Linus Fulton

Task 1:

Lock-ins are often categorised into two different types: technological and vendor lock-in. Vendor lock-in refers to a situation in which the cost or effort of switching to a different vendor is so high that the customer is essentially "stuck" using the same vendor. An personal example of this is a coffee machine i own, which only works with a certain type of coffee capsule. If I wanted to switch to another coffee capsule vendor, I would have to buy a whole now coffee machine.

Technological lock-in is similar. This can be due to several issues, including compatibility issues, standards, or costs. For example, someone using wanting to switch from one operating system to another might be unable to do so, due to different file formats on each operating system.

Lock-in generally benefits the company of the locked-in product, as it "forces" the customer to stick with their product and potentially spend more money on the company.

src: https://www.cloudflare.com/en-gb/learning/cloud/what-is-vendor-lock-in/

Task 2:

- why are phishing attacks effective enough to be widespread practice?

Phishing attacks are especially effective because they target what is often the most vulnerable part of the system: the humans. Since humans are naturally trusting, it is easier to take advantage of this. Often, attackers will make use of strong emotions such as excitement or fear ("you've won a prize" or "your system is at risk") to exploit people. Phishing often tries to trick the victim into believing the source is real, such as your bank sending you an email to "confirm" your password with them. Since it is usually much easier to just ask someone to send you their account information, instead of trying to hack a database, this is the route many attackers take.

- why social engineering works on people?

Social engineering targets psychology and tries to exploit peoples natural urge to trust others. This is especially true when it comes from a figure of authority, or to follow the will of a large group. This is why social engineering attacks often are disguised to come from someone like a manager or boss, since it is expected for us to listen to them. Another common attack is the "advance-fee scam" (also known as the Nigerian prince scam), in which the human psychological effect of "reciprocity" is taken advantage of. If we do something for someone else, they will help us back. Of course, in the case of social engineering, this fact is exploited.

- why many people have hard time using passwords in secure way?

People can struggle with managing passwords due to the nature of trying to remember and keep up with the number of complex passwords for multiple accounts. Since humans are "made" to recognise and utilise patterns, we can subconsciously start using the same or similar passwords for multiple accounts, which goes against the good practice of having random and distinct passwords. The habit of using the same password is easier for us to remember, even if it leads to less secure accounts. To combat this, using a password manager is a good idea, since it requires us to only remember one secure password (ideally with 2FA), and have others stored for us.

- why PGP fails to be effective way to secure email?

PGP (pretty good privacy) deals with the issue of effectively securing email due to its complexity. The user needs to manage the public and private key and configure settings, which many can't or don't want to do. Further, social factors, such as the fact that you have to convince others to use PGP, made it even less likely to be spread to enough people to be usable.

- why it is so easy to spread malware?

Linus Fulton

Similarly to some of the other answers, the spreading of malware makes use of social and psychological effects (for example through phishing). Humans tend to trust people they know, so an auto-forwarded email with a link seems like an innocent thing. Biases that are innate to all humans are exploited for an attacker to gain access to accounts. As mentioned before, the human element is always the weakest chain in an accounts security.

Task 3A:

- Intellectual Property (IP):

IP is a term that refers to non-physical creations such as inventions, books and art works, designs, names, and pictures. Legal protections for IP include copyright, patents, and trademarks, which are discussed in more detail down below. EX: Microsoft owns the IP for the Windows 11 operating system, including for example the graphical user interface, forbidding others from copying their IP.

- Copyright:

Copyright gives the owner of an IP the exclusive right to sell their product. It usually counts for the life of the creator plus several years. EX: Microsoft owns the copyright of the Halo games, preventing others from selling their games without permission.

- Patent:

A patent grants the inventor the rights to their invention for a certain time, preventing others from making, selling, or using the invention without their permission. EX: Often, new drugs and medicines are patented to prevent others from creating the same product.

- Trademark:

A trademark protects a specific symbol or logo from being used by other companies. This is to keep confusion low, in case two companies have the same logo. EX: McDonalds “Golden Arches” aren’t allowed to be used by anyone else.

- Non-Disclosure Agreements (NDAs):

A NDA is contact that forbids the participants from sharing certain information with others. This is usually done to protect business secrets. EX: Apple might make their display providers sign a NDA to prevent them from leaking information about their newest upcoming phone.

- Watermarks:

A watermark is a symbol put on top of other symbols to indicate ownership and prevent use from others. EX: Getty Images uses watermarks to mark their stock photos until they are bought.

- Software Licences:

Software licences decide how software is allowed to be used and sold. They set restriction for the use by customers. EX: Adobe’s software licences might state that a copy of photoshop can only be installed on one computers, and isn’t allowed to be shared to others.

- Digital Rights Managements (DRM):

DRM is used to control the use and spread of software. EX: Netflix might use DRM to forbid users from downloading movies directly from their site.

- Software Protection Dongles:

A software protection dongle is a device that verifies that a computer has the correct licence to use some software. EX: AutoCAD uses a dongle to make sure the user has a proper licence.