

9

NETWORKS AND COMPUTER SECURITY

Chapter Summary

We live in a networked world. Home computers are linked into the internet, and laptops, tablets and smartphones provide internet access on the move. Personal computing connects people via e-Mail and social networking. Members of the public can also access the vast resources of the World Wide Web, link to commercial computing via e-Business and to public administration in a development called e-Government.

Organizations have their own internal networks used for communications and to access Business Information Systems from the desktop, the shop floor and on the move. Organizations are networked to one another for e-Commerce and e-Government exchanges, and to the outside world by the internet.

The internet, a global web of interconnecting networks, some public and some private, unifies these networks as a global resource – a resource not owned or formally controlled by any corporation or government.

These networks, and the communications that they support, are a complex technical infrastructure. The infrastructure is built with network equipment, a connection and the message protocol – we will look at each of these components.

Networks, apart from their legitimate uses, can provide access to those with illegitimate intents (and that in turn gives rise to questions as to what is legitimate and what is not). In this chapter we look at computer security – in **Part 5** we will take a wider look at the societal implications of (networked) computing.

