
aka People Hacking

SOCIAL ENGINEERING

WHITE HAT

Jaxon Haws

CPSEC

ABOUT ME

- **2nd Year Computer Science**
- **Clubs:**
 - **White Hat: Archivist -> President**
 - **CPLUG: Treasurer -> President**
- **Finished my first racing season**



TABLE OF CONTENTS

- **What is social engineering?**
 - **Why is social engineering effective?**
 - **Types of Social Engineering attacks**
 - **Where/when has social engineering been used?**
 - **How can you prevent social engineering attacks?**
-

**DISCLAIMER: DON'T TRY ANY OF THIS AT
HOME, WORK, PUBLIC, ETC WITHOUT
CONSENT OF INDIVIDUALS INVOLVED**

WHAT IS SOCIAL ENGINEERING?

- Methods employed by hackers to gain the trust of an end user so that the hacker can obtain information that can be used to access data or systems.
 - Typically involves impersonating representatives of legitimate organizations to manipulate people into supplying sensitive information or access to restricted areas.
-

TYPES OF SOCIAL ENGINEERING ATTACKS

- Digital interactions
- Physical interactions

(PH)-ISHING

- **Phishing:** a type of social engineering attack that uses email to entice a user to click on a malicious link from a legitimate appearing source.
 - **When the user selects the ill-intentioned link, the user's device or system becomes infected with malware and data is often compromised.**
 - **Spear Phishing/Whaling:** a variation of phishing wherein a specific individual is targeted
-

JOB OUTREACH FOR SELECTED COLLEGE/UNIVERSITY STUDENT

1 ▾



Dr Jimmy Chandler <jayshapy0082019@gmail.com>

Sun 9/22/2019 5:46 AM

To: Elle Jax Harlow; Jane Xiao; Jax Ann Garrett; Jaxon Payne Haws; Jaxon Seltzer Green; jimchan008@gmail.com



Read Carefully.txt

3 KB

Read Attached

[Reply](#)

[Reply all](#)

[Forward](#)

Intern Offer



Ani Michelle Svadjian

Tue 8/27/2019 7:58 AM



Hello,

I will like to refer you to a part-time customer assessment job, You will be **paid** between \$300 for every assessment. Kindly [click here](#) for more details and how to apply.

Note: This job can be very exciting, For those who love to shop it's the perfect job that offers fun assignments and flexible schedules. Your contribution will bring improvement to customer services within your area.

Regards,
A. Svadjian

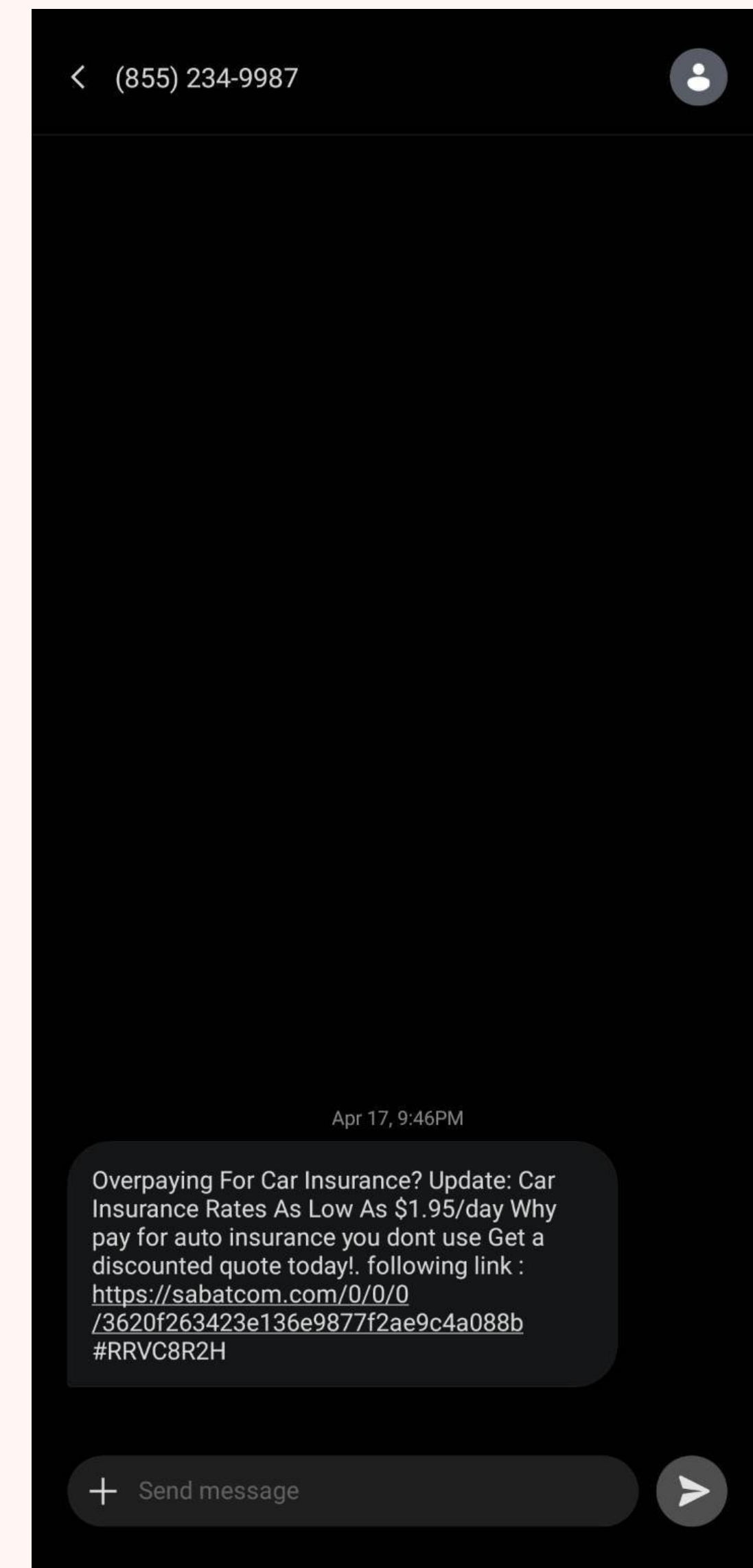
[Reply](#)

[Reply all](#)

[Forward](#)

(SMS)-SHING

- Look out for suspicious links
- Be wary of anyone who isn't in your contacts
- Don't click the links



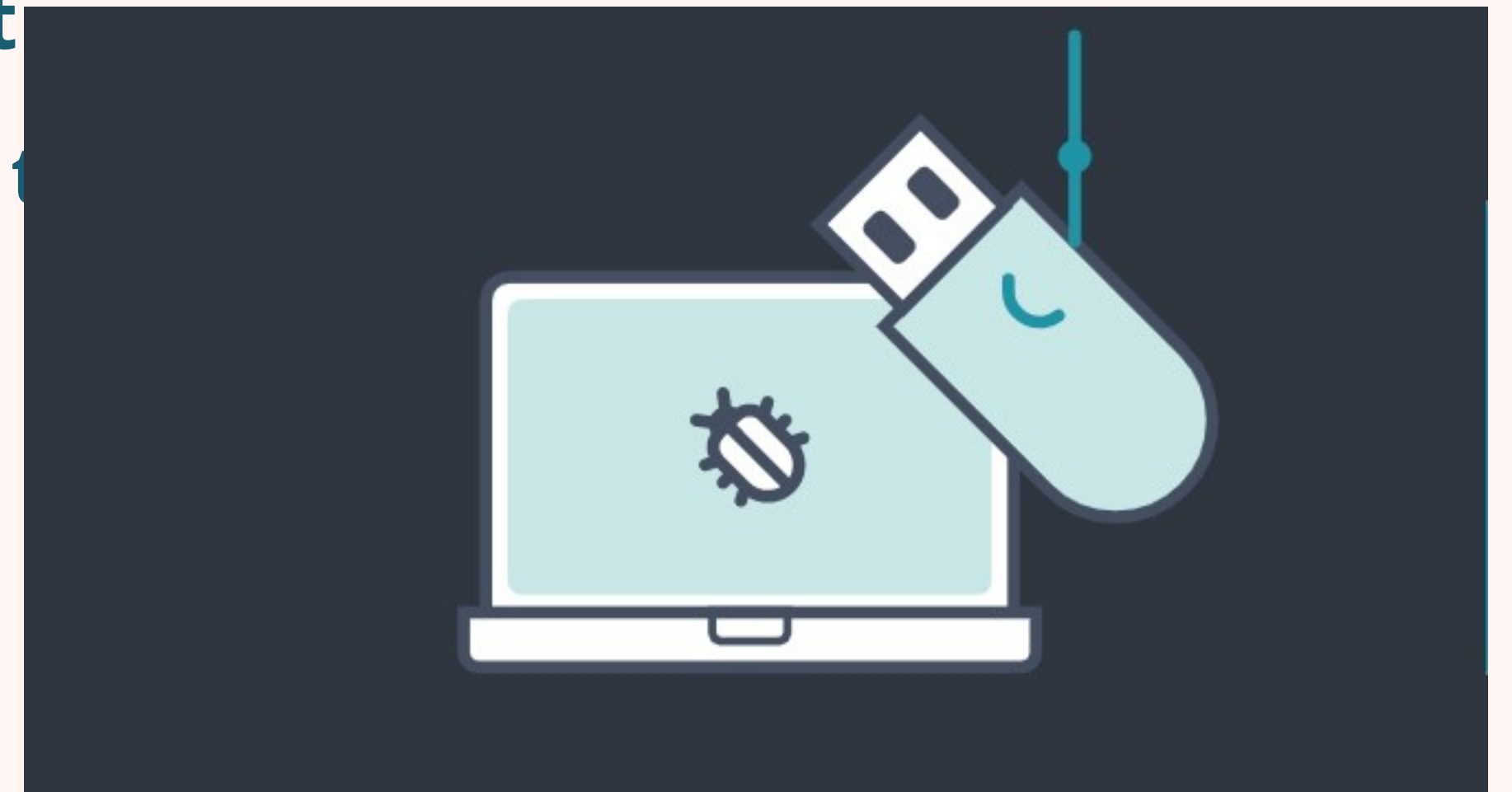
(VI)-SHING

- Usually an automated voice system that calls you with an urgent problem that requires sensitive information
- Spoofed phone number so you can't call back
- Can be about: banking errors, social security number frozen, Windows has encountered problems, your warranty is about to expire, etc



BAITING

- A social engineering attack where an attacker entices a user with a free item to lure them into clicking on a link.
- This may come in the form of a free music or movie download lined up with the user's interests.
- Can also be in the form of a 'lost' USB drive that gets unwittingly plugged into a machine to spread malware.



QUID PRO QUO

- **Quid Pro Quo: “something for something” social engineering technique, the quid pro quo attack involves promising a service or benefit for complying with the request of an attacker.**
- **For example, a social engineer may promise a free software upgrade to entice a user to download what is actually malware to their system**

PRETEXTING

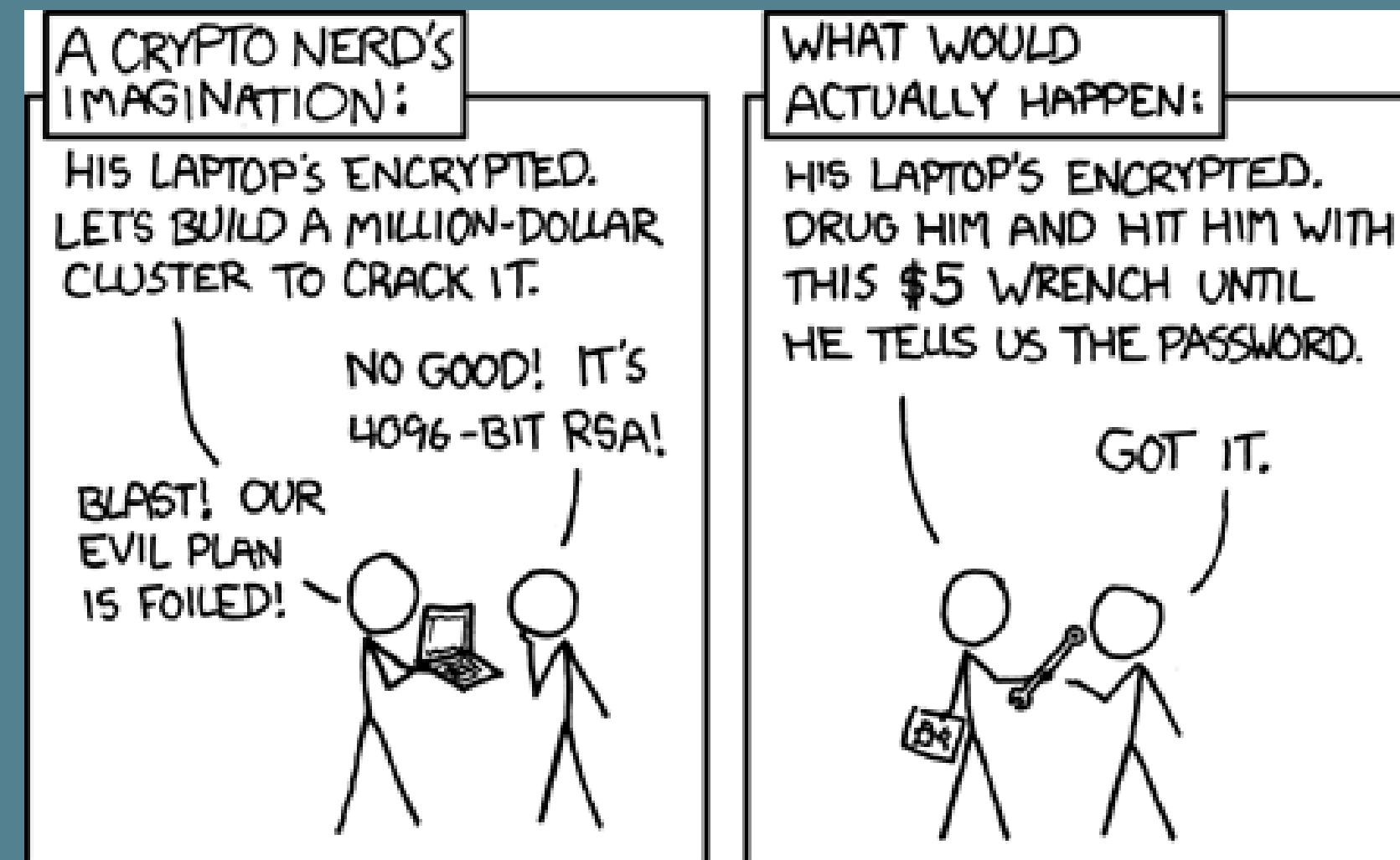
- **Pretexting:** With pretexting, an individual impersonates a representative from a trusted organization with the goal of acquiring sensitive information.
 - This social engineering technique relies heavily on gathering research before initiating contact with the target.
 - For example, a network admin/ IT person coming to speed up the internet
-

TAILGATING

- **Tailgating: when a person gains access to restricted areas by following an approved employee into the area and piggybacking on their credentials.**
- **This social engineering tactic is a physical attack.**
- **In these cases, the social engineer often pretends to be an employee or even a delivery person.**



WHY IS SOCIAL ENGINEERING EFFECTIVE?



WHY DOES THIS WORK?

- **Fear**
 - **Greed**
 - **Curiosity**
 - **Helpfulness**
 - **Urgency**
-

THIS HASN'T ACTUALLY HAPPENED IN THE REAL WORLD RIGHT?



HIGH-VIZ VEST

- Wearing a high-viz vest gives off an impression of authority
- Additional props such as radios, clipboards, lanyards, etc can increase authority
- Walking through exits surprisingly works



2013 TARGET DATA BREACH

- In 2013, more than 110 million customers fell victim to a social engineering attack on Target.
- Social engineering techniques were used on an HVAC company that had remote access to Target's network.
- The HVAC company was then compromised with malware, which in turn infected Target's systems.
- The attack resulted in the loss of emails, names, addresses, phone numbers and credit and debit card information.





KANE GAMBLE

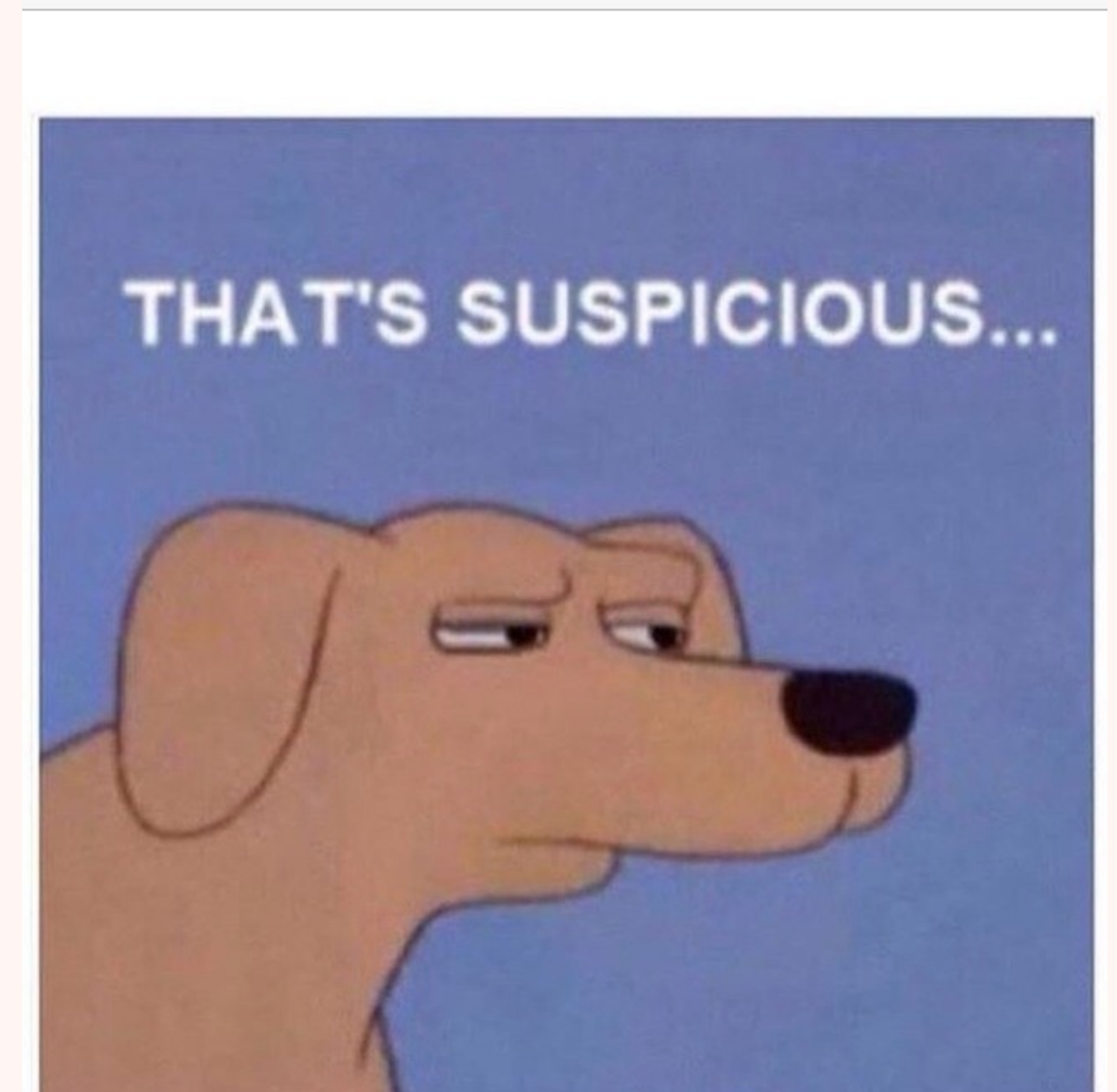
- A 15-year-old was able to take control of the secure emails of John Brennan, the director of the CIA.
- Kane Gamble used social engineering to convince Verizon to provide personal details about Brennan, which he later used to impersonate the CIA director.
- Gamble was able to access Brennan's email by changing security questions and passwords with gathered intel, allowing the 15-year-old to view sensitive military information.



HOW CAN YOU PREVENT SOCIAL ENGINEERING ATTACKS?

PREVENTING DIGITAL SOCIAL ENGINEERING ATTACKS

- Don't click on suspicious links
- Don't give out information over the phone if you didn't call them
- Don't plug in random devices that you find



PREVENTING IN PERSON SOCIAL ENGINEERING ATTACKS

- **Don't let random people into restricted areas**
- **Verify ID badges**
- **Ask questions and don't turn a blind eye**
- **In the workplace, conduct trainings**



QUESTIONS?

SOURCES

- <https://www.comptia.org/content/articles/what-is-social-engineering>
 - <https://terrannovasecurity.com/examples-of-social-engineering-attacks/>
 - https://en.wikipedia.org/wiki/Social_engineering_%28security%29
 - <https://youtu.be/dQw4w9WgXcQ>
 - <https://youtu.be/GyvRamX1VyA>
 - <https://youtu.be/tCRT3QFzwm8>
-