Case study 1: Fake employment 2020 Lessons.

- Attacker leveraged desperate job search
- Attacker leverage publicly available information of corp executives such as names, job roles and signatures
- Victim was unaware of adversarial tactics such as phishing and the dangers of sharing one time codes

Case study II: Instagram account takeover

- Attacker impersonates previously compromised victim's buddy
- Attack suggests victim to vote for buddy in an ongoing election
- If victim indicates interest, attacker instructs victim to send link received in SMS
- Naive victim sends link from SMS to impersonated buddy
- Attacker logs into victim's account, resets email and enables MFA