Exercise 1: Pick any version of the encryption program PGP or its free equivalent GPG preferably one with a GUI and list:

(a) Three potentially dangerous irreversible actions that a user might perform by accident (higher marks the more dangerous the action and the more likely the user is to invoke it by accident);

(b) Three common actions that users might get wrong, with explanations of why they might get it wrong and of how the user interface might be improved to decrease the likelihood of that happening.

Exercise 2: List three kinds of “costs” perceived by individuals of security tasks imposed by system administrators.

Exercise 3: Optional question
Describe at least 3 practices commonly adopted by system administrators to enhance password security that instead have the opposite effect. Explain why they backfire and discuss ways to improve them.

Exercise 4: How would you get hold of:

(a) The employee number of a mark in a corporation? (And, having obtained it, how could you use it?)

(b) A company-confidential internal phone directory?

(c) The credit card number and expiry date of a mark? (And, having obtained it, how could you get a couple of grand out of it without getting caught? Assume for simplicity that that’s in the days before CVV.)

More generally, what are the important traits of a successful social engineer?

Exercise 5: Explain three principles of human psychology that you can exploit to steal a hundred pounds cash from a stranger. Explain how you can exploit those same principles to attack a computer system. Explain how you can exploit those same principles to sell an overpriced car to a mark.
Exercise 6: For each of the items below, construct an example test of the type “Would you rather take choice A or choice B?” to illustrate the phenomenon. In each case, explain the insight.

(a) The crucial insight of Bernoulli’s Expected Utility Theory.
(b) “Bernoulli’s error” as described by Tversy and Kahneman.

Exercise 7: Describe with an example what Tversy and Kahneman call the “anchoring” effect. How might you account for some of the difficulties planning software projects and security policies? [By NCW]

Exercise 8: Optional question

Explain Bernoulli’s model for risk aversion. How would you design an experiment where the model fails? Briefly sketch an alternative model describing framing effects. [By NCW]

Exercise 9: Bell-LaPadula consists of two rules. What is the invariant that both rules are intended to preserve?

Exercise 10: In a military context, you have a BLP compliant system with a subject (= process) A cleared to TOP SECRET and a subject B cleared to CONFIDENTIAL. A file X containing nuclear launch codes is labelled as TOP SECRET. Is it possible for A to transmit the content of X to B? If yes, how (and why would A want to do that)? If no, why?

Exercise 11: Write a simple security policy describing a website to promote a new product. Consider what sort of attackers the policy covers and those not included in its scope. What resources are being protected, and for what purpose? (This document is called a “security policy model” by Ross Anderson.) [By NCW]

Exercise 12: Optional question

Describe how the Biba security model could be applied to an industrial site’s monitoring, safety and control systems.

Exercise 13: An effect which is not accounted for by the market price for a good is known as an externality.

(a) What people are affected by externalities?
(b) Consider the mining industry. Give one example of a positive externality, a negative externality, and a way to use the economic system to remove the externalities.
(c) What are the incentives for OS manufacturers, anti-virus manufactures, and enforcement agencies? How does the interplay between these influence what we see in practice?
(d) For each of the three markets (OS and anti-virus bought by consumers and enforcement bought by governments), give an example of an externality.

[a,b,d by NCW]
**Exercise 14:** Optional question

What are the incentives in banking for banks, customers and governments. What are they likely to result in? How can the incentives be changed to make things better?

**Exercise 15:** How and why does the attitude of software companies towards quality and security vary over time?

**Exercise 16:** What should ISPs do about malware on customer machines? Why? Does this happen? Why?