Solutions

Each answer shows the steps, then the **result**.

2.1

- information about an individual that identifies, links to, relates to or describes them; any three of: name, address, ID or passport number, date of birth, phone number, email address, fingerprint or other biometric, place of work

2.2

(a)

- faster purchases with no re-typing; the stored details enable identity theft or fraudulent purchases if the store is breached

(b)

- more relevant results and suggestions; the history can be used for targeted marketing, or reveal interests the user never stated

(c)

- directions and local recommendations; the record shows where the user lives, works and when their home is empty

2.3

- aggregation is combining disparate pieces of data - each harmless alone - to create knowledge about an individual. Example: geolocation gives a home address and cookies from a health forum suggest a condition, so together they identify a specific person's likely medical condition, which neither source stated. Accept any two genuinely separate sources with a deduced conclusion

2.4

- once information is placed online it is difficult to delete - it may already have been forwarded, retweeted, screenshotted or copied by others, so the original's removal does not remove the copies

2.5

- MFA grants access only after the user presents several separate pieces of evidence, typically at least two steps; each step is an additional layer that must be broken; so a stolen password is only one factor and the attacker still cannot reach the account without the second

2.6

- it is easy for the user to remember but difficult for someone else to guess even knowing that user - so not a birthday, a pet's name or anything posted publicly

2.7

(a)

- keylogging

(b)

- rogue access point

(c)

- phishing

(d)

- untrustworthy download / malware from freeware

2.8

- malware is the general category - software intended to damage a computing system or take partial control of its operation; a virus is one kind of malware that copies itself and often attaches to a legitimate program, running when that program runs

2.9

- every real-world system has errors or design flaws that can be exploited to compromise it; an update fixes those flaws, so an unpatched system stays exploitable by an attack that is already publicly known

3.1 B

3.2 B

3.3 B

- A certificate authority validates ownership of an encryption key, on a trust model. Without it, an attacker's key could be accepted as the recipient's

3.4 A

- Data sent over public networks can be intercepted, analysed **and modified**. A normal-looking page proves nothing, and a strong password does not stop interception of the traffic

3.5

(a)

- any two of: **location/route data** - reveals home address and daily pattern, enabling stalking or a burglary timed to an absence; **timestamps** - show when the home is regularly empty; **contacts** - allow phishing of friends from a trusted name; **name and account identity** - supports identity theft

(b)

- each source alone is ordinary, but a run that starts and ends at the same point every morning identifies the home, while a social post names the employer or school; combined they give a named individual, a home address and a predictable time window - none of which the user posted

(c)

- any two of: the data is not only about them - the contacts belong to other people who did not consent; data collected now can be used later in ways not intended, and cannot be deleted once shared; aggregation means harmless data becomes harmful in combination; a breach of the app exposes it regardless of the user's own conduct

(d)

- the attacker now holds a working password for the **email and bank accounts as well**, because re-use means one breach compromises every account sharing that password; and the email account is the reset route for the others, so control of it can unlock accounts that used a different password. Measures - any two of: a unique password per account, so a breach is contained; multifactor authentication, so a stolen password is not sufficient; a password manager, which makes unique passwords practical

(e)

- encryption encodes the data in transit and at rest so an interceptor cannot read it. It does **not** protect against threats that bypass it: a phishing message that gets the user to hand over the password, keylogging that captures it as it is typed, or malware on the device that reads the data after decryption; nor does it help once the attacker holds a valid credential, because the system then decrypts for them