Task 1

In the context of IT and business, lock-ins refer to situations where a customer becomes dependent on a vendor for products or services, making it difficult or costly to switch to another provider. Lock-ins are generally categorized into technological lock-ins and vendor lock-ins.

- **Technological Lock-ins** occur when a business is tied to a specific technology due to the high cost or difficulty of migrating to another system. This is common in software or hardware solutions where the architecture is proprietary or highly specialized. For example, an organization that has deeply integrated Microsoft's ecosystem may find it challenging to switch to alternatives like Linux or open-source software due to compatibility and retraining costs.
- **Vendor Lock-ins** happen when businesses rely heavily on a particular vendor for services or products. Cloud services like AWS or Azure are examples of vendor lock-ins, where switching to another provider could involve costly data migration, service disruptions, and retraining staff.

The potential costs of breaking free from lock-ins include migration fees, retraining employees, and the risk of service disruption. However, staying within a lock-in can provide stability, support, and seamless integration but can also limit flexibility and lead to higher costs over time as the vendor gains more control over pricing. Balancing the pros and cons of lock-ins is essential for strategic decision-making.

Task 2

** Why are phishing attacks effective enough to be a widespread practice?**

Phishing attacks exploit cognitive biases and trust. Attackers craft messages that appear to be from legitimate sources, taking advantage of users’ trust in known organizations or people. Cognitive psychology explains that when people are under pressure or distracted, they are more likely to make quick, less thoughtful decisions, which phishing attacks capitalize on. Phishing is effective because it targets human errors in judgment rather than technical vulnerabilities, making it easier to bypass security mechanisms.

** Why does social engineering work on people?**

Social engineering manipulates human psychology, particularly trust and authority. People tend to comply with requests when they believe the request comes from a legitimate authority or peer. Social engineering tactics like impersonation or emotional manipulation exploit this natural trust. Additionally, individuals may fail to recognize suspicious behavior when under stress, urgency, or pressure, making them more susceptible to manipulation. This behavior is tied to behavioral psychology concepts such as obedience to authority and cognitive shortcuts.

** Why do many people have a hard time using passwords in a secure way?**

People struggle with using secure passwords due to cognitive limitations like memory and convenience. Strong passwords are often complex and hard to remember, and many individuals opt for simpler passwords or reuse them across multiple accounts for ease of use. Cognitive psychology explains that people prioritize convenience over security when faced with complex tasks like managing numerous secure passwords. This tendency is reinforced by the lack of immediate consequences for poor password practices, making secure habits difficult to maintain.

□ **Why does PGP fail to be an effective way to secure email?**

PGP (Pretty Good Privacy) encryption, while technically secure, is often considered user-unfriendly and complex. The steep learning curve and cumbersome setup processes deter many users from adopting it. Behavioral psychology shows that people avoid complicated tasks, especially when alternatives are easier, even if less secure. Additionally, the decentralized trust model of PGP requires users to manually verify each other's keys, which can be inconvenient, leading to low adoption rates.

□ **Why is it so easy to spread malware?**

Malware spreads easily due to a combination of technical and psychological factors. Technologically, malware can exploit system vulnerabilities, and socially engineered attacks trick users into executing malicious files or links. Cognitive psychology explains that users are often unaware of the risks of their actions, such as clicking on suspicious attachments or visiting compromised websites. The interconnected nature of modern systems and the reuse of credentials across platforms further facilitate the rapid spread of malware.

TASK 3

Task 3A: Intellectual Rights - Explanation of Safeguarding Methods

1. **Intellectual Property (IP):**

   IP refers to the legal protection of creations of the mind, including inventions, literary and artistic works, symbols, names, and designs. Companies safeguard their IP to prevent unauthorized use and protect their competitive advantage.
   Example: Apple’s design patents on the iPhone to prevent other companies from copying its design.

2. **Copyright:**
   Copyright protects original works of authorship like books, music, and software from being reproduced without permission. It grants the creator exclusive rights to use and distribute the work.
   Example: Music labels using copyright to prevent unauthorized distribution of songs.

3. **Patent:**
   A patent provides an inventor with exclusive rights to make, use, or sell an invention for a set period. Patents encourage innovation by protecting novel inventions.
   Example: Pfizer’s patent on certain pharmaceutical drugs, preventing generic drug production.

4. **Trademark:**
   Trademarks protect brand names, logos, and slogans that distinguish goods or services. It helps consumers identify and trust specific brands.
   Example: Coca-Cola’s trademark on its logo and bottle design to prevent counterfeit products.

5. **Non-Disclosure Agreements (NDAs):**
   NDAs are legal contracts that prevent parties from disclosing sensitive information shared during business dealings. They are crucial for maintaining confidentiality in business negotiations.
   Example: An NDA signed by employees of a tech company to protect trade secrets.

6. **Watermarks:**
   Watermarks are visible or invisible markings on digital or physical assets used to assert ownership and prevent unauthorized use. They are commonly used on images and videos.
   Example: Photographers watermark their images before posting them online to prevent unauthorized use.

7. **Software Licenses:**
   Software licenses define how a program can be used and restrict unauthorized copying or modification. This ensures that the software creator gets paid for their work.
   Example: Microsoft Office's software license prevents users from sharing it with others without proper authorization.

8. **Digital Rights Management (DRM):**
   DRM is a technology that controls how digital content is used and distributed. It prevents piracy and ensures that only legitimate users can access certain media.
   Example: Streaming services like Netflix use DRM to prevent unauthorized sharing of their content.

9. **Software Protection Dongles:**
   A dongle is a hardware device that must be plugged into a computer for certain software to work. It acts as a physical key, preventing software piracy.
   Example: High-end software for engineering applications often requires a dongle to operate, preventing unauthorized copies from being used.

Task 3B: Freedom of Information

Two safeguarding methods that are often bypassed are **DRM** and **copyright**. Instances of this occur frequently in the digital space.

1. **DRM Circumvention – Video Games:** DRM is commonly employed in video games to prevent piracy, but this protection method has often been bypassed by hackers. For example, the game "Assassin's Creed: Origins" from Ubisoft used a sophisticated DRM system known as Denuvo. However, within weeks of its release, the DRM was cracked, and pirated copies became widely available.
   The rationale behind this circumvention is often attributed to a protest against the inconveniences DRM systems cause for legitimate users. Many consumers argue that DRM restrictions affect their experience by requiring constant online connectivity or slowing down their system performance, while pirates enjoy a smoother, unrestricted version of the game.

2. **Copyright Circumvention – Digital Media Sharing:** In 2012, the U.S. file-sharing service Megaupload was shut down by authorities due to massive copyright infringement. The website was used to share movies, music, and software illegally. Copyright owners such as film studios argued that the site was profiting from distributing pirated content. Despite legal actions against such platforms, many argue for "freedom of information," stating that digital media should be freely available for all, particularly in less economically developed regions where individuals cannot afford the high cost of licensed media.

In both cases, the individuals or groups circumventing the safeguards often justify their actions through the argument of **free access to information** or **protest against restrictive practices** that, in their view, limit user freedom or create unnecessary barriers to accessing content or software.

However, from the perspective of content creators and companies, these methods of protection are necessary to ensure fair compensation for their work and to fund future innovation.