GRACE HOPPER CELEBRATION

ANITA B.ORG

Social Engineering for Fun and Profit - The Power of Persuasion

#GHC19

Social Engineering for Fun and Profit

The Power of Persuasion in Cyber Red Teams

Social Engineering is the art of exploiting human trust to achieve a malicious objective and one of the most effective attack methods for delivering malware.

Based on tried and tested offensive cybersecurity exercises, this presentation aims to build an ontology of the applied social engineering tactics by explaining their practicality in modern cybersecurity breaches and the lessons learned.

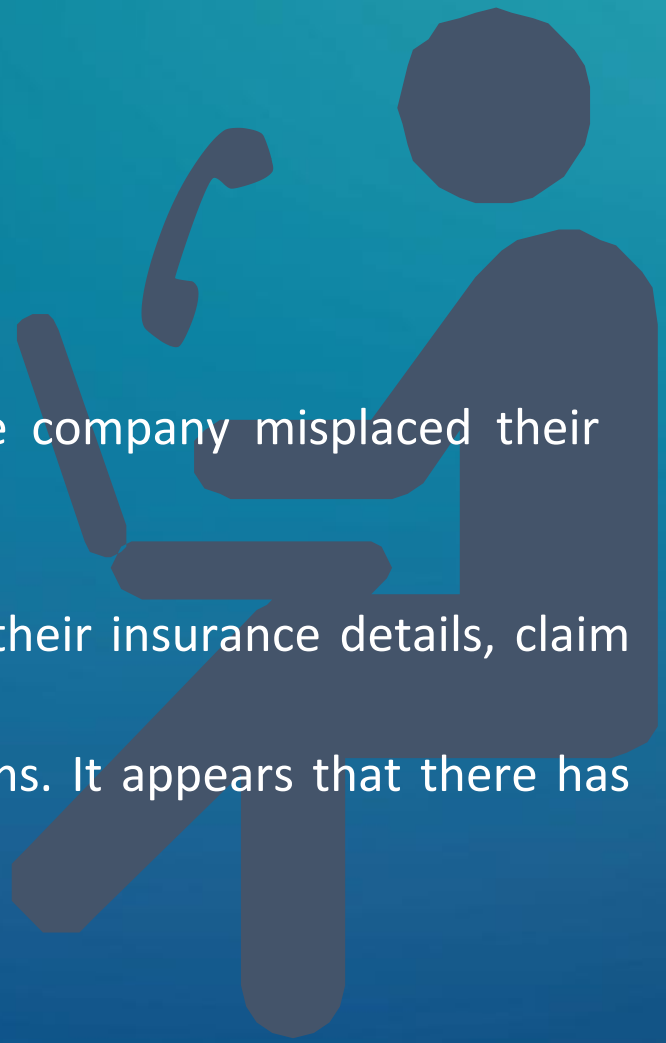
About me

Saminah Amin

- Senior Associate in the Cybersecurity Advisory practice at PwC
- Left Brain : Curious, Background in Computer Engineering, Professional Penetration Tester, Red Teamer, Social Engineer
- Right Brain : Creative, Likes reading, photography, painting
- Advocate for Women in STEM and Women in Security and Privacy
- First Time at GHC

You: The Victim

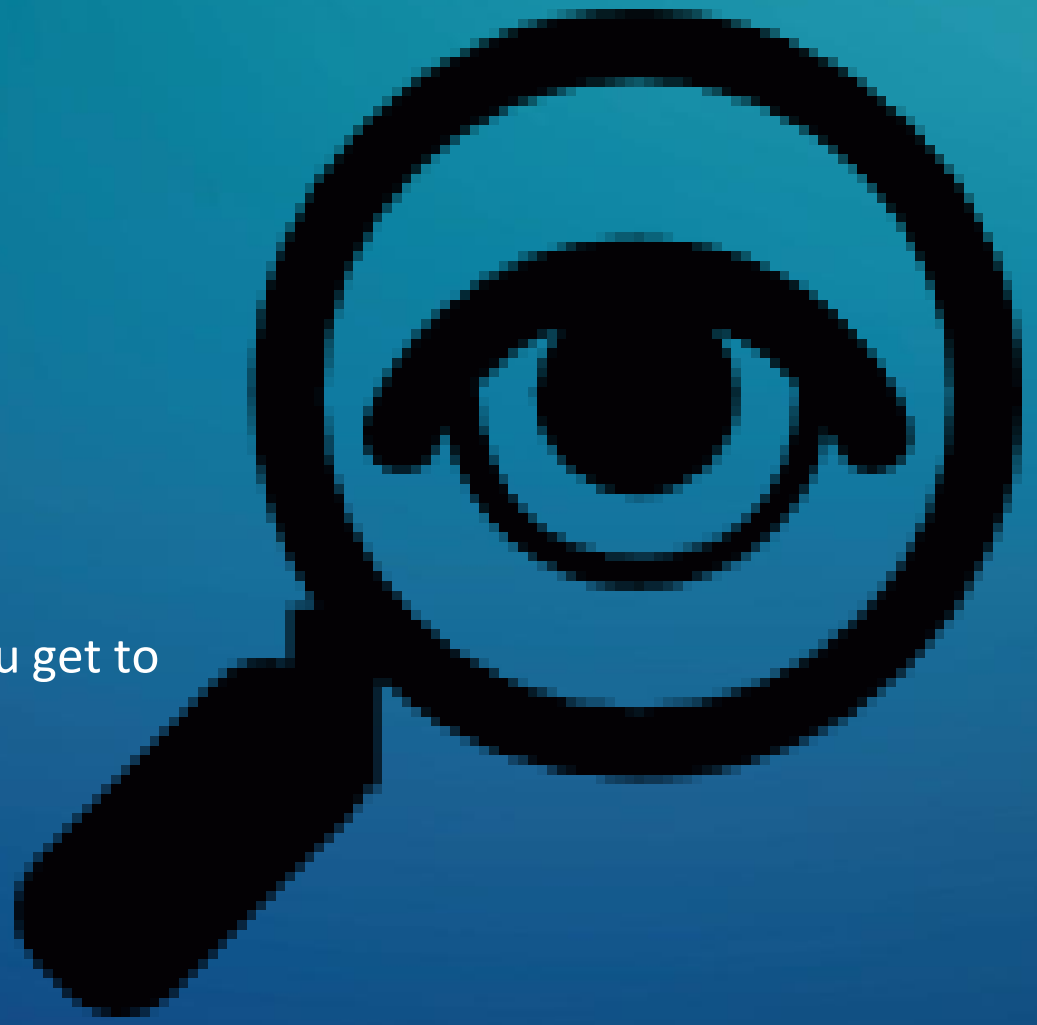
- You are a customer service rep at an insurance company.
- Frustrated customer calls you during business hours, saying the company misplaced their insurance claim and you allow them to send you an email.
- They send you what looks like a harmless Document containing their insurance details, claim date and address.
- Nothing alarming happens when you open the file - or so it seems. It appears that there has been a mistake on the customer's end and they hang up.



Forgot to mention – you have full authorized access to a central insurance database with customer PII and PHI.

You: The Attacker

- Gather information on the target company
- Use available tools, social media channels
- Perform a quick **reconnaissance** on the company*
- What is your goal?
  What kind of information can you recover to help you get to the goal through social engineering?
  - Names / Contact Info?
  - Pictures of Access cards?
  - Office space / Technologies?
  - Recent events?



**publicly available, open-source data access*

Cyber Red Teaming

- **Red Team**: Military Term for Offensive / Attack Tactics. Break everything. Bad Guys.
- **Blue Team**: Defensive Techniques. Monitors behavior, prevents compromise, reduces impact, performs forensics. Good Guys.
- Simulated Cyber intrusion exercise to test defensive control effectiveness. Ethical hacking, with authorization. Tests the following:

TECHNOLOGY

Security of Information and Computing Systems for regular business operations.

PEOPLE

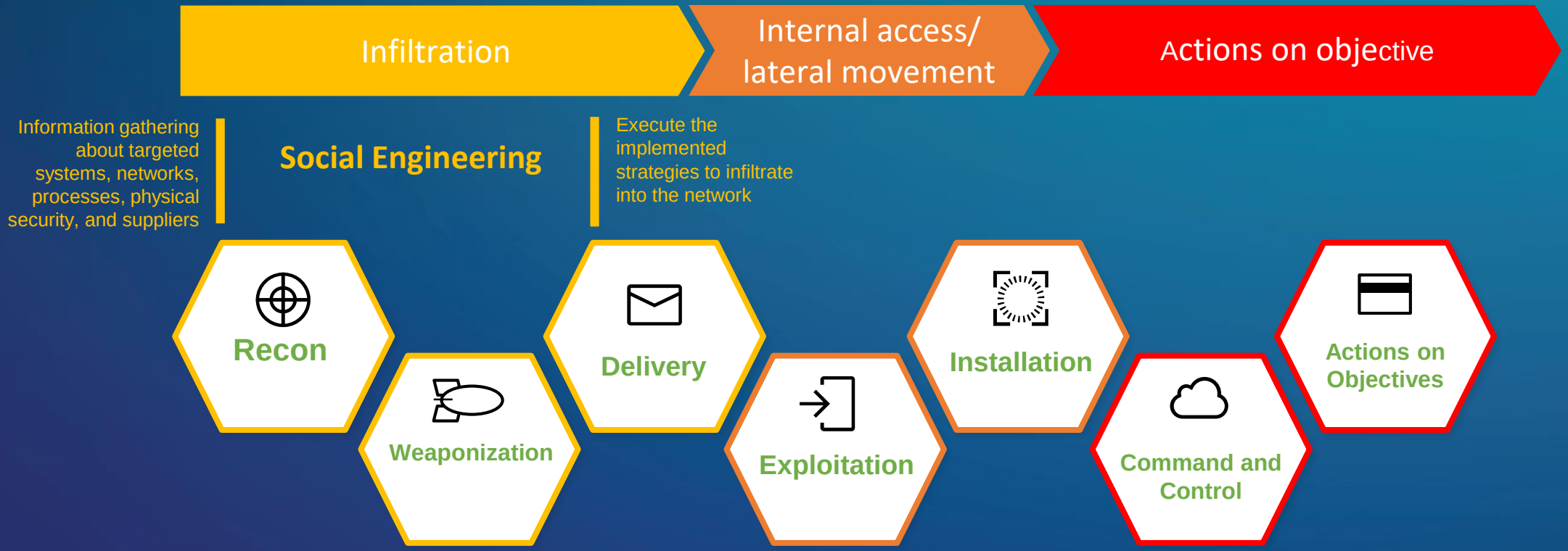
The “Smartest” Weakest Link – Human Behavior

PROCESS

Enforcement and Compliance of securely designed formal mechanisms, governance, policies.

Cyber Attack Lifecycle

Stages of a cyber attack:



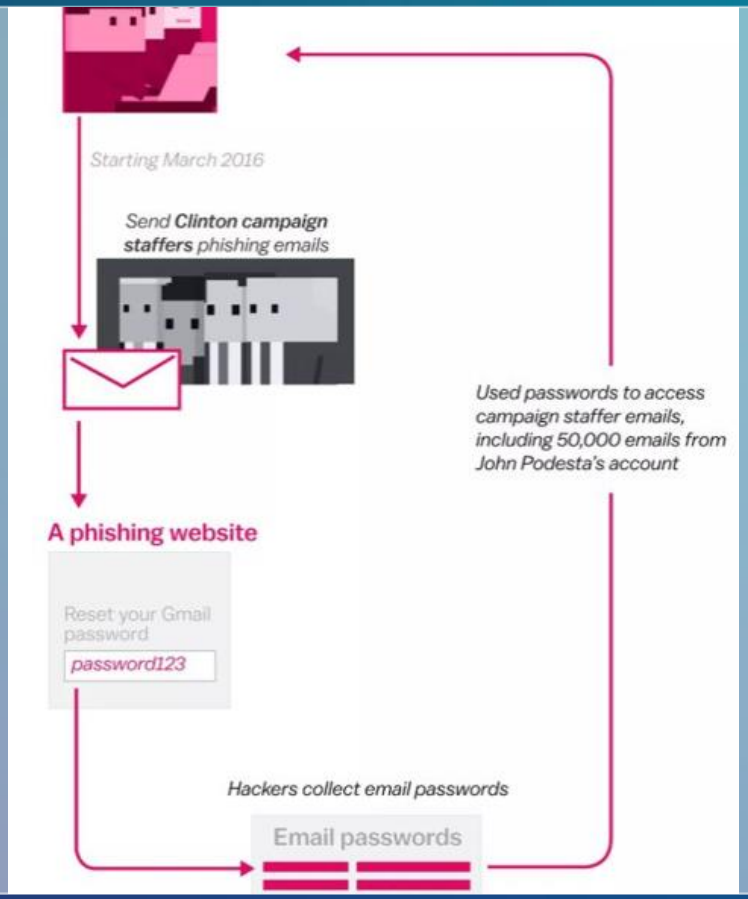
Real-World Situations

01

DNC Hack

Targeted

Spear-phishing



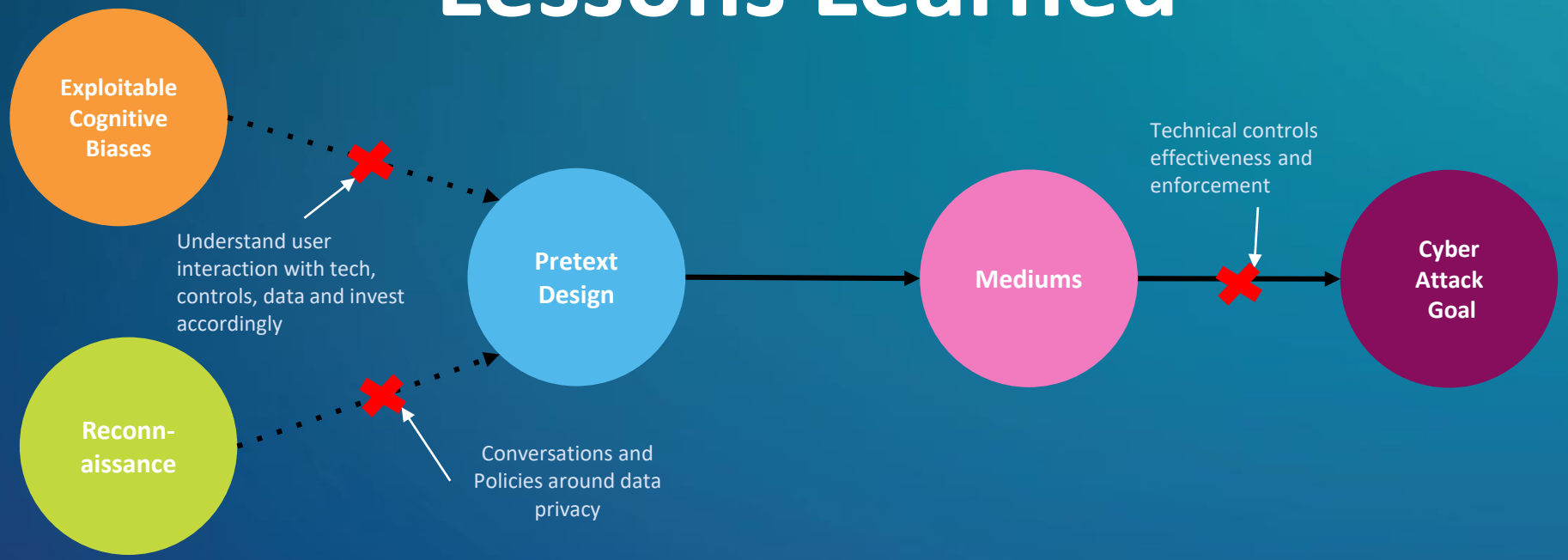
Voice

Deepfake

Voice-phishing

02

Lessons Learned



TACTICAL DETERRENTS

- A complex SE attack can be deterred by simple questions.
- Ask for a phone number to call back on.
- A single question can cause a ripple effect to unravel the pretext since it has no substantial basis.

STRATEGIC MITIGATIONS

- Increasing convergence of human and technology requires constant conversation .
- Evaluate a collective response over individual behaviors, such as contingency.
- Human-centered approach, work and security culture.
- Awareness campaign alone is not enough; No single solution can guarantee prevention.

“It's easier to ask forgiveness than it is to get permission.”

-Rear Admiral Grace Hopper

“But not in cyber. Always obtain authorization.”

-Every Ethical Hacker

Please remember to complete the session survey in the mobile app.

THANK YOU

YOU CAN *CONNECT WITH ME* @

https://ca.linkedin.com/in/saminah-amin-159a1851

GRACE HOPPER CELEBRATION

ANITA B.ORG

#GHC19