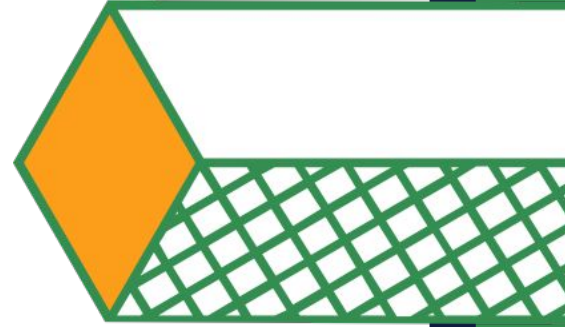
Dumpster diving

Quid pro quo

Diversion theft

Reverse social engineering

SOCIAL ENGINEERING MYTHS

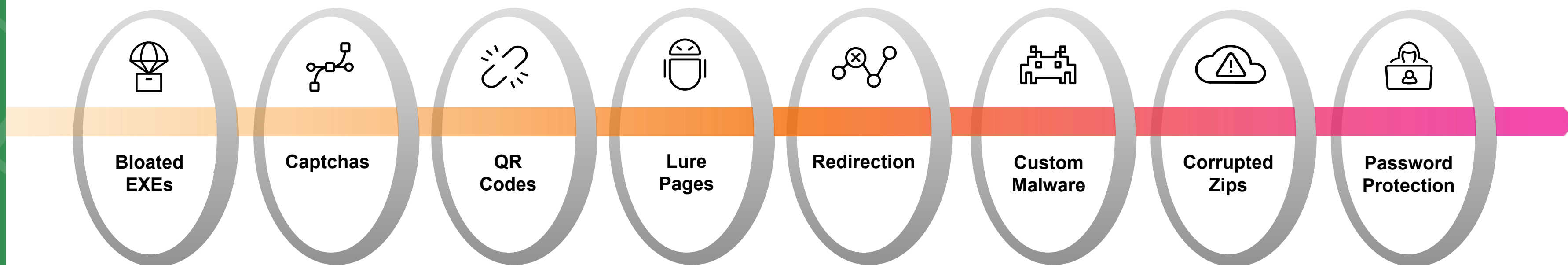


“Social engineering only involves phishing.”



“Our security technologies will protect us.”

WHY DO SOME THREATS GET THROUGH TRADITIONAL SECURITY TOOLS?



SOCIAL ENGINEERING MYTHS



“Social engineering only involves phishing.”

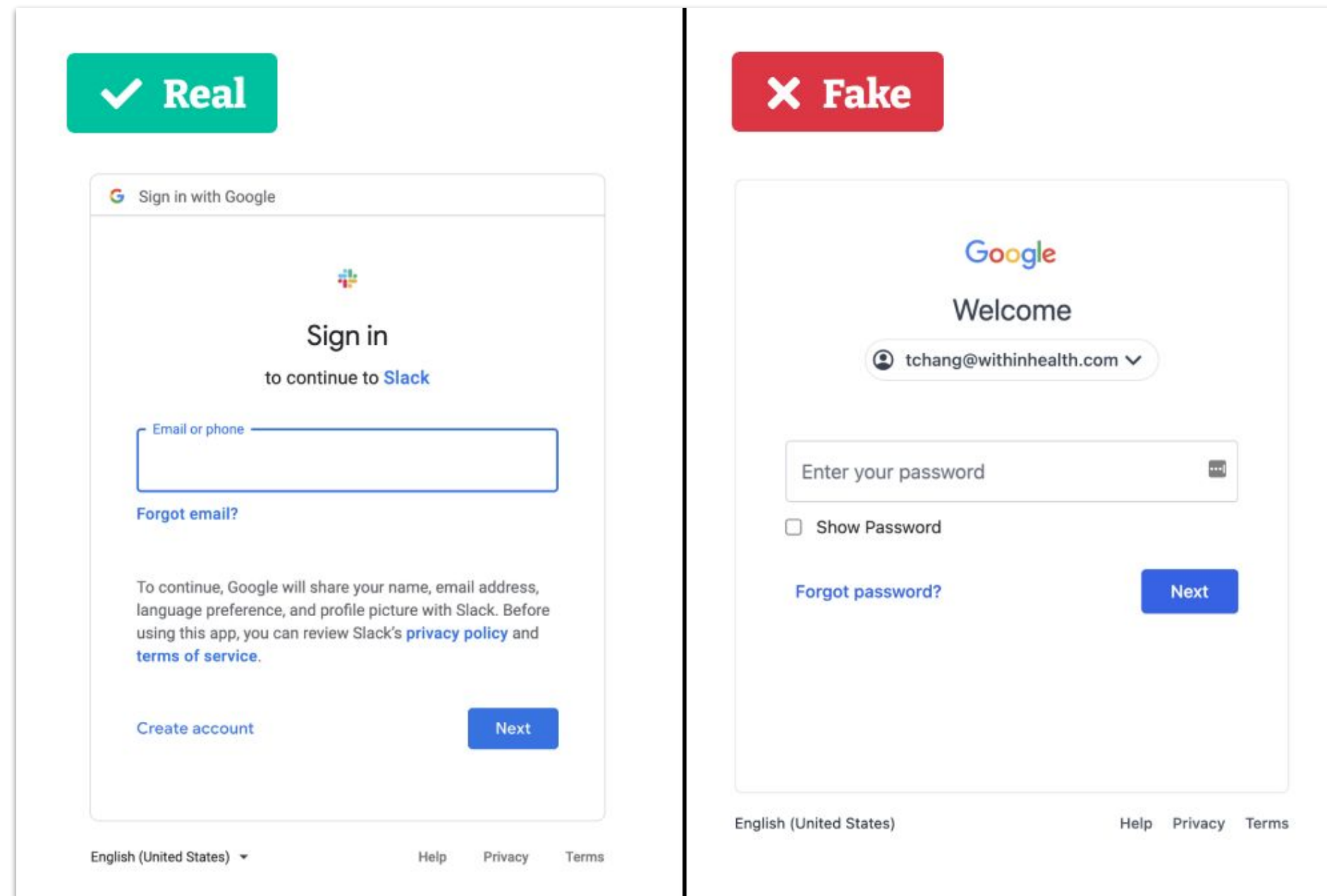


“Our security technologies will protect us.”



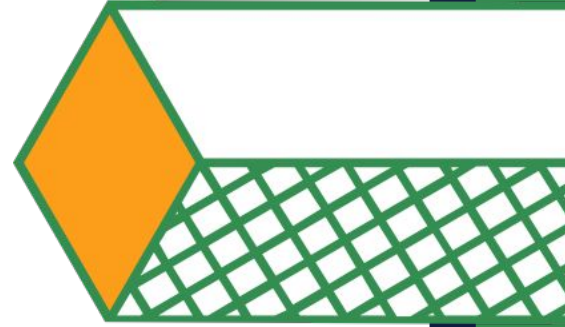
“Fake emails and logins are easily spotted.”

WHICH IS THE FAKE?



Source: <https://www.verified.org/articles/scams/slack-email-verification-scam>

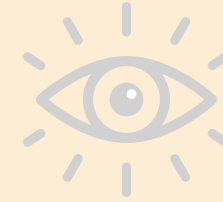
SOCIAL ENGINEERING MYTHS



“Social engineering only involves phishing.”



“Our security technologies will protect us.”



“Fake emails are easily spotted.”



“No one would want to target me/us.”



EVERYONE IS A POTENTIAL TARGET

COMMON SCHEMES: TARGETING STUDENTS



Gift card & Venmo scams



Unsolicited scholarship & grants



Fake internship, research & employment offers



Fake listings for apartments, used books, movers



Student loan debt relief scams



Essay & resume editing services

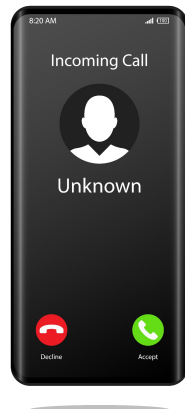


Tech issue

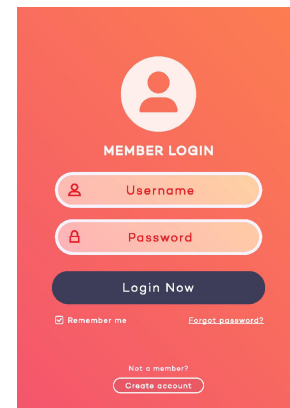


Social media scams

COMMON SCHEMES: TARGETING FACULTY



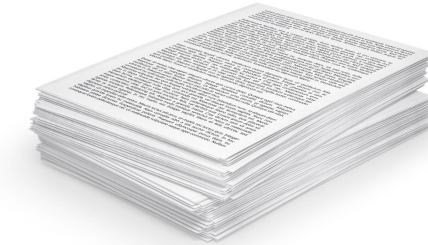
Pretexting calls



Fake conference registration



Tailgating



Malicious links
in research
collaborations



Tech issue

**PRACTICE
MAKES
PROGRESS**

SOCIAL ENGINEERING

RED FLAGS

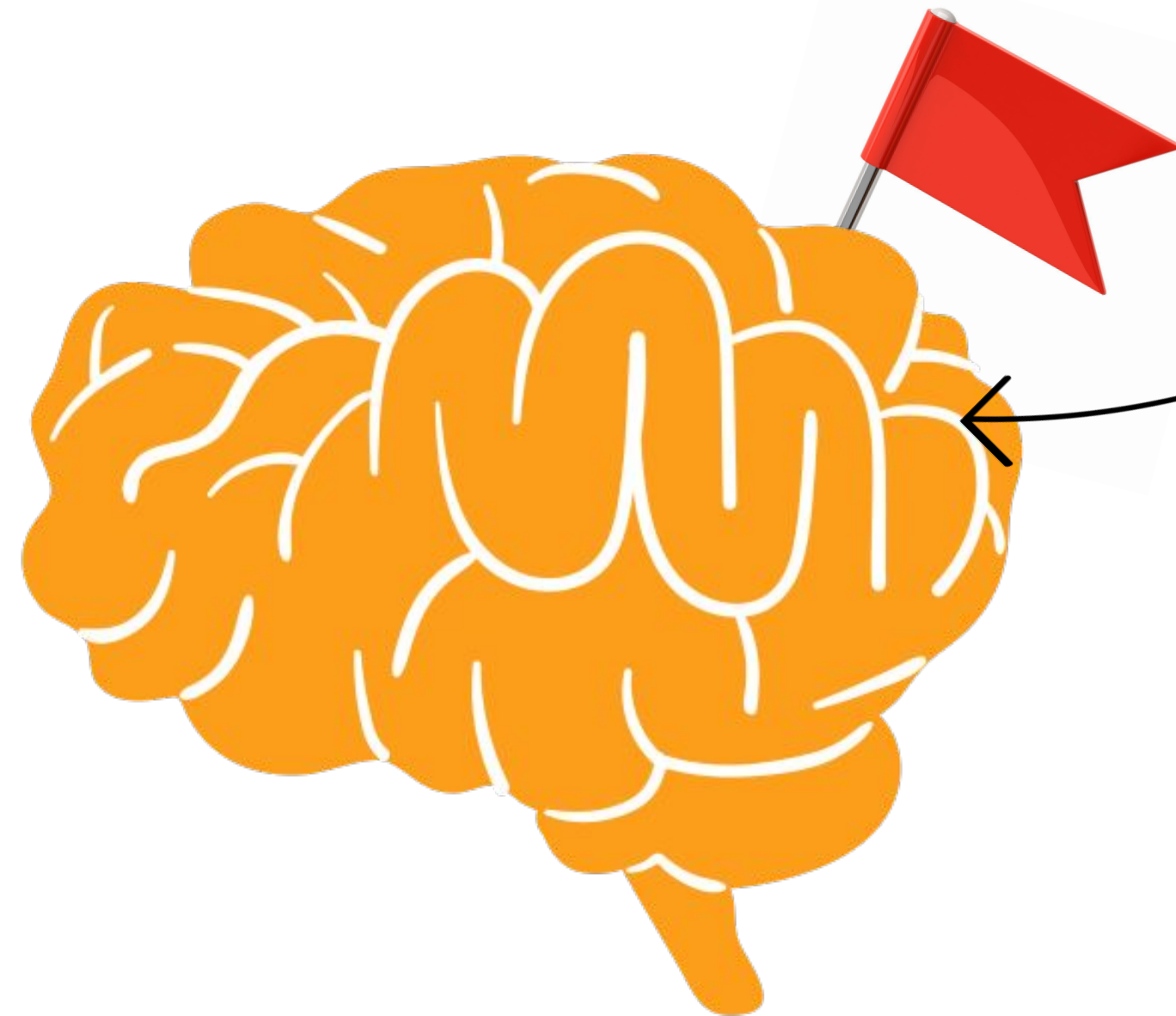
SOCIAL ENGINEERING RED FLAGS

Posing as a legitimate source

- Your "friend"
- Your "boss"
- Your "professor"
- Your "bank"
- The "IT department"



SOCIAL ENGINEERING RED FLAGS



Emotional manipulation

- Fear
- Excitement
- Curiosity
- Guilt
- Grief
- Anger

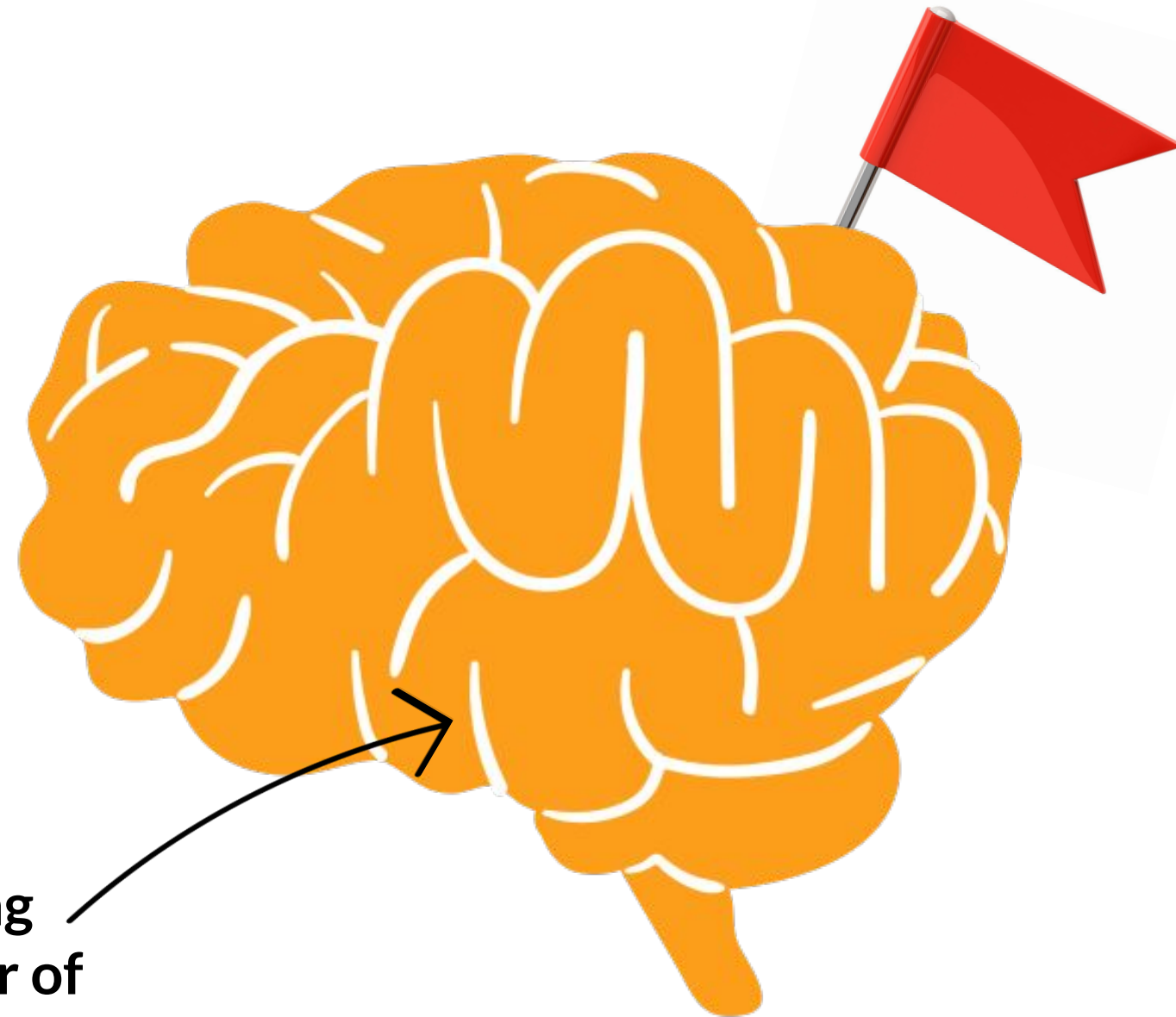
SOCIAL ENGINEERING RED FLAGS



Sense of
urgency to
pressure action

- Act immediately
- Call now
- Urgent
- Pay today
- Respond within 48 hours

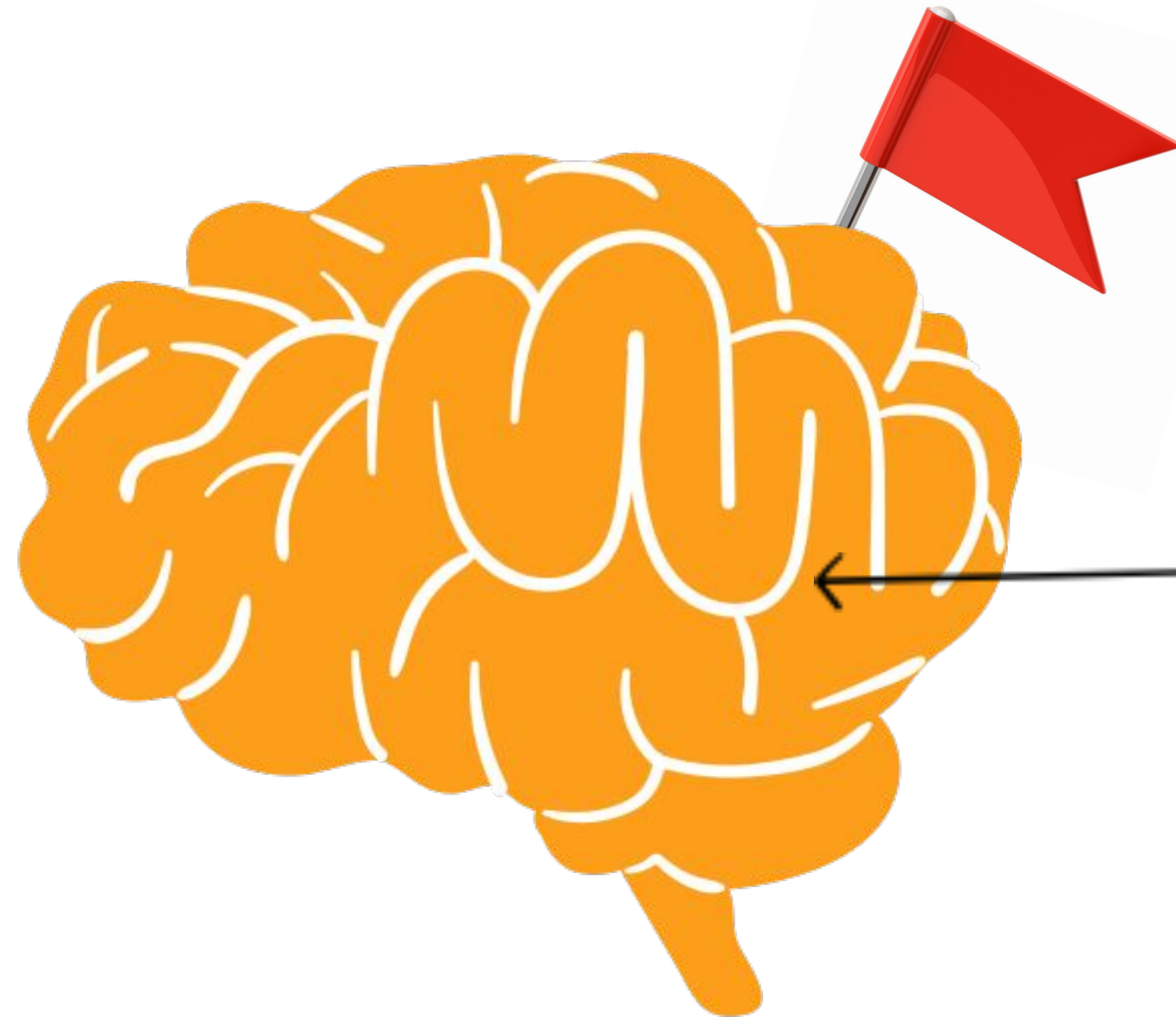
SOCIAL ENGINEERING RED FLAGS



- Free trial
- Limited-time offer
- Expires today
- Flash deal
- Special access
- Guaranteed results

Tempting
offer / fear of
missing out

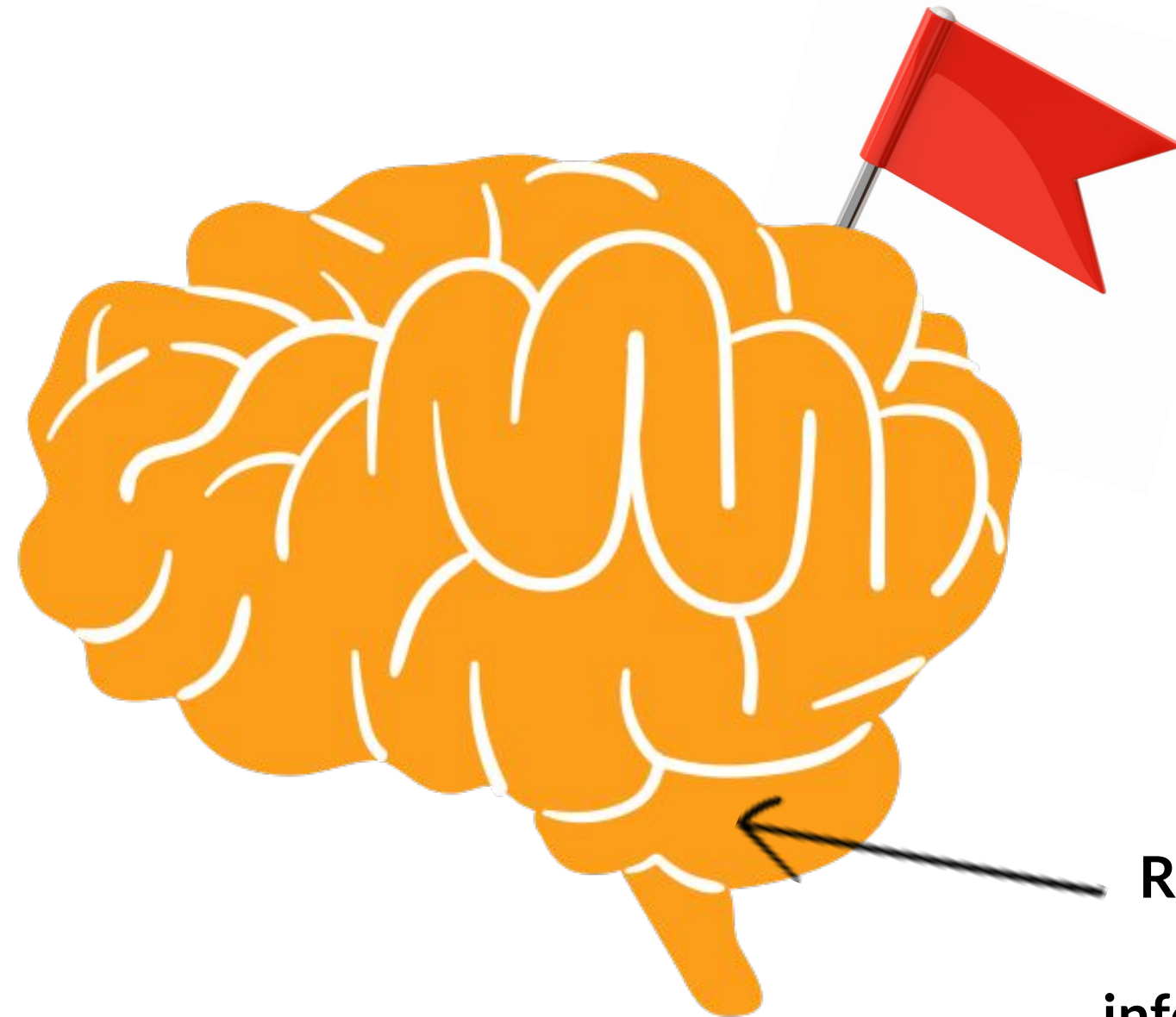
SOCIAL ENGINEERING RED FLAGS



Unexpected /
unsolicited request
or communication

- Help you didn't ask for
- Unusual request for money or assistance
- Unexpected email
- Unexpected phone call

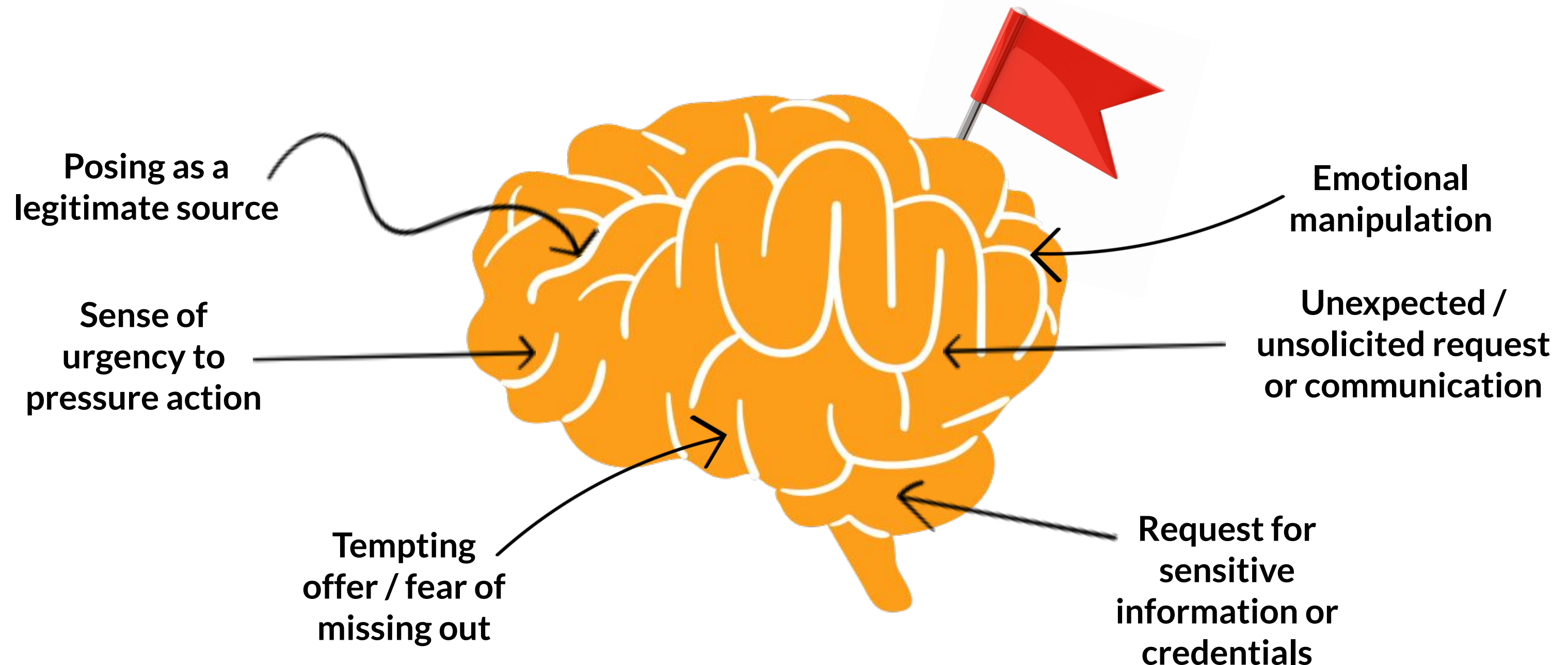
SOCIAL ENGINEERING RED FLAGS



Request for sensitive information or credentials

- Payment
- Upfront fees
- Login
- Personal details

SOCIAL ENGINEERING RED FLAGS



CAN YOU SPOT ALL OF RED FLAGS?

Payment Declined -- Update Required Immediately!


From: **ApplePay Support** <customer_support_ref_@apple.com>

Dear Apple User,

It has come to our attention that you're recent payment was declined. An update is required immediately..

To make this change, visit the support section at the link below.

<https://www.applepay.com/subscriptions/payment-update>


 <http://944.535.32/index/apple.html>

If you do not update your payment information in the next 24 hours, your account will be deactivated.

Regards
ApplePay Support

—

Copyright © 2012 Apple Inc.
All rights reserved
3 Loop, Madisonville KY 42001

 [apple-invoice.zip](#) [Download](#)

Source: <https://www.varonis.com/blog/spot-phishing-scam>

CAN YOU SPOT ALL OF RED FLAGS?

1. Sense of urgency using intense language, scare tactics
2. Imitating recognized brand using fake email address
3. Generic and impersonal greeting
4. Unprofessional communication with typos
5. Rolling over the link shows a malicious address
6. Sense of urgency using intense language, scare tactics
7. Generic and impersonal signature
8. Outdated copyright and incorrect address of the business
9. Malicious attachment

1 Payment Declined -- Update Required Immediately!

2 From: **ApplePay Support** <customer_support_ref_@apple.com>

3 Dear Apple User,

4 It has come to our attention that you're recent payment was declined. An update is required immediately..


To make this change, visit the support section at the link below.

5 <https://www.applepay.com/subscriptions/payment-update>
<http://944.535.32/index/apple.html>

6 **If you do not update your payment information in the next 24 hours, your account will be deactivated.**

7 Regards
ApplePay Support

8 Copyright © 2012 Apple Inc.
All rights reserved
3 Loop, Madisonville KY 42001

9  apple-invoice.zip [Download](#)

Source: <https://www.varonis.com/blog/spot-phishing-scam>

SIMPLE STEPS *YOU* CAN TAKE

01

Keep your operating system and applications up to date

02

Stay vigilant of your surroundings

03

Verify the source

04

Be cautious with links, downloads and attachments

05

Be skeptical of unexpected requests and tempting offers

06

Take a moment to think and ask questions

07

Log into your account via official website

08

Use passphrases and multi-factor authentication

09

Educate yourself and pay it forward

COMMON SOCIAL ENGINEERING METHODS

Technology-based

Phishing (email, SMS, website, Wi-Fi or “evil twin”, spear phishing, whaling, watering hole, angler, QR code)

Typosquatting / URL hijacking

Deepfakes

Baiting

Pretexting

Pop-up applications

Pharming

Scareware

Human-based

Vishing (voice phishing)

Impersonation (CEO fraud, supply chain compromise)

Physical breaches (piggybacking, tailgating)

Shoulder surfing

Dumpster diving

Quid pro quo

Diversion theft

Reverse social engineering

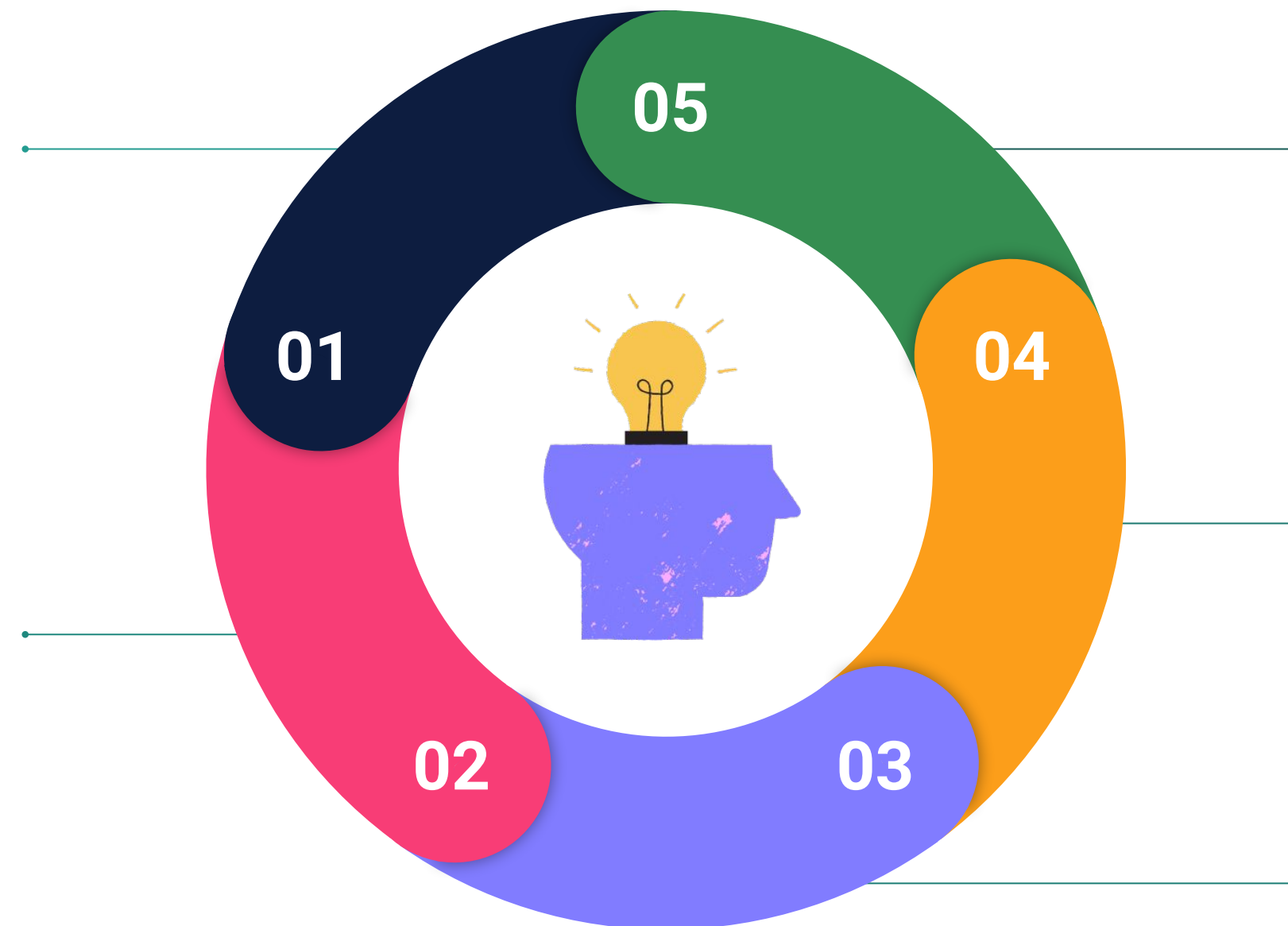
IT TAKES A VILLAGE

Collaborate

By marshaling all the populations of a university — administrators, faculty and students — you can create a large and diverse cybersecurity team.

Communicate

Connect and communicate through a variety of formats and media (e.g., posters, videos, social media, email, student portals, in-person events).



Listen & Practice Empathy

Students are often the first to hear about new methods of social engineering, so their input can be invaluable for educating the rest of the university population.

Empower

Provide everyone with the tools (e.g., **Phishbowl** and **phishing.report@unh.edu**) they need to be part of your security framework and establish an ongoing partnership for engagement, feedback, and building a culture of cybersecurity awareness.

Motivate

Set the right tone and gamify the learning/training process to keep everyone engaged as a key part of your cybersecurity defense.

<https://business.bofa.com/en-us/content/cybersecurity-for-students.html>

https://csrc.nist.gov/csrf/media/Projects/usable-cybersecurity/documents/Final_Proof_Users_are_not_stupid.pdf

THANK YOU