- Filename: eccouncil-ceh31250-v10-9-1-3-social_engineering_pt3.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Social Engineering Pt.3
- Description: In this episode, Daniel and Zach discuss the practice of performing Social Engineering techniques during a pentest engagement. Here you will learn the concepts and tactics that Social Engineers use to elicit information from their targets. These include the use of malicious apps for mobile devices, elicitation, Business Email Compromise(BEC), Interrogation, and Impersonation.

==========

Social Engineering Pt.3

- **You mentioned Vishing and Spimming, but are there other Social Engineering attacks that we may see against mobile devices?**
- Mobile
    - Publish malicious apps
    - Repackaging apps with malware
- Elicitation
    - Collecting data FROM humans vs ABOUT humans
        - Insider information about systems
    - Business Email Compromise(BEC)
        - Attacker pretends to executive
        - Attacker compromises executive's email account
            - Attacker sends fake email to Finance requesting funds
                - Wire transfer
                    - Finance complies (request seems legit)
        - **DEMO: Spoof email request for funds**
            - `EHLO`
            - `MAIL FROM:<spoofed sender>`
            - `RCPT TO:<victim email addr>`
            - `DATA`
            - `Subject:`
            - `From:`
- Interrogation
- Impersonation
    - Pretending to be an authority
        - Helpdesk/IT
            - Can gather target info for increased believability
                - Social Media
    - Use that disguise to get target to perform task/give info
        - Change your password to XXXXXX
        - Need to check your account for errors. What's your pass?