In this chapter, you have learnt about:

- ✔ the difference between the internet and the World Wide Web
- ✔ what is meant by a URL
- ✔ the purpose of hypertext transfer protocols (http and https)
- ✔ the purpose and function of a (web) browser
- ✔ how to locate and retrieve web pages from a website
- ✔ session and persistent cookies
- ✔ digital currency and blockchaining
- ✔ cyber security threats (brute force attacks, data interception, DDoS, hacking and social engineering)
- ✔ malware (viruses, worms, Trojan horses, spyware, adware and ransomware)
- ✔ phishing and pharming
- ✔ ways of alleviating cyber security threats (anti-malware, access levels, authentication, firewalls, proxy servers and SSL)
- ✔ improving security using automatic software updates, privacy settings and looking for security clues in emails and URL links.

Key terms used throughout this chapter

internet – the world-wide interconnection of networks; the internet makes use of TCP and IP protocols

World Wide Web – a massive collection of web pages and is based on hypertext transfer protocols (http and https)

(web) browser – software that connects to a domain name server (DNS) to locate IP addresses; a browser interprets HTML web pages sent to a user's computer so that the user can read documents and watch multimedia

hypertext mark-up language (HTML) – the language used to design, display and format web pages, and to write http(s) protocols

uniform resource locator (URL) – a text-based address for a web page

hypertext transfer protocol secure (https) – http with extra security (such as SSL) applied

hyperlink – highlighted text or an image that is activated by clicking and links to further text, images, a web page or a website

domain name server (DNS) – a server that looks up domain names for websites (for example, www.hoddereducation.com) in order to find the IP addresses that a computer needs to locate the web servers (for example, 107.162.140.19)

cookie – a text file sent from a website to a user's browser; it is used to remember user preferences each time they visit the website

user preferences – settings or options stored in cookies that can remember customised web pages or indicate browsing history to target adverts

session cookie – a cookie that is stored temporarily on a computer; it is deleted when the browser is closed or the website session ends

persistent cookies – a cookie that is stored on the user's hard drive and only deleted when the expiry date is reached or the cookie is deleted by the user

virtual shopping basket – an area of memory in a website where items a user wishes to purchase are temporarily stored; items remain in the basket until payment is made or the session has ended

digital currency – currency (a system of money) that exists in electronic form only; it has no physical form and is essentially data on a database

cryptocurrency – a form of digital currency that uses a chain of decentralised computers to control and monitor transactions

cryptography – the protection of data/information by use of coding; it usually involves encryption and decryption

blockchain – a decentralised database where all transactions are stored; it consists of a number of interconnected computers but not a central server

timestamp – a digital record of the date and time that a data block is created in blockchain networks

proof-of-work – the algorithm used in blockchain networks to confirm a transaction and to produce new blocks to add to the chain; special users called miners complete and monitor transactions on the network for a reward

brute force attack – a 'trial and error' method used by cybercriminals to crack passwords by finding all possible combinations of letters, numbers and symbols until the password is found

word list – a text file containing a collection of words used in a brute force attack

data interception – an attempt to eavesdrop on a wired or wireless network transmission; cybercriminal often use

packet sniffing or access point mapping / wardriving to intercept data

packet sniffing – a method used by a cybercriminal to examine data packets being sent over a network and to find the contents of a data packet, which are sent back to the cybercriminal

wardriving – using a laptop, antenna, GPS device and software to intercept Wi-Fi signals and illegally obtain data; sometimes called Access Point Mapping

wired equivalency privacy (WEP) encryption protocol security – an algorithm for wireless networks to protect them against data interception

denial of service (DoS) attack – a cyberattack in which cybercriminals seek to disrupt the normal operation of a website by flooding it with requests; also used to clog up a user's mailbox by sending out thousands of spam emails

distributed denial of service (DDoS) attack – a denial of service (DoS) attack in which the fake requests come from many different computers, which makes it harder to stop

spam – unsolicited emails sent to a user's mailbox

hacking – the act of gaining illegal access to a computer system without the owner's permission

malware – programs (such as viruses, worms and Trojan horses) installed on a user's computer with the aim of deleting, corrupting or manipulating data illegally

virus – a program or program code that replicates itself with the intention of deleting or corrupting files or by causing the computer system to malfunction

active host – functioning software that a virus can affect by attaching itself to the code or by altering the code to allow the virus to carry out its attack

worm – a stand-alone type of malware that can self-replicate; unlike viruses, worms don't need an active host; they can spread throughout a network without the need for any action by an end-user

Trojan horse – a type of malware that is designed to look like legitimate software but contains malicious code that can cause damage to a computer system

spyware – a type of malware that gathers information by monitoring a user's activities on a computer and sends the gathered information back to the cybercriminal who sent out the spyware

adware – a type of malware that attempts to flood the end-user with unwanted advertising

ransomware – a type of malware that encrypts data on a user's computer and 'holds the data hostage' until a ransom is paid

phishing – sending out legitimate-looking emails designed to trick the recipients into giving their personal details to the sender of the email

spear phishing – similar to phishing but targeting specific people or organisations rather than carrying out a blanket attack

pharming – redirecting a user to a fake website in order to illegally obtain personal data about the user without their knowledge; unlike phishing, pharming is initiated without needing any action by the user

DNS cache poisoning – altering IP addresses on a domain name server (DNS) with the intention of redirecting a user's browser to a fake website; carried out by a pharmer (see pharming) or hacker (see hacking)

social engineering – manipulating people into breaking normal security procedures (such as giving away their password) in order to gain illegal access to computer systems or to place malware on their computer

access levels – different levels of access in a computer system allowing a hierarchy of access levels depending on user's level of security

anti-spyware – software that detects and removes spyware programs installed on a system; the software is based on typical spyware rules or known file structures

authentication – the process of proving a user's identity by using something they know, something they have or something unique to them

biometrics – type of authentication that uses a unique human characteristic, such as fingerprints, voice or retina blood vessel pattern

two-step verification – a type of authentication that requires two methods of verification to prove the identity of a user

patch – an update for software that is developed to improve the software and/or to remove any bugs

typo squatting – the use by cybercriminals of subtle spelling errors in website addresses used to trick users into visiting their fake websites

firewall – software or hardware that sits between a computer and an external network (for example, the internet); the firewall monitors and filters all incoming and outgoing traffic

proxy server – a server that acts as an intermediary server through which internet requests are processed; it often makes use of cache memory to speed up web page access

privacy settings – controls available on social networking and other websites which allow users to limit who can access their profile or what they are allowed to see

secure sockets layer (SSL) – a security protocol used when sending data over a network (such as the internet)

SSL certificate – a form of digital certificate which is used to authenticate a website; providing the SSL certificate can be authenticated, any communication or data exchange between browser and website is secure