Component 3 mock exam revision topics:

Communication platforms e.g. social media, VOIP, DM, email

Positives:

Available 24/7 • Used for advertising • Cheap/cost effective • Track visits/analytics • Global audience / wider reach • Client can provide feedback/reviews

External threats:

Unauthorised access (hacking) • DOS • Phishing • Pharming • Social engineering • Shoulder surfing • Man in the middle attack • Theft of device • Natural disaster

Why anti-virus?

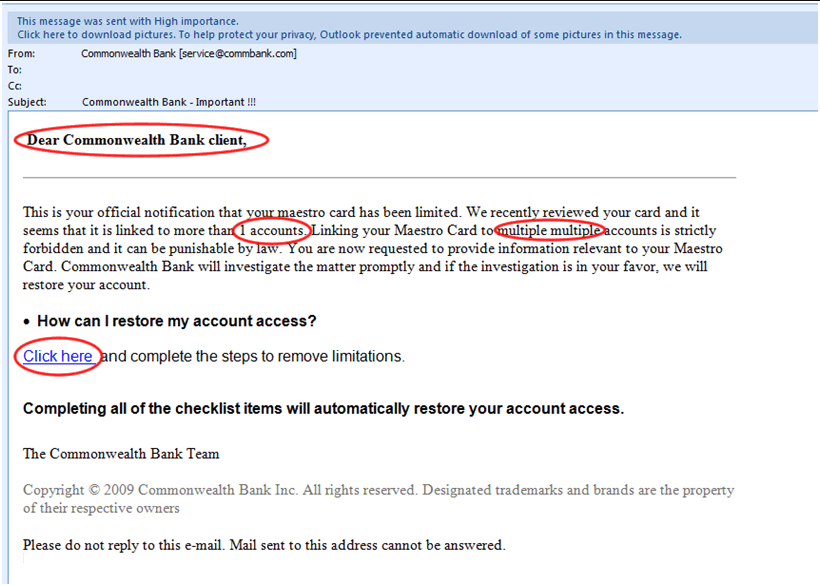
Anti-virus runs in the background (1) • It automatically updates its database of threats (1) • It scans files/sources/emails (in real time) (1) • Then compares to known threats (stored in its database) (1) • Then quarantines/refuses to download/removes suspicious files/emails (1) • And informs the user (1

Benefits of working from home:

Savings on travel/transport cost • No travel time/don’t need to travel • More flexible start/finish times/ work anytime • Can work around family/friends/social commitments • Saving on clothes for work • Can be a more relaxed working environment • No dress code • Can improve productivity/efficiency • Can improve morale/mental health • Can work globally/anywhere

Disadvantage of working from home:

Interruptions/distractions (1) as this can stop staff concentrating/make mistakes (1) • Stress/anxiety (1) because the company may expect staff to work outside their normal hours (1) • Isolation/loneliness (1) as there is a lack of face-to-face interaction with other staff/customers (1) • Poor work life balance (1) as staff have 24/7 access to work emails/cloud storage/video conferencing (1) • Need reliable/adequate internet connection (1) as constant connection is needed to complete work (1) • Rise in household bills (1) as they will be using more electricity/energy to run devices/increase internet usage/speed (1)



Benefit of using messaging apps:

Private/secure (1) because messaging apps use (end-to-end) encryption (1) • Staff can see if other staff are online/away/busy/available (1) as they can set their status (1) • You can have a real conversation (1) as it is in real time (1) • Record/backup of messages (1) as threads are kept for future use (1) • You do not need to repeat information (1) as you can use group chat (1) • Share files (1) which would aid collaborative working (1) • Can receive notifications (1) so important information can be shared/responded to quickly (1

IT Acceptable Use Policy

Not send indecent images/text/video (1) as could be illegal/cause offence (1) • Not send chain/spam emails (1) as could include malware (1) • Not send information that is personal/can identify a donor/client/company (1) as could breach GDPR (1) • Not share copyrighted charity material (1) as could be fined (1) • Not use inappropriate language (1) to maintain the charity’s good reputation (1) • Not to use for personal use (1) as staff could get distracted/waste time (1)

o be more environmentally friendly and save on resources

Use auto-power off/turn off (1) (so that equipment is switched off) when not in use (for a set period of time) (1) • Use power saving settings (1) to extend battery life (of portable devices)/reduce electricity consumption (1) • Use digital copies (1) so that files do not need printing off/download software not buy a disc (1)

Explain two drawbacks of sharing this data

• (Ensure staff meet the) GDPR/DPA/legal requirements (1) as they could be in breach/fined/sued (1) • The data could be intercepted/hacked (1) which could lead to the data could be leaked/stolen (1) • Personal data may need to be anonymised (1) so that the donor’s privacy is maintained (1) • (Ensure data is) not misused/wrongly used (1) as the donor could be upset that their personal data is being shared/known to others (1)

**FLOW CHARTS – buying something from Amazon**

A security breach would have an impact on the company. One possible impact of a security breach would be data loss. Explain one other impact of a security breach:

Financial loss/lack of profit/income (1) as they would not be able to sell products (1) • Damage to public image/loss of reputation (1) which means they would lose customers/customers would not trust them (1) • Reduction in productivity (1) as without the designs they would not be able to make products (1) • Legal action (1) as customer information is personal data that is covered by GDPR/could be fined (1) • Downtime (1) as they would need to rebuild the data/reinstall a backup (1)

Describe how net neutrality can benefit small companies

By law all internet traffic is treated equally (1) • (ISPs) must not favour wealthier companies over those who cannot afford to pay higher fees (1) • Responsibility for this is with ISPs (1) • (ISPs) cannot block access to sites (1) • Or slow down speed/throttle (1) • Net neutrality is enforced by Ofcom (1)

user access restriction methods the company could use

Use physical security measures e.g. door locks, keypads, swipe cards, fobs, security guards - to prevent physical access to areas where the system is located. • Users have passwords – only authorised users can log on securely to the systems. • Settings/levels of access – set up users with the correct access rights so only certain tasks can be done users e.g. read, read/write, full control. • Biometrics entry systems – e.g. facial, retina, iris, fingerprint, palm, as these are unique to the user and can’t be forged. • Using two-factor authentication - users have to prove their identity using something that they are, what they know or what they have – methods of receiving authentication e.g. email, text etc.