Physical Security

I am focusing on the physical aspects of security and what potential problems are out there.

First we will go over potential threats.

1. Open computers

Open computers allows anyone nearby to just simply use the computer without proper authorization, some employees also tend to write down passwords and leave them as sticky notes incase they forget their password, making their computer more openly accessible.

1. Baiting

This is a technique of leaving open unknown USBs with either nothing or a company logo (hence baiting) and having employees to pick it up and plug into their computer.

1. Lack of physical security (IE locks, or ID scanners)

Some companies have strangely easy access for supposedly sensitive information or supplies. Some buildings have unlocked doors, and even those with scanners, tailgating is an issue. (Tailgating is where someone follows closely to another employee who has physical access and uses that employee to illegally enter the building.

1. Theft and lack of tracking

This applies mainly to IT, but people tend and do steal from the work environment. However, in some companies, theft can go unchecked and worse undocumented. Some companies do not have cameras or even have proxies (to save money) so that even if something goes wrong, it’s hard to find out the source without proper tracking.

1. Lack of security (both cyber and physical) knowledge

Many employees simply do not have standard cybersecurity knowledge, which leads to bad practice like writing down passwords, having simple passwords, being not careful around suspicious and new people in workplace, and a general lack of care to their environment.