Exercise – 3
Abdurrehman Syed
2308546

Task – 1

Technological lock-in can be either when the user relies on a certain technology or software system, or vice versa; switching becomes either difficult or expensive. It could be due to proprietary formats and complex integrations. For example, sometimes using an Apple ecosystem makes it hard for users to move to an Android device because there are applications or other features they have grown accustomed to.

Vendor lock-in implies dependence on a particular seller or supplier of goods and services, whether this be via binding long-term contracts, bespoke solutions, or simply lack of competitive offerings. An example could include organizations investing heavily in the implementation of an ERP system from a particular vendor experiencing difficulty and cost when looking to use an alternative provider.

Breaking lock-ins can be very expensive and time-consuming. Besides other things, it means investment in new hardware or software, migration, and retraining of staff. There could also be risks associated with disruption during the transition process. However, there could also be a number of disadvantages in remaining in a lock-in, including stifling innovation, reducing flexibility, and possibly even increasing costs over time.

Sources:

- Laudon, K. C., & Laudon, J. P. (2016). Essentials of Management Information Systems. Pearson.
- TechTarget. (n.d.). Technological Lock-in. SearchEnterpriseSoftware.

Task – 2

Why are phishing attacks effective enough to be widespread practice?

Phishing attacks have been successful due to the exploitation of human psychology and vulnerability. Many times, they use methods of social engineering in such a way that victims are compelled to click on links with malware or download infected files. They may be presenting spoofed identities of trusted people or organizations, where actors may create urgency or fear among the victims or offer big rewards that would eventually make the victims take bad decisions. In addition, phishing attacks get more sophisticated over time, making their detection more tedious; and thus, defending against the attack.

Why social engineering works on people?

Social engineering works on people because it plays to our underlying nature of trusting others, cooperating when asked to do so, and acting like everybody else around us. The phishers will employ plays like authority, scarcity, and social proof to get people to do what is being requested of them. Example Phishing attempts will impersonate trusted organizations or quote customer testimonials in establishing trust. Besides, people more easily perceive and believe those they perceive as similar to themselves. This is another reason phishers often craft messages targeting specific demographics.

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

Many people have a hard time using passwords securely because they find it difficult to remember complex and unique passwords for all of their accounts. The uneasiness of remembering every single password is the reason why most people have the same one for every account. This can lead to vulnerabilities and cyber attacks. Additionally, some people may be unaware of the importance of using strong passwords and may not take the necessary precautions to protect themselves from online threats.

Why PGP fails to be effective way to secure email?

PGP (Pretty Good Privacy) is a cryptographic protocol that can be used to encrypt and decrypt email messages. However, it is not always effective in securing email because it requires both the sender and the receiver to have PGP encryption keys. If either party does not have a PGP key, the email will not be encrypted and will be vulnerable to interception.

Why it is so easy to spread malware?

Malware can infect a computer through various means: email, messaging, social media, and file-sharing networks. Other sources of malware infection include infected websites, advertisements, or drive-by downloads. Once installed in any device, malware can quickly spread to other devices over the network or through removable media like USB drives. Additionally, malware has become increasingly sophisticated over time, thus making it even more challenging and tricky to trace and remove.

Task – 3 (A)

Legal Mechanisms:

- **Intellectual Property (IP):** A broad term that encompasses any intangible asset that can be owned, including inventions, literary works, designs, and symbols.
- **Copyright:** Protects original works of authorship, such as books, articles, music, and software etc.
  - **Use case:** A writer protects their novel from unauthorized copying and distribution.
- **Patent:** Grants exclusive rights to an invention for a limited period of time.
  - **Use case:** A pharmaceutical company patents a new drug to prevent competitors from producing and selling it.
- **Trademark:** Protects words, phrases, symbols, or designs that identify a product or service.
  - **Use case:** Coca-Cola protects its iconic logo and name from unauthorized use.
- **Non-Disclosure Agreements (NDAs):** Legal contracts that prohibit the disclosure of confidential information.
  - **Use case:** A company requires employees to sign NDAs to protect trade secrets and proprietary information. I signed such a document when I was working on a project for my internship.

Technologies:

- **Watermarks:** Visible or invisible marks embedded in digital content to identify ownership.
  - **Use case:** A photographer adds a watermark to their photos to prevent unauthorized use.
- **Software Licenses:** Legal agreements that govern the use of software.
  - **Use case:** A software company licenses its product to customers under specific terms and conditions.
- **Digital Rights Management (DRM):** Technologies that control access to digital content.
  - **Use case:** A music streaming service uses DRM to prevent unauthorized copying and distribution of songs.
- **Software Protection Dongles:** Hardware devices that are required to run certain software.
  - **Use case:** A video game company uses dongles to prevent unauthorized copying and distribution of their games.

Task – 3 (B)

IP and DRM are necessary mechanisms for safeguarding digital content against unauthorized access, distribution, and duplication. The same has, however, undergone numerous compromises in the past, therefore creating highly debated arguments concerning a delicate balance between protection of creators' rights and dissemination of information freely.

One of the highest-profile cases of DRM bypassing occurred in 2013, when hackers took advantage of security holes in the newly released "Grand Theft Auto V" video game to bypass the authentication mechanism and access the multiplayer part without actually buying a copy. The result was huge losses to the publisher, Take-Two Interactive, which is known to be raking in massive revenues from post-launch multiplayer engagement. The hacking community justified the action based on the fact that too much limitation on the DRM restrictions has been made and that was against the freedom of the consumers.

The circumvention of DRM also significantly affected e-book DRM. DRM-free software tools, such as Calibre, were used to remove the DRM protections of e-books bought from platforms such as Amazon Kindle. People who caused the circumvention of these e-book DRM say that this technology restricts consumer choice and locks consumers into proprietary systems. This is recognized in part by the 2012 ruling of the U.S. Librarian of Congress to provide an exemption under the DMCA that enables users to bypass e-book DRM for accessibility.

Another very common form of IP circumvention concerns pirated content through torrenting websites. These are websites, like The Pirate Bay, that enable people to download copyrighted movies, music, TV shows, and software without permission. While this is illegal in many countries, this continues to be common, partly because the cost for some types of media is very high, or the media are unavailable. Such operators typically defend the action based on the grounds that they are providing a neutral site for file sharing, and hence they are not responsible for what the users upload.

Outside of the realm of entertainment content, IP circumvention has had huge consequences elsewhere. In the context of pharmaceuticals, the denial of a patent on Novartis' cancer drug Glivec by the Indian government allowed several Indian pharmaceutical companies to sell cheaper generic versions. Labeled as a decision to be condemned by Novartis, public health advocates praised the fact that such a decision favored access to life-saving medication over corporate profits.

The circumvention of IP and DRM protections is a multidimensional issue, encompassing significant ethical, legal, and social dimensions. While creators and owners merit protection in order to keep their business models alive, excessive limitations on DRM hamper consumer choice and hinder innovation. There is a desperate need to balance intellectual property rights with the free flow of information in the digital era. Given that technology is developing day in and day out, reassessment should be given regarding how effective the measures are with regard to IP and DRM, while seeking alternative ways that favor both fairness and accessibility.

Sources:

- Business Insider. (2013). Hackers Breach Rockstar’s GTA V
- Electronic Frontier Foundation. (2021). “Digital Rights Management (DRM) and Restrictions on Your Devices.
- U.S. Library of Congress. (2012). “DMCA Exemptions for E-books and Accessibility.
- The New York Times. (2013). India Rejects Patent for Novartis Cancer Drug.

I took the help of AI for this task (3B) - for searching real world examples (search engine).