Banking Security

1. Why is the optimal amount of card not present fraud non-zero? Who benefits from the current liability regime for card not present fraud, and who shoulders the cost?
2. Many banking apps now use on-device biometrics (like finger prints) to authenticate users. How could a criminal log into the victim's account using the only using the criminal's finger print?
   (There are at least 2 examples, with varying digress of likelihood)
3. Historically, joint bank accounts required a signature from both account owners on both cheques and bank transfer requests. What are the barriers to adopting a similar separation of duties in online banking? Which cybercrimes would this help prevent?
4. How committed is the banking industry to customer security?

Economics

5. What is the tension between backwards compatibility and card fraud?
6. Microsoft issued patches for 1,246 Common Vulnerabilities and Exposures (CVEs) across its products in 2025. What economic ideas help explain why individuals and businesses continue to use Microsoft products?
7. To what extent does market concentration help intelligence communities? How does this explain attempts to ban foreign social media networks?
   (Relate this back to the spooks part of Lecture 2)
8. Which of the following is the biggest driver of security failures:
   a. Principal agent problems
   b. Negative externalities
   c. Information asymmetry
   d. Market concentration

   Explain.
9. Antivirus software is sometimes considered a "market for lemons". To what extent is this true, and is it down to hidden information, hidden action, or both?

Psychology

10. To what extent is blaming the user a valid explanation for why security failures happen?
11. Provide an example of a cyber attack technique that exploits each of: (1) skill-based behaviour; (2) rule-based behaviour; and (3) knowledge based-behaviour. Can you think of an example that exploits multiple?

12. Which aspects of psychology would you have expected to be covered in thise course, but were not?
13. Imagine that you are designing a spear-phishing attack designed to scam Edinburgh students out of money. How would you do it, who (or what) would you impersonate, how would you extract the money, and could you use Prospect Theory to increase your chances? Are there any other social-psychology tricks that might help?